View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by CERN Document Server

THE UPGRADED ELETTRA ACCESS CONTROL SYSTEM

A. Vascotto, D. Bulfone, F. Giacuzzo, S. Grulja, M. Lonza, G. Tromba, Sincrotrone Trieste, Italy
A. Mazzoli, M. Salvador, FASI TECH srl, Pordenone, Italy

Abstract

The access control system of the ELETTRA accelerators must guarantee that access to the machine tunnels is allowed when safety conditions for personnel are fulfilled.

The system is based on Programmable Logic Controllers (PLCs) providing redundant logic in a fail-safe configuration.

At present, the supervisor consoles of the system are based on UNIX PCs running the Santa Cruz Operation (SCO) operating system and X-11 applications. These are being replaced by Microsoft Windows NT PCs, equipped with a SCADA (Supervisory Control And Data Acquisition) package, which is used for the development of the new application programs.

1 THE ACCESS SYSTEM LOGIC

The ELETTRA access control system [1] is made of Programmable Logic Controllers (PLCs) supervised by Santa Cruz Operation (SCO) UNIX PCs located in the linac and storage ring control rooms. The system main characteristics are fail-safe logic, redundancy and ultimate operator authorization. The fail-safe logic guarantees that if a fault occurs to the safety dedicated equipment the machines are stopped in a safe status; the redundancy assures that permission to enter a controlled area is given only if at least two independent safety conditions are fulfilled. The operator intervention is eventually requested to provide the final assent during an access procedure or to verify that nobody is present inside the accelerator tunnels (patrol inspection) before starting-up the machines after a shutdown.

The access control system considers the ELETTRA facility as divided into three logical areas (fig. 1): the linac, the Transfer Line (TL) and the Storage Ring (SR).

There are one entrance door to the linac (A1) and two entrance doors to the ring (A2 and A3). The T1 and T2 doors delimit the TL. Three emergency exits are located along the linac tunnel (E1, E2 and E3) and two around the SR (E4 and E5); the SR entrance doors themselves (A2, A3) can be used as emergency exits.

The linac and the SR, which are physically separated by the TL, can be operated independently from each other.

The access control system gets data from the TL and SR beamstoppers, linac gun, linac and SR radio frequency (RF), door proximity switches, entrance equipment (badge reader controllers, key panels), emergency and patrol buttons, beamlines. According to the status of these inputs the PLCs permit or interdict the operation of the accelerators and subsequently control the access to the machine tunnels.

Access to the linac tunnel is allowed if its gun and the RF accelerating sections are switched off. Access to the SR tunnel is permitted if the beam has been dumped and, in case the linac is on, the beamstoppers placed along the underground section of the TL are closed. Access to the TL (through T1 or T2) is allowed only if both the linac and SR are switched off.

The beam dump in the SR is performed through a double action: a short interruption of the RF cavities driving signal and the closure of the SR beamstopper.

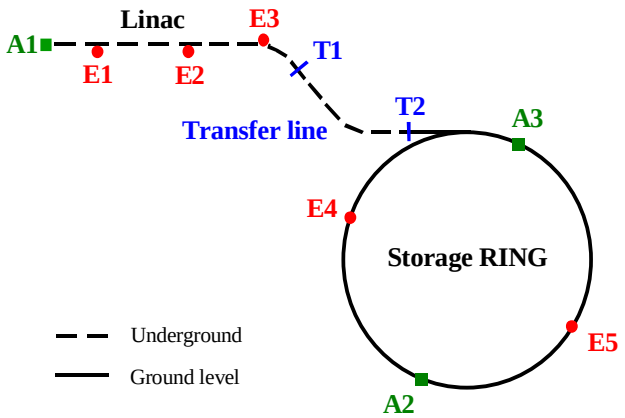

Figure 1: Logical areas

The access procedure for entering the accelerators during a stand-by period consists of four successive steps:

- the entering person presents his badge to the automatic badge reader; if the accelerator is switched off and the badge identifier was pre-loaded in the list of authorized personnel, the system gives the first assent to open the door;
- one of the keys on the panel close to the door is automatically unlocked and the person takes it out;
- the control room operator, after recognizing the person through a TV camera, gives the third assent and unlocks the door;

- the person enters, closes the door and deposits the key into an internal panel.

