ALBA, THE PLC BASED PROTECTION SYSTEMS

D. Fernández-Carreiras, D. Beltran, J. Klora, O. Matilla, R. Montaño, M. Niegowski, R. Ranz,
A. Rubio, S. Rubio-Manrique, CELLS, Bellaterra, Barcelona, Spain

Abstract

Alba [1] is a synchrotron light source under installation located nearby Barcelona. This 3 GeV third generation light source is planned to deliver the first X-rays beam to the users in 2010 [2]. The Linac has been commissioned in 2008 and the booster will be commissioned in December 2009. The Equipment Protection System (EPS) and the Personnel Safety System (PSS) ensure that the operations are done safely for the machine components and people. Both have many similarities, although the purpose and the technology are different.

The PSS is an independent system built on Pilz Safety Programmable Logic Controllers (PLCs)[3]. It is designed to match the Safety Integrity Level 3 defined in the norm IEC 61508.

The EPS on the other hand is fully integrated in the control system. It is based on B&R PLCs [4]. The EPS is complemented with a redundant fast protection system (Fast interlocks Units) implemented on the event based timing hardware (Event Generator, Event Receivers and fiber optic Links).

PSS

PSS provides access to restricted areas, such as Linac, Tunnel and Beamline lead hutches, and surveys radiation levels. It prevents people to get a radiation dose higher than the limits given by the law. It is subjected to Ionizing Radiation Regulations. It is independent from any other system in Alba and the Spanish Nuclear Safety Council shall approve it.

The PSS is governed by the international norm IEC 61508. It rules the use of electrical and software driven safety systems to provide risk reduction up to an acceptable level. The ALBA PSS Safety Integrity Level aims SIL3. Besides this, the PSS follows the rule of "Redundancy and Diversity". Redundancy will be achieved by having two independent lines for every signal (as specified SIL3 in the norm IEC 61508). Diversity means that any action will be applied to two different parts of the system, for example disabling the RF comprises revoking the permit for the RF driver and for the High Voltage Power Supplies (HVPS). In other words, each action results in two redundant outputs. The installation of the system has been outsourced and is being achieved by the companies Pilz and PROCON. Although the PSS is one independent system, It has two parts: Accelerators y Beamlines, The accelerators PSS controls the Tunnel and The Linac bunker. It consists of two PLCs intercommunicated by the safety bus. The tunnel has four access doors, whereas the linac bunker has one door.

Hard X-Ray beamlines have two hutches controlled by the PSS. In the case of Soft X-Rays beamlines only the Optics hutch is lead-shielded and controlled by the PSS. A beamline has a "quite-independent PSS" with a dedicated PLC connected to the Acelerators PSS (Main) by the Safety Bus..

Functionality

The radiation monitors, manufactured by Thermo [7] (FHT 6020A controller) are distributed in the service area and experimental hall. They monitor both gamma and neutron doses integrated over four hours and providing two alarm levels. Each alarm level has a Pilz PNOZ S4 Safety Relay, activated when the radiation reaches the alarm threshold. All inputs/outputs to/from the PSS are digital. Every door has two different limit switches (redundant and diverse) and a magnetic lock (Pilz PSEN lock, and PSEN code).

Interlocking the doors once the restricted areas have been evacuated ensures access control. In order to make sure that a zone is clear of personnel, a search patrol is needed. A Search patrol is started from the control room and performed in bunker and tunnel by two authorized people. Once the Permit is given in the control room, the patrol begins. Nobody but the person performing the patrol is allowed in the bunker and tunnel. Search buttons all around the tunnel are pressed in sequence. Every button has to be pressed in a time interval, not before a minimum time and having a timeout. The PSS has four main states, OPEN (free access), INTERLOKED (once the search patrol has been completed, RESTRICTED, and SAFE. An indicator shows also the presence of beam in the restricted areas. The restricted access function is implemented only for the Accelerators PSS in order to make short interventions in the restricted areas without needing a new patrol. This restricted access mode is allowed in the control room to one (up to six) authorized person (magnetic card). After taking one of the personal keys this person can go in the restricted area. Once all keys are in place in both the door cabinet and the control room, the system goes to interlock again. When an unsafe condition arises, the system goes to safe state. Doors are unlocked only after a decay time, unless an emergency stop is pressed.

