ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA108

VERSATILE SERVICE FOR THE PROTECTION OF EXPERIMENTAL AREAS AT CERN

F. Valentini, M. Munoz Codoceo, P. Ninin CERN, Geneva, Switzerland

Abstract

CERN hosts a number of other experimental areas with a rich research program ranging from fundamental physics to medical applications. The risk assessments have shown a large palette of potential hazards (radiological, electrical, chemical, laser, etc.) that need to be properly mitigated in order to ensure the safety of personnel working inside these areas. A Personnel Protection System, typically, accomplishes this goal by implementing a certain number of heterogeneous functionalities as interlocks of critical elements, management of a local HMI, data monitoring and interfacing with RFID badge readers. Given those requirements, reducing system complexity and costs are key parameters to be optimized in the solution. This paper is aimed at summarizing the findings, in terms of costs, complexity and maintenance reduction, offered by a technology from National Instruments® based on cRIO controllers and a new series of SIL-3 certified safety I/O modules. A use case based on a service for the protection of Class 4 laser laboratories will be described in detail.

INTRODUCTION

The safety management of CERN has brought to light the need to mitigate the risks in a large number of different experimental areas of different configurations ranging from large caverns to small bunkers of a few square meters. These experiments are often the outcome of collaborations between CERN and worldwide research institutes and, therefore, access to these areas is granted to a potentially large and heterogeneous population of users.

Considering the large number of facilities we are requested to secure and the fact that the budget for safety is, in most of the cases, funded by the different home institutes, there is a strong need to look for solutions being: *simple*, in terms of architecture and number of devices to be installed; *compact,* in terms of space occupied inside the facility (a huge rack 2m high cannot fit in most of the cases); *easy to operate and maintain* and *cost effective*, especially considering that they might be used only during the short lifetime of the research activity.

Another key aspect to take into account is that, behind the purely safety interlock, a wide range of access control functionalities [1] are necessary in order to operate these facilities, such as: RFID identification of users, verification of required access rights, count of users in a zone, implementation of dedicated graphical display of relevant information for local users, and remote control/monitoring capabilities for control room operators.

In this paper we investigate the possibility to employ the NI cRIO 9030 controller [2] in conjunction with the new Functional Safety modules from National Instruments® in order to increase the global reliability and to make it suitable for safety related applications. The 903X generation of cRIO controllers are particularly interesting due to the fact that NI replaced their proprietary OS with a new version based on Real-Time Linux. This adds much more flexibility to the controller, on one hand offering the possibility to interface the cRIO with a wide palette of devices such as: USB key-board, USB mouse, video monitors, smart cameras, etc. In addition, thanks to the LabVIEW programming environment, it offers the possibility to easily implement IT tasks, such as big file management, database connections, OPC communications, image processing, complex vector/matrix manipulation, mathematical analysis, etc.

Another interesting aspect of the LabVIEW environment is the possibility to fully validate the entire user software even if the real hardware is not connected thanks to the emulation capabilities and testing tools of the programming environment. This allows to spot all logical bugs before the site commissioning tests.

CASE STUDY

The specific case study considered to demonstrate our technical proposal is the ATRAP[1] experiment [3] is has been used to apply our technical solution. ATRAP is a collaboration between CERN and Harvard University, with the intent to produce anti-hydrogen atoms and investigate their properties against their matter equivalents. To perform these measurements, a wide set of powerful class 4 lasers are employed for spectrography and for cooling the anti-electron particles down to an energy compatible with the formation of anti-hydrogen.

The ATRAP operational modes foresee to run these laser beams inside specific interlocked containment boxes that can be either closed or open. In the latter case no-one can access to the room with the exception of a restricted number of experts, who can only gain access by entering a personal pin code into a keypad.

The securing strategy for ATRAP experiment consist of a combination of two types of functionalities: access control and safety interlocks. The access control functionalities being the following:

- RFID CERN badge identification in addition to the keypad code in order to log and track all entries in the room. For this, an RFID reader has to be controlled and the access card data has to be checked against a central database storing all authorization models.

1 Anti-Hydrogen Trap

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA108

- A local HMI to provide detailed information to the laser operators on the powering state of all lasers and on the safety conditions of the room.
- Remote monitoring of all system I/O signals and other internal variables related to the safety conditions. The SCADA system used is a CERN in-house software system largely employed for supervision and maintenance purposes.