Exit operations require similar steps, but with an opposite sequence: the person takes the key out from the internal panel, opens the door by pressing a button, deposits the key in the external panel and presents the badge.

During the shutdown periods free access is permitted and all the doors are unlocked.

2 THE UPGRADE PROJECT OBJECTIVES

The upgrade involves only the supervisor consoles while the low level PLCs are not modified.

The main objectives of the upgrade project are:

- the use of a new hardware/software platform for the supervisors, Y2K compliant, with improved graphic interface and management tools;
- the use of a RAD (Rapid Application Development) environment, to facilitate the development of the application software and Graphic User Interface (GUI);
- the use of Local Area Network (LAN) PC cards able to run both the Sinec H1 and the 'standard' TCP/IP protocols, in view of future upgrades of the PLCs;
- to improve the diagnostics for the operators.

3 HARDWARE ARCHITECTURE

The new hardware architecture is shown in fig. 2.

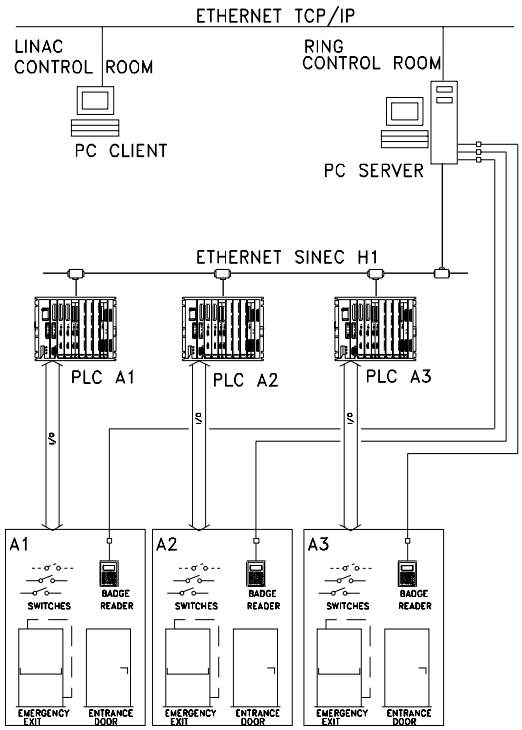

Figure 2: Hardware Architecture

There are three Siemens Simatic S5 PLCs connected to two supervisors through a dedicated Ethernet network running the SINEC H1 Siemens proprietary protocol. The badge readers (from Schlage Electronics) are connected in a redundant way to both the PLCs and, through a serial line, to the supervisors.

The supervisors are Hewlett-Packard KAYAK XAs PCs. The SR control room PC, configured as a server, is equipped with a SINEC H1 Applicom PCI 2000ETH card. The other PC, which is installed in the linac control room, is connected to the server PC by means of the main plant Ethernet network running the TCP/IP protocol.

4 SOFTWARE ARCHITECTURE

The access control system has a two level software architecture:

- the lower level is in charge of automated tasks, performed by the PLCs.
  These tasks are the acquisition of signals and interlock signals from sensors, micro-switches, etc.; transmission of commands to the actuators; automatic interlock command transmission.
- the upper level is in charge of the supervision of the various areas and of the access management. The two PCs connected in a Client/Server configuration via the main plant Ethernet network carry out these tasks.

The main guidelines followed in the choice of the PC software are:

- adoption of an Open Architecture, carried out through both 'de facto' and officially approved standards;
- availability of a modular environment for the development of applications and easy maintenance.

The Microsoft (MS) Windows NT has been eventually selected as the basic operating system and the CUBE [2] Supervisory Control And Data Acquisition (SCADA), from Orsi, as the modular development environment.

