# SAFETY REQUIREMENTS IN SPES CONTROL SYSTEM: PRELIMINARY DESIGN

G. Bassato, A. Andrighetto, L. Costa, M. Giacchini, Minglong Li#, G. Prete, J. Vásquez*
INFN, Laboratori Nazionali di Legnaro, Viale dell' Universita' 2, 35020 Legnaro PD, Italy
#on leave from China Institute of Atomic Energy, Beijing 102413, PRC
*on leave from Universidad Simón Bolívar, Caracas, Venezuela

*Abstract*

SPES (Selective Production of Exotic Species) is an INFN project whose aim is the realization of a RIB (Radioactive Ion Beam facility) as an intermediate step toward EURISOL. The site selected for SPES is Legnaro National Laboratory (LNL), in the north-east region of Italy. The main reason for the site selection is the availability at LNL of the superconducting Linac ALPI, which will be used as re-accelerator of neutron-rich nuclei with mass in the range 80-160 to an energy of 8÷13 MeV/u. The schedule of SPES project foresees the beginning of building construction in 2010 and the completion of the facility by the end of 2014. We report a preliminary analysis on control system requirements for safety applications.

## FACILITY OVERVIEW

The RIB facility is based on two main components: a proton driver and a production target coupled to the ion source. Since the first technical proposal in 2002, the choice of the proton driver underwent many revisions. In 2008 INFN management decided for a commercial cyclotron with an energy up to 70MeV and a current of 750μA. The ion source is of surface ionization type with the possibility of superimposing a laser beam to improve selectivity using the photo-ionization process; a charge breeder will provide the charge state required for the optimal injection into the Linac. To produce high purity exotic beams a HRMS (High Resolution Mass Spectrometer) with a mass resolution 1/20000 is also planned. The most innovative (and critical) part of the SPES facility is the target, based on a novel concept of a multi-disk UCx device, optimized for power dissipation and release time of fission products. According to the simulations, a rate of $10^{13}$ fragments/s will be achieved with a proton beam power of about 8 kW, that is relatively low if compared to that required in other RIB installations, thus reducing the impact on civil construction and radioprotection requirements. The SPES project also includes the realization of a neutron facility for medical (BNCT, Boron Neutron Capture Therapy) and material science applications (see Fig. 1); this latter will be based on the operation of a high current RFQ (5MeV, 30 mA proton beam) originally designed for the TRASCO project (transmutation of nuclear waste) and now under assembly; the construction of BNCT and neutron physics facility is scheduled from 2012.

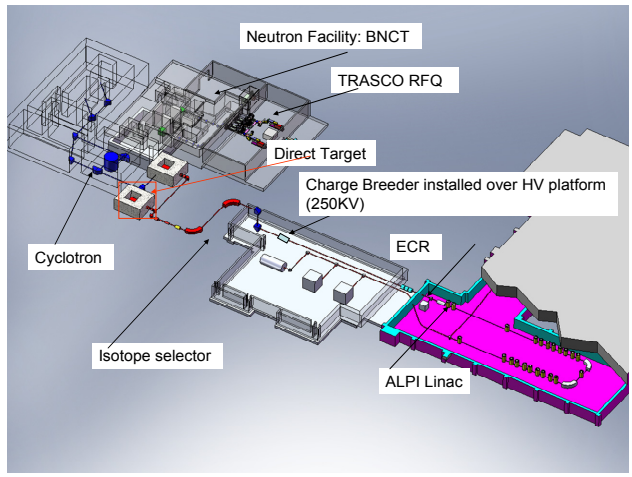


Figure 1: Facility layout.

## RADIATION SAFETY ASPECTS

The neutron and gamma production by the high energy proton driver and the radiation activity induced in the Direct Target by the Uranium fission (estimated $10^{13}$ Bq) are the items imposing the most severe constraints in the design of the radioprotection system. Differently from the accelerators currently in operation at LNL (the Tandem and the Linac, where the beam current is negligible and the activity induced around the experimental targets is low), SPES will require the application of the most up-to-date techniques of nuclear engineering to minimize the hazard of contamination and comply with the safety rules imposed by the Italian law. A part the target itself, there are many ancillary components that can undergo activation in the ion source area (i.e. vacuum pumps, heat exchangers and venting systems etc.) A bunker with concrete walls of 3 m. width is foreseen to stock the exhausted targets and the material resulting from maintenance of devices exposed to the high neutron flux.

The radioprotection system must provide the control over a distributed topology including, in the first phase of the SPES project, several areas in the cyclotron and target buildings; it has to be easily extensible to integrate the BNCT facility when this part of the project will be funded. Safety and highest availability are the primary concepts underlying its design.