The Interlock Functions (IF) were identified in accordance with the risk assessment prescriptions that recommended a factor 100 (SIL 2) of risk reduction for ATRAP and are the following:

- **IF-1**: to *detect important operational errors and dangerous situations as the opening of a door when lasers are powered on.*
- **IF-2**: to *manage transitions between different operational modes allowing to safely operate the lasers*.
- **IF-3**: *to handle all warning signs and the evacuation sirens of the room*.
- **IF-4**: *to cut off power to every laser individually if all safety conditions are not met*.
- **IF-5**: *to maintain in closed position the two access doors by controlling a locking magnet.*

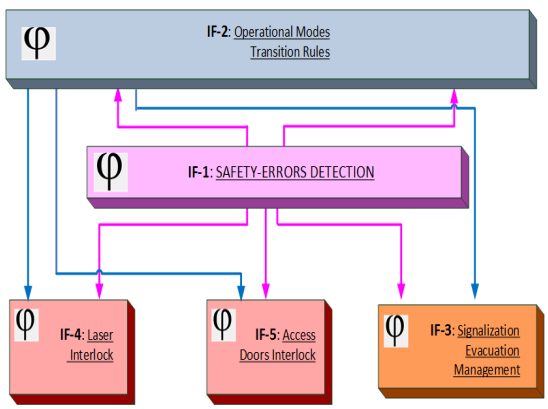

Figure 1: Interlock Functions dependence schema.

The safety objective of the system is ensured against *single point of failure* by an overlap of the interlock functions. For instance, when lasers are powered and their containment boxes are opened, the access doors are kept locked by two electromagnets (IF5) but, in case of failure, other functions of the system can ensure the complementary mitigating actions: *interruption of laser power* (IF4)*' activation of an evacuation alarm* (IF3)*, maintaining of light on all laser warning signs* (IF3).

It is an evidence that this interlock logic coupled with access control functionalities appears too complex to be constructed with a hardwired system, based only on relays or electronic components. For this reason we moved towards a solution based on a programmable controller. After analysing and prototyping different market proposals, such as the Allan-Bradley® Guard Master and Siemens PLC 1215F, we pursue our investigation on the cRIO 9030 that offers automation and IT capabilities.

NI TECHNOLOGY

The CompactRIO Controller

The main component of the proposed architecture is on the cRIO 9030 controller. It is made up of a real-time Linux OS running on a Dual-Core Intel Atom processor, an Ethernet connection embedded card, an FPGA reconfigurable chip and a wide series of modules for the I/O tasks.

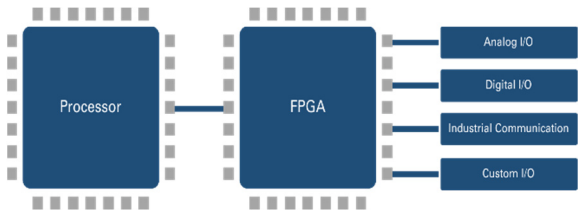

Figure 2: Architecture of the CompactRIO controller.

The real-time part of the controller includes a microprocessor for implementing network communication, data logging, control algorithms, and supporting deterministic controls thanks to the presence of a real-time OS.

The FPGA user-programmable module is completely independent from the microprocessor and it is typically used to implement high-speed controls, inline data processing, or complex timing and triggering operations.

The Functional Safety Modules

The other core component of the architecture is the new NI 9035 SIL-3 Functional Safety modules. These add a safety integrity level (according to IEC 61508) to the cRIO controller and make it suitable to operate in safety critical applications.

Figure 3: Safety Module NI 9350.

The NI 9350 are not simply a SIL rated I/O device, it features a self-contai8ned logic solver that can be used to implement safety functions independently from the main cRIO controller's chassis where it can be mounted. While these modules can provide the status of the inputs to the cRIO, the safety logic inside the NI 9350 continues to run regardless of the state and condition of the controller.

The logic in each safety module can be programmed with the Functional Safety Editor, an easy-to-use standalone tool that incorporates a graphical programming technique based on state machine formalism.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA108

In total, each module incorporates 8 digital (sink) inputs and 8 digital (source) outputs that make them very suitable in most of the cases but that require some workarounds when the safety logic is more complex.

