PERSONNEL PROTECTION, EQUIPMENT PROTECTION AND FAST INTERLOCK SYSTEMS: THREE DIFFERENT TECHNOLOGIES TO PROVIDE PROTECTION AT THREE DIFFERENT LEVELS

D. Fernández-Carreiras, D. Beltran*, J. Klora, J. Moldes, O. Matilla, R. Montaño, M. Niegowski, R. Ranz*, A. Rubio, S. Rubio-Manrique, CELLS, Cerdanyola del Vallès, 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 2012. The Linac has been commissioned in 2008, the booster in 2010 and the Storage Ring in 2011. The seven Beamlines included in the “Phase One” are being commissioned at the end of 2011.

The Fast Interlock System, Equipment Protection System (EPS) and the Personnel Safety System (PSS) ensure that the operations are done safely for the machine components and people.

All three use independent hardware and communication channels, and they guarantee different response times and safety levels. The Fast Interlock System, works in the microsecond range, the EPS in the millisecond, and the PSS has a cycle time of 150 milliseconds. However, the PSS has some extra requirements, since it is related to human lives safety, and therefore it requires the highest possible reliability. It ensures a Safety Integrity Level 3 (SIL3) according to the international norm IEC 61508.

FAST INTERLOCK

The Fast Interlock is implemented upgrading the single channel links channels employed by the Timing system, to a bidirectional system. It is based on events, relying on a tree architecture where the root (event generator) gathers and redistributes the interlock events from/to all the leaves (event receivers). Each event receiver is configured to perform an action (i.e. activate pulse on an output) for a particular event code. The cards (event generators, event receivers and fiber optics fan-outs) have been produced by MRF [2]. There is one event generator and about 88 Event Receivers distributed, which currently have configured about 480 connections to equipments [3].

When an interlock signal is produced in the Beam Position Monitors (BPM), Radio Frequency plants (RF), and Front Ends (FE), it is transmitted back to an event-receiver adjacent to the event generator which redistribute the events to the whole tree. The fiber optic links have all a fixed length, 200 meters, required for ensuring the precision in the synchronization events. The time between the generation of one interlock event in one node, and the reception is in the order of four microseconds.

The fast interlock system, provides accurate timestamps of each event (interlock), allowing a 8 nanosecond resolution in the discrimination of interlock-events for postmortem analysis.

EPS

Besides few hundreds of interlock signals, which require an action in the microsecond range, there are other seven thousand managed by the EPS. The EPS guarantees a transmission in the millisecond range. Typically the cycle times are below the 20 ms. The EPS is responsible for all interlocks in the machine and the beamlines. All signals managed by the Fast interlock are also backed up by the EPS.

The Equipment Protection System manages permits and interlocks avoiding damaging the hardware. It is built on B&R PLCs [4] with CPUs installed in cabinets in the service area and distributed I/O modules installed in shielded boxes inside the tunnel and in the beamline hutches. CPUs and remote periphery are interconnected by the X2X fieldbus. A deterministic network, Ethernet-PowerLink, interconnects all CPUs to each other.

Architecture and Technology

The EPS is built on a network of PLCs and remote peripheries. The EPS for the Accelerators includes 56 B&R CPUs X20CP1484, all equipped with Ethernet interface 100 Base-T and Ethernet PowerLink.

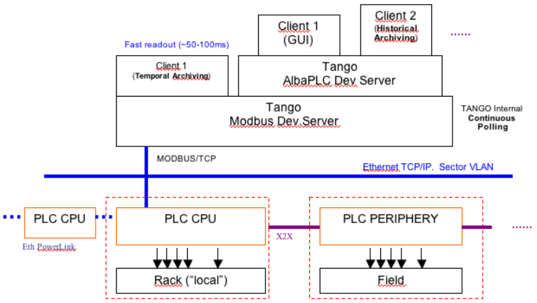

Figure 1: Architecture of the EPS PLC System.

In addition, 110 main periphery cabinets are linked to the CPUs by the X2X bus. Lead-shielded boxes are installed inside the Tunnel to make cables shorter, cheaper and easier to install. The deterministic Ethernet PowerLink network runs on a separated industrial switch. It is a deterministic OSI Level2 network. Interlocks between different subsystems are transmitted over this media. Every Beamline has an independent system, usually composed by one CPU and 2 main remote peripheries, having few hundreds of signals. Figure 1 shows the conceptual design of the EPS.

The standard Ethernet network handles communication with Human Machine Interfaces, Archiving services, etc.

*On leave

Copyright © 2011 by the respective authors — cc Creative Commons Attribution 3.0 (CC BY 3.0)

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 SCADA.

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.