## SELECTING THE TECHNOLOGY FOR SAFETY

It's a commonly accepted statement that a control system designed for safety critical applications should be based on PLCs. Many good reasons support this assumption: these devices, targeted for heavy duty applications in harsh environments, offer a variety of components and configuration schemes to bring the reliability to the highest level. In a nuclear installation like SPES, the control system capability of preserving its functionality under fault conditions is highly desirable for all subsystems but is mandatory for the machine protection and radioprotection systems. So, when looking for PLC technology for safety we focused on products suitable to implement fault tolerant solutions. Fault tolerance is a quite wide concept that doesn't simply indicate a specialized family of devices but is the result of a careful choice of hardware components, software and configuration. According to Siemens terminology (we'll refer to Siemens products in the following discussion, but devices with similar characteristics are available from major PLC manufacturers) we should distinguish between "fail safe" and "fault tolerant" devices. A fail safe PLC (i.e. Siemens F-series) is a component in which some hardware elements are duplicated: in particular, the CPU has separate memory blocks for standard and safety-related data. During the normal operation, diagnostic checks are performed transparently to the user application. Even if a single fail-safe processor used in conjunction with F-series I/O modules (devices that have a dual-channel internal design) allows to achieve a good level of reliability (Safety Integrated Level = 3, according to the IEC 61508 standard [1]), we consider this solution not adequate for the control of safety-critical systems. For this class of applications the fault tolerance should be based on a full redundancy of hardware elements. If a loss of control can be tolerated for a period not greater than a few seconds, a good approach could be constituted by a "soft redundancy backup". This solution is based on a distributed architecture (Fig. 2) in which two CPUs (Master and Reserve) are connected, through a dual channel communication interface, to a remote subsystem where the I/O modules are installed. The CPUs use a third link to exchange data among them and maintain in their memory a synchronized copy of data and code. If the master station fails, the reserve takes the control over the remote hardware. Figure 3 shows the result of a test: the soft generated ramp stops for about 2 sec. when the master is turned off. A not negligible advantage of this scheme is the reduced cost because it can be implemented using standard processor modules.

For applications where the availability of control is imperative and a latency can't be tolerated even for a short time (this is the case, for example, of the machine protection system) specialized processors are available to implement full hardware redundant schemes (i.e. Siemens S7-400-H series). This architecture relies on fast, dedicated links between the CPUs (based on optic fibers and proprietary synchronizing modules). The cost of this solution is high.

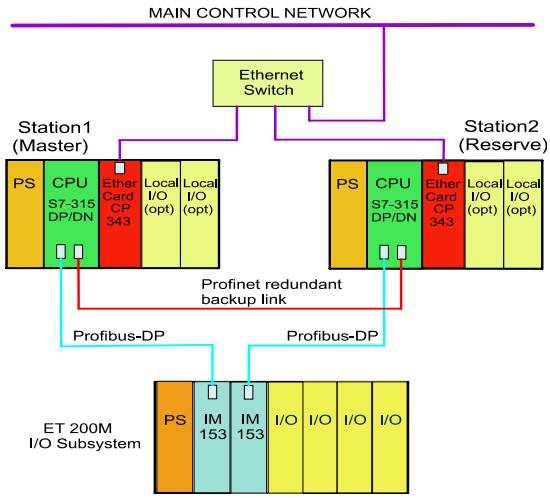


Figure 2: Layout of a redundant configuration based on software backup (hardware modules by Siemens).

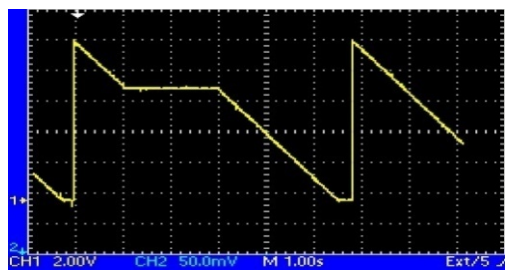


Figure 3: Timing of master to reserve switching.

The choice of a particular technology or configuration depends on many factors and finding the optimal compromise between the cost and reliability for each facility subsystem or instrumentation class is not straightforward. We summarized in Table 1 a preliminary classification of controlled areas and applications and indicate for each of them a suitable technical approach.