PROTOTYPING OF THE SOLUTION

The first approach followed in our prototype was based on a clear separation between access control functionalities, all implemented in the real-time cRIO Linux part, and the interlock functions, directly coded inside the NI 9350 safety modules. However, due to the I/O limitations mentioned in the previous chapter, this approach appeared quite inefficient to be put in place, both in terms of number of modules needed to cope with the whole I/O space of our use case (*5 modules were required to pilot the 10 lasers individually*), and in terms of programming effort to distribute our complex safety logic among the 5 safety modules.

For this reasons, the solution we propose consists in using the NI safety modules to perform highly reliable diagnostic checks of the health state of the standard I/O modules and the cRIO controller, this in order to reveal dangerous hardware faults during the operational phases. The diagnostic checks constitute, then, the Safety Instrumented Functions of the system. This choice allows to drastically reduce the number of safety modules (only one is then required) and to overcome the limitations of the programming tasks. Furthermore it can be a very interesting technique to make existing cRIO based control systems more reliable with minimal development efforts.

General Architecture

The main building blocks of our system architecture are the following:

Laser Veto Relays (x10). Every relay is used in failsafe manner to allow the powering of the 10 lasers independently via normally open contacts of the relays (make contact = powering allowed).

General Veto Relay (x1). This relay is used in failsafe manner to switch off the main power feeding all other veto relays. This is done via normally open contact of the relay (make contact) that, when opened, causes an immediate shutdown of all lasers.

Input modules NI 9425 (x2): sink digital input modules used to acquire the state of the door positions (two in ATRAP), the feedback of the door locking magnets, the emergency stops, the laser powering modes and the position of the 10 laser covers. The different input signals are distributed between the two input modules in a way to minimize the impact on safety objectives of a failure in a single acquisition channel.

Output module NI 9475 (x1): source digital output module used to pilot independently the 10 laser powering relays, the door locking magnets, the evacuation siren and the laser ON warning signs.

The Controller cRIO 9030 (Real-Time part): the real-time Linux part of the controller is used to implement all non-safety functionalities, including RFID badge reader, management of a local HMI and dispatching of monitoring data to the CERN SCADA system (TIM).

The Controller cRIO 9030 (FPGA part): the FPGA integrated chip is used to implement all interlock functions described above. The FPGA controls directly the three I/O standard modules and, via the internal bus of the cRIO backplane, it dispatches the states of all I/Os and all the internal variables to the real-time part for monitoring purposes.

Safety SIL Module NI 9350 (x1): digital I/O module SIL-3 rated used to perform diagnostic checks on the cRIO controller and on the three I/O modules and to pilot the General Veto Relay.

Implementation of the Safety Functions

The FPGA part of the cRIO controller is used to compute all interlock functions while a single NI 9350 safety module is employed to perform a set of four Safety Instrumented Functions (SIF) consisting in a series of periodic diagnostic checks to ensure the correct behaviour of the FPGA chip and all the I/O modules. This, as we will show in the next paragraph, allows to increase the global system reliability without the need to translate the whole set of interlock functions, easily and intuitively implementable in LabVIEW, into the language of the safety modules.

The safety instrumented functions can be summarized as follows (see figure 4):

- **SIF-1**: *Diagnostic of Input Module 1*. It sends a check signal (DO0) to the NI 9425 Input module **1**, which has to be acknowledged (on DI0 channel) within a given time otherwise a general stop (DO2) of the laser room is performed.
- **SIF-2**: *Diagnostic of Input Module 2*. It sends a check signal (DO1) to the NI 9425 Input module **2**, which has to be acknowledged on DI1 within a certain time otherwise a general stop (DO2) of the laser room is performed.
- **SIF-3**: *Alive Watchdog Check*. DI2 awaits for a periodic alive message certifying the correct execution state of the FPGA's program main cycle. The non-arrival of this signal implies a general stop (DO2) of the laser room.
- **SIF-4**: *Software Fault Check*. The SW fault signal is computed by the FPGA user program and expected on DI3. It is built by a specific LabVIEW routine running inside the main program cycle; it periodically verifies the most relevant internal variable values against a specific set of invariant properties or logical assertions [4] that must be always TRUE during each loop. In the opposite case a general stop (DO2) of the laser room is performed.