The Control Room

The SCADA and the Operation keys are in a cabinet in the control room. The SCADA, only meant for monitoring and diagnostics, reads tags from standard (not-safety) data blocks in the PLCs. It does not have write access to the PLC. The most critical operation permits are given with physical keys. The Pulsed power supplies and the Booster and Storage Ring bending magnets can also be manually disabled from the control room.
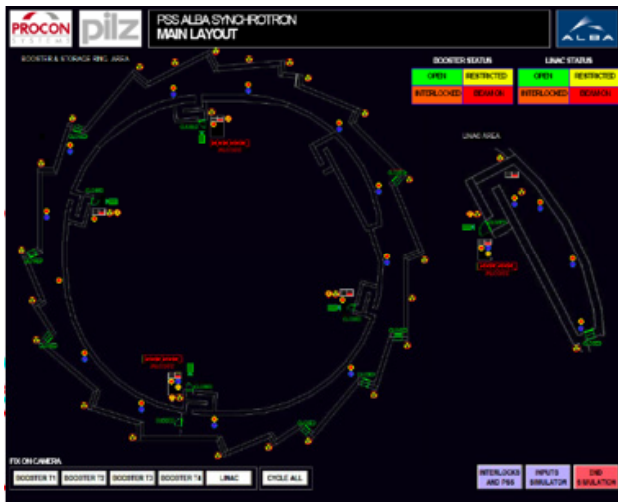
Figure 1: View of the PSS SCADA.

Architecture and Technology

The system is built around the Pilz PSS SB2 3006-3 ETH-2 CPU, two of them for the accelerators, tunnel and linac, and one for each beamline. All CPUs are intercommunicated by a Pilz Safety Bus (certified SIL3). Keys, door switches, emergency stops and relays are also SIL3. Safety relays are installed in radiation monitors, Bending magnet power supplies, Radiofrequency (RF) High Voltage Power Supplies (HVPS) and Inductive Output Tubes (IOT), as well as in other electronic boxes like the RF detectors and the Electron beam current detectors. The RF waveguides and Front-End Shutters have also SIL3 PILZ PSEN 1.1p20 switches.
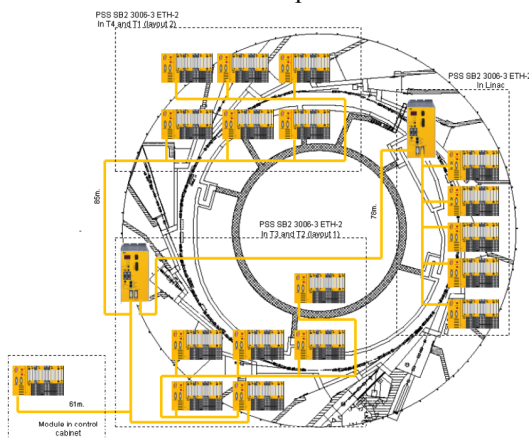

Figure 2: General architecture of the PSS.

Logic

The logic is organized in permits and interlocks, a permit is the result of a set of conditions fulfilled. An interlock is a condition for granting or revoking permits. For example, in order to open the front-end, the hutch must be interlocked, emergency-stops armed, the operation keys in place, etc.
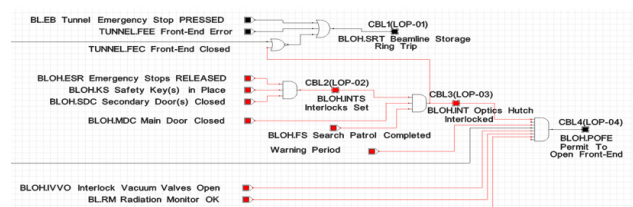
Figure 3: Extract of the logic for one beamline. Permit to open the front-end.

EPS

The Equipment Protection System manages permits and interlocks avoiding damaging the hardware. It is built on B&R PLCs with CPUs installed in cabinets in the service area and distributed I/O modules installed in shielded boxes inside the tunnel. CPUs and Remote interconnected by the X2X fieldbus. PLCs manage interlocks, temperature readouts, flowmeters, flowswitches, thermoswithces, actuators for shutters, fluorescence screens, etc. The typical cycling time is of few milliseconds, whereas the Ethernet powerlink cicling are few microseconds. Vacuum devices, Radiofrequency plants, and power supplies interlocks are also managed by the EPS. The PSS and the EPS are totally independent from both hardware and software point of view.