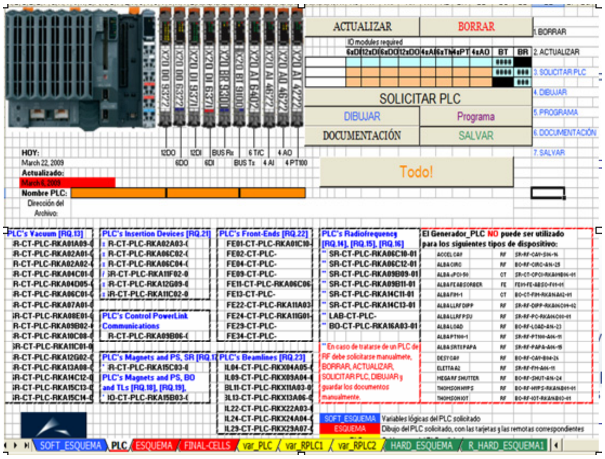

Figure 2: Excel application for EPS code generation.

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. Figure 2 shows a view of this excel file. The parts of the code still excluded from the automatic generation are the logic conditions. Additionally, Tango attribute names and the expert GUIs are also generated from the controls equipment and cabling database.

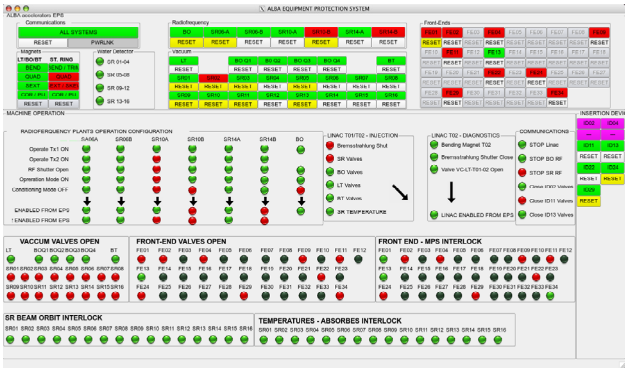

Figure 3: The main EPS GUI for the Machine.

Subsystems and Logic

The EPS covers mainly six subsystems. Those are: Vacuum, Magnets, Radio Frequency, Insertion devices, and Front-Ends. Besides, every Beamline has an independent EPS system, connected to the Accelerators with eight wired signals. The logic of each subsystem is complex and adapted to every particular case. As a general rule, when a problem arises, any other subsystem 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 and the beam killed. All these communications are transmitted over PowerLink, although there are some cases considered more critical which are also wired from one PLC to another, like interconnections of different vacuum sectors or as we have just mentioned, the links between Beamlines and Front-Ends. Figure 3 shows the main user interface for the Equipment Protection System.

PSS

The PSS is an independent system built on Pilz Safety Programmable Logic Controllers (PLCs) [5]. It manages 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. 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 “Independent” PSS with a dedicated PLC connected to the Acelerators PSS (Main) by the Safety Bus. It can be disconnected from the Main PSS, only in some well defined safe conditions. In case of failure it provokes the Main PSS goes to safe state.

Functionality

There are 24 radiation monitors, manufactured by Thermo [6] (FHT 6020A controller) are distributed in the service area and experimental hall. They monitor both

Copyright © 2011 by the respective authors — cc Creative Commons Attribution 3.0 (CC BY 3.0)

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, one of which works also as 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 persons performing the patrol are 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 "interlocked" 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 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.

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.

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.

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. Where the required response times are several microseconds, a solution with PLCs is not viable anymore. Those cases are often a reduced subset and can be accomplished with "ad-hoc" solutions. For this particular case, the upgrade of the Timing system, to support bidirectional links for implementing fast Interlocks, took place. It was proposed by Alba and Implemented and made available in the market by MRF.

CONTRIBUTIONS

Many people has worked in these projects, in particular we would like to thank X. Queralt, the Safety Officer, S. Marchal, B. Saló, J. Jamroz (electronics group). Also, special thanks to P. Berkvens, the safety officer of the ESRF, for his help and his advises with the PSS logic. The EPS is one of the most important customers of the cabling database, developed and maintained by CELLS Management Information System group, especially I. Costa and O. Sánchez.

REFERENCES

[1] CELLS-ALBA. http://www.cells.es
[2] MicroResearch Finland. http://www.mrf.fi
[3] O. Matilla et Al, "The Alba Timing System. A known architecture with a Fast Interlock System Upgrade". These proceedings.
[4] B&R Automation. http://www.br-automation.com
[5] Pilz. http://www.pilz.com
[6] http://www.thermofisher.com

Copyright © 2011 by the respective authors — cc Creative Commons Attribution 3.0 (CC BY 3.0)