The above safety functions perform four periodic diagnostic checks capable of revealing the most common dangerous failures that can affect the standard I/O modules or the FPGA chip and automatically act on the General Veto Relay to set the entire laser facility into a safe controlled state.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA108

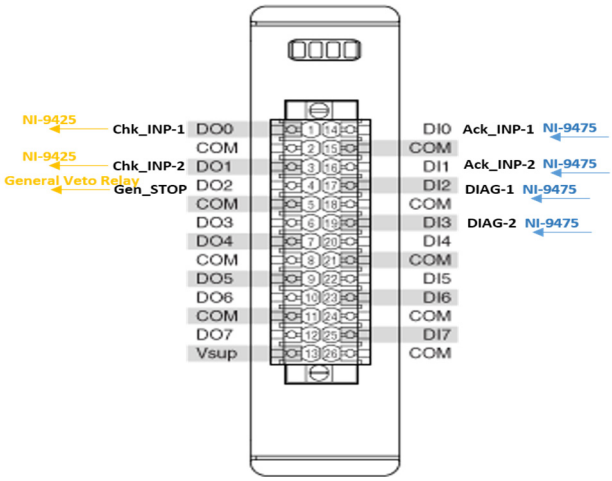

Figure 4: NI 9350 Cabling Interface.

RELIABILITY CALCULATION

In order to evaluate the increase in reliability that can be obtained with the integration of a SIL module NI 9350 into a non-safety cRIO chassis, we performed a FMEA on the system (Table 1). The following assumptions were taken for the implementation of the statistical model:

1. **Hp-1**: the failure rates (λ) for dangerous failures of the different components are derived from the general National Instruments official MTBFs and we assume that all different failure modes of the components are uniformly distributed.
2. **Hp-2**: this study does not take into account the final elements of the studied architecture, as relays, door position sensors, etc. It is mainly focused on contributions to dangerous failures given by all NI devices in the system.
3. **HP-3**: the failure rate of the NI 9030 controller is assimilated to the failure of its FPGA (*Xilinx Kintex-7*) where the interlock functions are performed. The reliability data are taken from the Xilinx reliability manual [4] that explain how to estimate the FIT (Failure in Time per billion of hours) in function of the model of chip and the size of embedded RAM for the most redoubtable failure on an FPGA: *the single event upset (SEU)* [5]. The value used is then relative to this particular failure event and calculated on the base of our model of FPGA, hosting 5MB of RAM.
4. **Hp-04**: according to NI technical specifications the failure rate (λ) per hour applicable for the SIL-3 module is 1E-08.

Table 1: Failure Mode and Effect Analysis (FMEA) for the non-SIL rated part of the system

ID	ITEM	MTBF	FAILURE MODES	TYPE	λ_D	DETECTION
1	NI 9425 Digital Input Module. 24V, 32 channel, sink.	1.25E06 h	**FM.1**: *general electrical failure in any of the powering elements of the module. As consequence all inputs are seen LOW.*	SAFE	0	
			FM.2: *failure in any component used for the serial bus communication between the module and the cRIO controller. As consequence all input channels are seen HIGH.*	UNSAFE	1.98E-07	SIF-1, SIF-2
			FM.3: *failure of a voltage comparator of an input channel. The corresponding input is seen as LOW.*	SAFE	0	
			FM.4: *failure of a voltage comparator for an input channel. The corresponding input is seen as HIGH.*	UNSAFE	1.98E-07	None
2	NI 9476 Digital Output Module. 24V, 32 channel, source.	1.09E06 h	**FM.5**: *general electrical failure in any of the powering elements of the module. As consequence all outputs are set LOW.*	SAFE	0	
			FM.6: *failure in any component used for the serial bus communication between the module and the cRIO controller. As consequence all outputs remain blocked to HIGH.*	UNSAFE	2.29E-07	SIF-1, SIF-2
			FM.7: *failure of an output channel controller setting the output to a constant LOW value.*	SAFE	0	
			FM.8: *failure of an output channel controller setting the output to a constant HIGH value.*	UNSAFE	2.29E-07	None
3	Xilinx FPGA Kintex-7 7K70T.	2.7E06 h	**FM.9**: *soft errors caused by single event upset (SEU) affecting memory cells for configuration and routing. Possible errors in interlock functions calculation,*	UNSAFE	3.7E-07	SIF-3, SIF-4

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA108

On the base of these reliability data we can easily compute via a Fault Tree Analysis (FTA) the probability of dangerous system failure (PFH) assuming to have a mission time (proof testing interval) of 1 year and 30s time of diagnostic interval performed by the 9350 SIL module.