Table 1: PLC Control Application Examples

| Control Application | PLC Architecture |
|---|---|
| Vacuum instrumentation, magnet cooling system, conventional services. (SIL2 SIL3 are both adequate) | Standard PLCs or Fail Safe CPUs in NON-redundant configuration. |
| Radiation monitors, Personnel Access Control, cooling systems in the Target area: SIL3 minimum | Redundant configuration based on software backup and distributed I/O. |
| Machine protection system, control of beam dumpers, critical interlocks. SIL4 mandatory | Full hardware redundancy based on specialized CPUs closely tied by high speed links e.g. Siemens S7-400-H. |

## SPES CONTROL SYSTEM

The control system of the facility will result from the integration of different technologies. We chosen EPICS as general framework for software development and, as consequence, the Channel Access will constitute the "middleware" underlying the communication among the different subsystems. Where possible, we'll use "native" EPICS IOCs for the control of the accelerator instrumentation: in this category we can include, for example, the secondary beam diagnostics, the HV power supplies used for the electrostatic deflectors and the ion source platform, the charge breeder, the mass separator and all general purpose instruments for which there is no strict demand for fault tolerance. Most of EPICS IOCs will be embedded controllers running under Linux: few of them (i.e. MicroIOCs delivered by CosyLab) are already installed for the control of various equipments in the Target prototype Laboratory [2]; in cases where a fast and deterministic response is important (i.e. in the beam diagnostics) we plan to use VME systems running under Vxworks.

We are aware that some recent EPICS developments are in the direction of supporting redundant configurations for high availability [3], but for applications that can affect the personnel life we must rely on certified devices. We also know we shall have a limited chance of imposing technical solutions on systems that are delivered as turn-key (the cyclotron is the first example) and, by the other hand, we must integrate the control of existing accelerators (i.e. the radioprotection system of the Linac).

Integration among PLC based systems is rather straight-forward thanks to the OPC technology that allows exchanging data among CPUs of different manufactures using a common communication interface. The integration of PLCs in the EPICS network can be accomplished using well proven technical solutions that have been developed in some Laboratories [4] and made available to the EPICS community. The most used method consists in having an IOC server running on a Windows PC connected to the LAN; the process variables are accessed from the PLC memory through a device driver specific for each PLC family and then exposed to the Channel Access; as alternative, PLC data can be accessed through an OPC server [5].

A still open issue is the choice of a general supervisor for all facility subsystems. As well known, EPICS includes many native tools (i.e. EDM) for creating graphic interfaces; while these tools are suitable for rapid prototype development, they probably are not the optimal solution for the design of a new control system that should remain in operation for 20 years at least. Other more modern tools based on Java are available: a nice and powerful solution is CSS (Control System Studio) [6] originally designed at DESY and whose development is being carried out in collaboration with Argonne, SNS and Los Alamos National Laboratories.

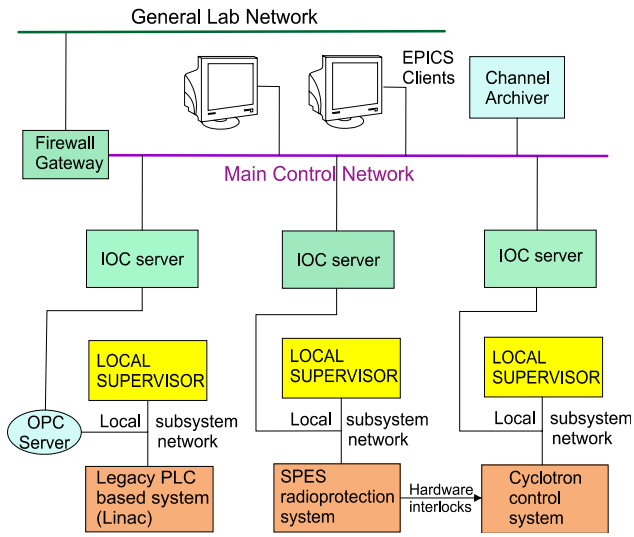


Figure 4: Integration of PLCs into the main control network.

A possible alternative we are also considering for the development of the graphic interface is using LabView (officially supported by National Instruments as EPICS client since the release 8.6); the result is appealing from the point of view of graphic rendering, but extensive tests must be done to verify the reliability and the response time when the number of process variable becomes high.

## CONCLUSION

Several PLC based systems will have to be integrated in the control of SPES. The technology used for the control of the cyclotron will likely drive the choice of PLCs for the radioprotection and safety-related systems. For pre-existing installations, for which there is no availability of EPICS drivers, we'll use OPC servers as communication gateway; for new installations we'll make use of IOC servers as described in [4]. At the upper level, all subsystems will be unified under a common communication protocol constituted by the Channel Access. The EPICS Channel Archiver will be the main archiving tool of the overall facility.

## REFERENCES

[1] http://www.iec.ch/zone/fsafety/
[2] M. Giacchini et al., The Control System of SPES Target: Current Status and Perspectives, These Proceedings.
[3] M. Clausen et al., Redundancy for Epics IOCs, Proceedings of ICALEPCS07, Knoxville, USA.
[4] http://epics.web.psi.ch/software/s7plc/
[5] http://www-csr.bessy.de/control/SoftDist/OPCsupport/
[6] http://css.desy.de/content/index_eng.html