The CUBE system (fig. 3):

- is developed upon MS Windows NT and based on the MS DNA (Distributed interNet Application) architecture;
- is equipped with a native Client/Server architecture;
- is highly scalable;
- supports commercial standards, such as OLE, DDE, ODBC, OPC, IEC 1131-3;
- provides a large MS Windows NT driver library, which can be expanded to custom interfaces by the use of dedicated development tools;
- allows to install an hot back-up server;
- is characterised by a process data server made of the Real Time Data Base (RTDB), Alarm Data Base (ADB) and Process Data Base (PDB);
- has a powerful environment for the development of application modules (data processing and control logic, Application Programming Interface (API) to

integrate external applications, real-time communication drivers);
- provides special modules for designing and running synoptic interfaces (Graphic Monitoring System (GMS) module in Development (GSMD) and Runtime (GSMR) versions);
- features robust debugging tools.

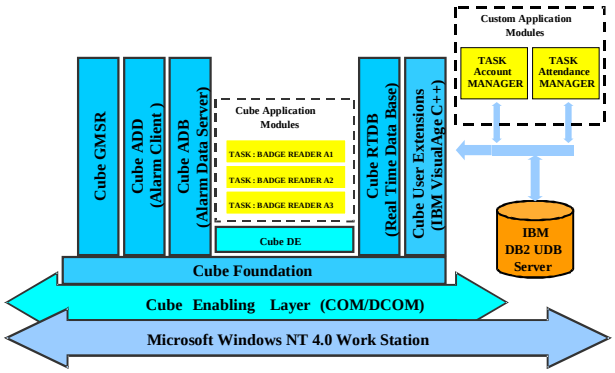

Figure 3: Server PC software architecture

4.1 Requested Features

The main features requested by the access control application are:
- synoptic functionality;
- Data Base operation (list of authorized personnel, list of people present inside the tunnel);
- control logic made of 'finite state machines' gathering data from the PLCs, the badge reader controllers and the Man-Machine Interface (MMI);
- logging of events.

4.2 Specific Problems

As far as the Data Base management is concerned, it was necessary to consider the following needs:
- the lists have to be readable and changeable by qualified personnel through permission passwords;
- any change in the lists has to be transferred to the badge reader controllers, which hold a local copy of them;
- the control logic can interrogate the lists to check access permission conditions.

The following issues had to be considered for the communication with the badge reader controllers:
- the controllers use an ASCII half-duplex protocol for the transmission of the badge read data to the PCs;
- the controllers use an XMODEM-CHECK protocol for the reception of data from the PC's.

For the reasons above, the standard CUBE driver could not be adopted, and an application external to the SCADA had to be developed. This application, while waiting for events from the serial lines, has to interface with the control logic and analyze possible changes in the Data Base to automatically update the badge reader controller lists in case of changes.

4.3 Adopted Solutions

As the Data Base is small and seldom accessed, the CUBE Track Data Base oriented module was not adopted. A dedicated solution based on the IBM DB2 Universal Data Base was chosen.

Two applications (fig. 3), called Account Manger and Attendance Manager, were written to read and edit the Data Base lists. These were developed using the Visual Builder available with the IBM Visual C++ 4.0. Both applications can be launched from the main synoptic.

The main control logic tasks for the access to the machine through the A1, A2 and A3 doors were developed taking advantage of the CUBE Data Engine (DE) environment. Each task is dedicated to one of the doors and uses the RTDB to interface with the PLCs, the MMI, the badge reader controllers, the Data Base and to log alarms.

The specific applications for the dialogue with the badge reader controllers are based on the IBM Visual Age C++. They are interfaced with the RTDB through some Orsi DLL.

5 CONCLUSIONS

A specific project has been defined at the beginning of 1999 for the upgrade of the ELETTRA access control system. The use of an off-the-shelf SCADA product has minimized project times providing an effective environment for the development of the application software. Changes in the underlying low level software running on the PLCs were negligible.

The upgraded ELETTRA access control system has been successfully tested during the last two weeks of September and will be definitively installed during the shut-down period of November.

REFERENCES

[1] G. Tromba, “The Project and Construction of the Shielding at the ELETTRA 1.5-2 GeV Synchrotron Radiation Facility – Radiation Measurements During the First Period of the Commissioning”, Proceedings of the Specialists’ Meeting on Shielding Aspects of Accelerators, Targets and Irradiation Facilities, Arlington, Texas, April 1994.

[2] ORSI Automazione S.p.A, “CUBE Overview”, document code MT249/01E, July 1999, Genova, Italy.