The probability of a system failure, potentially leading to the loss of safety mission, during 1 year time can then be estimated by the formula:

$$PFH_{system} = P_r(F_{M2})P_r(D) + P_r(F_{M4}) + P_r(F_{M6})P_r(D) + P_r(F_{M8}) + P_r(F_{M9})P_r(D) \quad (1)$$

Were $P_r(D)$ is the probability of dangerous failure given by the NI 9350 module where the four safety functions are performed. Every $P_r(X)$ for **1 year** of mission time is then given by the following exponential probability distribution:

$$P_r(X) = (1 - e^{-\lambda x * 8760}) \quad (2)$$

From above we can conclude that the usage of diagnostic functions basically zeroed the contribution of failure rates FM.2, FM.6 and FM.9 lowering down the global system probability of failure from *0.0107* to *0.0037 events per year* (corresponding to a failure every 270 years) which is compatible with a **SIL-2** grade.

The employment of the safety module allows to spot a wide series of failures and to react in a safe/deterministic manner.

The main advantage of this approach is that it is possible to reach a high SIL level in a cRIO based architecture with a minimum development effort; it allows to maintain the interlock logic inside the FPGA part of the controller and it makes the development of safety related applications much more easy (take maximum advantage from the LabVIEW environment) and cost effective (one SIL rated module is necessary).

CONCLUSION

The current market offers a large range of controllers and devices suitable for safety applications from many vendors and they strongly compete with the traditional PLC technologies. Several requests to secure small experimental facilities have led us to investigate the most suitable technology in terms of: low-cost, simplicity, maintainability, availability; and also to overcome the limitations we experienced with the safety-PLCs. As reported in [6]: "*PLC programs do not deal with graphical interfaces, large data structures; they do not create files, do not perform complex operations*". This is a limiting factor for the implementation of *access control* functionalities and it is typically resolved by integration of different COTS products [1]; which may cause an unpredictable increase in complexity of the final system.

Our investigation highlighted that a high level of Safety Integrity (SIL-2) is achievable using technologies that offer a wide connectivity and bring new solutions to control serial devices, to communicate with external databases and to implement local HMIs. Our work was conducted in accordance to the IEC 61511 standard according to which the SIL level of a component can be increased by adding diagnostics functionalities.

In the domain of Functional Safety, the main driving principle of all systems is: *keep it simple*. The reason is that a Safety Instrumented System is intended to perform really simple but critical actions for which failures due to logical bugs are unacceptable. We believe in fact that the massive usage of software for implementing safety instrumented functions may present several potentially serious problems [7], evident when the user's software, in absence of strict and clear development guidelines, becomes difficult to fully test and to maintain. It is largely recognized that in any system the failures caused by software dominate those caused by hardware.

For the above reasons we are also investigating other kinds of technologies, mainly based on hardware, in order to minimize the impact of software on the global system reliability. Even though at the moment we do not have a complete and satisfactory simple hardware solution fitting all our requirements, we believe that our approach goes in the direction of this simplicity. The LabVIEW tool offers an ideal environment for the safety functions programming. Furthermore, it features powerful testing functionalities (as the tool *TestStand* [8]) that allow to increase significantly the quality of user's software and to save time during the system commission phase.

REFERENCES

[1] *Integration of heterogeneous access control functionalities using the new generation of NI cRIO 303X controllers,* ICALEPCS15 proceedings, MOPGF143, F. Valentini et al. Melbourne, AUSTRALIA, October, 2015.

[2] NI cRIO-9030, http://www.ni.com/en-us/support/model.crio-9030.html

[3] *Trapped Antihydrogen in Its Ground State*, Dissertation Thesis of HARVARD University, P. J. Richerme, Cambridge, Massachusetts, USA, 2012.

[4] *Loop invariants: analysis, classification, and examples*, ACM Computing Surveys, Vol. 46, no. 3, Carlo A. Furia *et al.,* Feb. 2014.

[5] *Device Reliability Report*, XILINX Report V10.6.1, USA, July. 2017.

[6] *What is special about PLC software model-checking?* ICALEPCS17 proceedings, THPHA159, D. Darvas, E. Blanco Vinuela, Barcelona, SPAIN, Oct. 2017.

[7] *Evaluation of Safety-Critical Software*, ACM Computing Surveys, Vol. 33, no. 6, D. L. Parnas *et al.,* Jun. 1990.

[8] TestStand tool, http://www.ni.com/teststand/whatis/