Architecture and Technology

Around six thousand signals are handled by 49 B&R CPUs X20CP1484 having a Celeron 266 32 MB DRAM, 1 MB SRAM, Ethernet PowerLink and a regular Ethernet interface 100 Base-T.
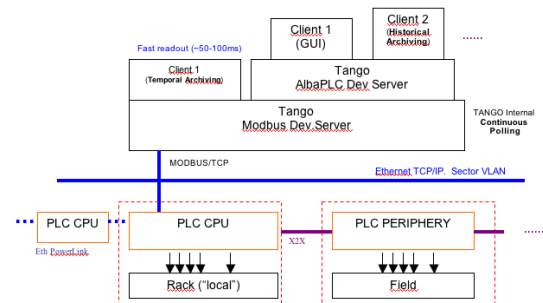
Figure 4: Architecture of the EPS PLC system.

In addition, 101 periphery cabinets are linked to the CPUs by the X2X bus. Lead-shielded boxes are installed inside the Tunnel to make cables shorter and cheaper and easier to install. A fast communication Ethernet PowerLink runs on a separated Virtual Local Area Network (VLAN). It is a deterministic OSI Level2 network. Interlocks between different subsystems are transmitted over this media.

Other services, Graphical User Interfaces (GUIs), etc in the control system communicate via Ethernet with the PLCs. The PLCs is connected to the main control system VLAN in that sector (or beamline). A Tango device server polls values from PLC CPUs using Modbus/TCP. On top of this, another Tango device Server, AlbaPLC provides dynamic attributes named according to the field

devices, in order to make easier the integration in the Tango clients.

Automatic Code Generation

The controls and cabling database stores the information concerning not only cables, but equipments, channels, connectors, domain names, boot servers, etc. In particular all equipment codes with channels names and connections are stored in this database.

Figure 5: Excel application for EPS code generation.

Most of the code in the PLC is generated automatically from the cabling database. A Visual Basic Script running in excel generates another file containing the declaration of variables, data structures, software tasks, modbus mapping and documentation. The interlock logic is not produced automatically yet. Additionally, Tango attribute names and the expert GUIs are also generated from the controls equipment and cabling database.

Figure 6: One of the expert GUIs of the EPS.

Subsystems and Logic

The EPS covers mainly six subsystems. Those are, Vacuum, Magnets, RF, Insertion devices, Front-Ends and Beamlines. The logic of those subsystems is complex and has many particularities. For example cooling water in magnets and temperatures are surveyed by the in order to interlock the corresponding power supply when an unsafe condition is produced. Though, as a general rule, when a problem arises, other subsystems shall be informed. In particular if a vacuum valve closes as a result of an overpressure in a vacuum pipe, the RF shall be shut down

Protection Systems

and the beam killed. This communication is transmitted over the PowerLink.

FAST INTERLOCK, EPS AND PSS

The PSS and the EPS are totally independent systems. The PSS gives and revokes permits whereas the EPS manage the actuators. For example, the Bremsstrahlung shutters are operated by the EPS, but the permit to open is given by the PSS on a different channel. Both EPS and PSS have their own switches in the shutters. PSS uses Pilz magnetic switches (SIL3), whereas the EPS reads Telemecanique mechanical switches on the same device. Both EPS and PSS actuate on the millisecond range. A Fast Interlock system working on the microsecond range complements the EPS. It is implemented on the Timing system, using fiber-optic links, Interlocks are transmitted from any Timing event receiver to the event-generator and from there distributed to all event-receivers. In other words, the Timing system has been upgraded to be bidirectional and therefore, besides synchronization, provides the infrastructure for transmitting fast interlocks from anywhere to everywhere in the accelerators. In most cases an interlock is communicated over both the Fast Link and the PLCs.

CONCLUSION

Nowadays, the PLC technology is used in a wider range of applications that traditionally were linked to other technology. Safety PLCs are today a common choice in the industry for high risk environments where a failure might have many people killed, like trains, etc. Also, standard PLCs are cheaper, smaller and more powerful and we found a large variety in the market today. A distributed system combining Ethernet (used as a fieldbus) and a proprietary X2X fieldbus is proven to be cost-effective solution. Periphery can be closer to the devices, making cabling easier and cheaper.

CONTRIBUTIONS

REFERENCES

[1] http://www.cells.es
[2] D. Einfeld, "Status of the ALBA Project", Proceedings of EPAC-06, Edinburgh 2006.
[3] http://www.pilz.com
[4] http://www.br-automation.com
[5] D. Beltran et Al, "Alba Controls and Cabling database". These proceedings.
[6] http://www.tango-controls.org
[7] http://www.thermofisher.com