Versatile service for the protection of experimental areas at CERN

BE Beams Department

Barcelona, Spain
08-13 October 2017

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

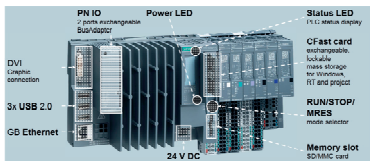
CERN hosts a number of other experimental areas with a rich research program ranging from fundamental physics to medical applications. The risk assessments have shown a large palette of potential hazards (radiological, electrical, chemical, laser, etc.) that need to be properly mitigated in order to 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.

Evaluation of Different Technologies

Solution 1: full hardware interlock (LaserMET box)

Solution 2: Siemens PLC 1215F + Simatic HMI Touch

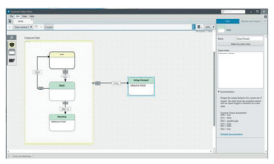
Solution 3: Siemens OpenController (Windows 7)



	LASERMET	PLC 1215f + HMI	Open Controller
Interlock logic implementation	*Prebuild relays logic. Not possible to implement custom logic.*	*Max flexibility for custom logic & HMI programming.*	*Max flexibility for custom logic & HMI programming.*
Safety Integrity Level (SIL)	*Up to SIL-4. No software, system based on safety relays & auto-diagnostic.*	*Limited. SIL I/O modules are very space consuming.*	*Up to SIL-3. I/O modules compacts and well integrated.*
Development effort	*No development, no configuration is required.*	*Very easy for logic & HMI with TIA Portal environment.*	*Very easy for logic & HMI with TIA Portal environment.*
Access control functions (RFID)	*No Possible to implement any other custom function.*	*Very difficult to communicate with a RDIF reader.*	*Very difficult to communicate with a RDIF reader.*
Connectivity Oracle DB/TIM	*NO. No possible to remotely supervise the system.*	*Very limited. Difficult to communicate with external systems.*	*Very limited. Difficult to communicate with external systems.*
Local HMI	*NO POSSIBLE.*	*Possible to program an external Simatic HMI module via TIA Portal.*	*Possible to program a HMI via the integrated WinCC. No external HMI required.*
Installation/maintenance costs	*Extremely EASY to install and maintain.*	*HIGH. Management of software versioning and updates.*	*HIGH. Management of software versioning and updates.*
Return of experience	*GOOD. More than **10** installations at CERN.*	*VERY GOOD. More than **100** installations at CERN.*	*POOR. New product, None or few installations at CERN.*
Equipment costs	*ICS-6 controller has a catalog cost of **1'900€***	*PLC 1215F, I/Os, power and HMI PC catalog cost: **1'700€***	*OpenController 1515SP + WinCC 2048pt catalog cost: **3'555€***

Functional Safety Modules NI 9350 (SIL-3)

- 8 DI Sink 24V Inputs
- 8 DO Source 24V Outputs
- Integrated logic solver, FPGA based
- IEC 61508 SIL-3 certification
- Min input response 20us
- Min output response time 5us
- Fault detection test pulses



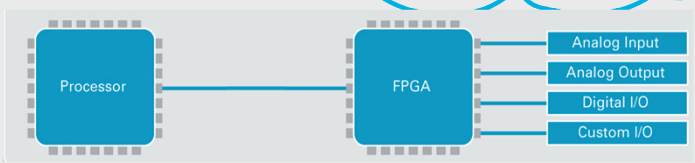
- 4 slots for C series modules
- 1.33 GHz dual Core Intel Atom
- Kintex-7 70T FPGA
- 4GB HD / 1GB RAM
- Linux RT
- 2 USB ports
- RS 432 + RS485/422
- Mini Display Port
- 100base-T Ethernet

Access ORACLE DB

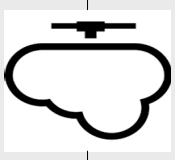
- **F-1**: Recover users ID via serial RFID badge reader.
- **F-2**: Verify access rights against a remote database containing the access models.
- **F-3**: Implement a local graphical HMI providing all relevant safety informations for local users.
- **F-4**: Export all relevant I/O signals and internal variable values for supervision and maintenance purposes.

- **IF-1**: Detect critical operational errors as the opening of a door when lasers are powered ON.
- **IF-2**: Manage transitions between different operational modes: Access, Patrol, Beam.
- **IF-3**: Control warning signs and evac sirens.
- **IF-4**: Cut power to lasers when safety conditions are not met.
- **IF-5**: Maintain all access doors in locked positions when lasers are in operation.

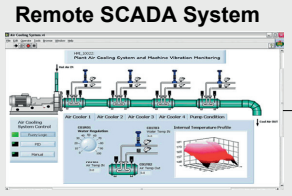
- **SIF-1**: Diagnostic of Input Module 1. A periodic check signal is acknowledged on DI0 certifying that the module-1 is operational.
- **SIF-2**: Diagnostic of Input Module 2. A periodic check signal is acknowledged on DI1 certifying that the module-2 is operational.
- **SIF-3**: Alive Watchdog Check. Signal periodically sent by a dedicated routine in the FPGA.
- **SIF-4**: Software Fault Check. A dedicated routine in the FPGA, periodically, verifies the holding of logical assertions that must always be TRUE.



Real-Time **FPGA** **Safety**



Remote SCADA System



	NI cRIO/SIL
Interlock logic implementation	*Max flexibility for custom logic & HMI programming (LabVIEW).*
Safety Integrity Level (SIL)	*Up to SIL- with the new NI 9350 Safety Modules.*
Development effort	*Easy, LabVIEW for FPGA and RT Linux + Safety Editor for SIL modules.*
Access control functions (RFID)	*Easy to implement in LabVIEW (RT Linux) using rs485 port of cRIO.*
Connectivity Oracle DB/TIM	*Easy to implement in LabVIEW (RT Linux).*
Local HMI	*Possible to program (LabVIEW) local HMI connected to HDMI port.*
Installation/maintenance costs	*HIGH. Management of software versioning and updates.*
Return of experience	*VERY GOOD. More than **50** installations, cRIO based, at CERN.*
Equipment costs	*cRIO 9030 + I/Os + 1 NI 9350 SIL Module, catalog cost: **4'960€***

Equipment Under Control

CONCLUSION

Our strong convinction is that for critical safety applications software represents a weak point and **it should not be used**, it is largely recognized that in any system the failures caused by software dominate those caused by hardware. However when it is not avoidable, because a Large palette of heterogeneous and complex functionalities have to be provided, we showed that a satisfactory Level of Safetety Integrity (up to SIL-2) can be reached also with devices other than PLCs. These could offer a more open connectivity for communicating with external databases or to implement local HMIs and allow to conceive systems more rationals In terms of cost, installation and maintenance.
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. This can be an useful approach to increase the reliability of NI cRIO based systems when it is too laborious to implement all the critical logic inside the new National Instruments SIL-3 modules.

ICALEPCS2017
Barcelona · Spain, October 8-13