

EUROPEAN LABORATORY FOR PARTICLE PHYSICS
LABORATOIRE EUROPEEN POUR LA PHYSIQUE DES PARTICULES

CERN-ST-99-031
February, 1999

**A TEST BED FOR THE FUTURE ACCESS CONTROL SYSTEM:
THE AD PROJECT**

L. Scibile

Abstract

This paper describes the design, management and development of the new access control system for the Antiproton Deceleration experimental area, called the AD Project. As this project includes all the elements for the industrial evolution of the present access control system it is an ideal test bed for future access systems. The adoption of new technologies and techniques are described, and the benefits and the shortfalls are highlighted. The open redundant architecture solution, based on a PROFIBUS network and standard industrial components (HP-UNIX, Siemens S7 PLC, Siemens Industrial PC, door locks), guarantees reliability, safety and optimal integration. The project team took advantage of the Goal Directed Project Management technique and managed to define a clear and effective strategy.

Presented at the 2nd ST Workshop
Chamonix, France, February 2 - 5, 1999

1 INTRODUCTION

At CERN there are five different access control systems for the radiation areas. It is CERN's policy to unify these systems into one unique technical solution which allows customized operations [1]. These requirements imply equipment standardization, system modularity and system integration in the technical infrastructure. Moreover, compliance with strict safety regulations [e.g. *Installations Nucléaires de Base* (INB)] and industrial collaboration make quality in terms of management and organization essential. Quality also has direct benefits with respect to the optimization of resources.

In order to implement these requirements, new technologies and techniques must be adopted. New technologies allow greater flexibility, modularity and efficiency, thus maintaining, if not increasing, a high level of security. Project-based management has proved to be effective [2–3] and can be used to attain quality in terms of management and organization. The new access control system for the Antiproton Deceleration (AD) [4] experimental area, called the AD Project, implements the requirements described above and will be used as a test bed for future access systems, in particular the LHC.

The aim of this paper is to describe the design, the management and the development of the new access control system for the AD experimental area. In Section 2, the objectives/scope and the management of the AD project are presented, and the different phases of the project are illustrated based on the Goal Directed Project Management (GDPM) methodology. In

Section 3, the technical solutions are described highlighting the benefits and the shortfalls. In particular, details are given about the open system architecture, the security aspect, the fieldbus network, and the integration of the Authorization Management System (AMS) [5].

2 THE AD ACCESS CONTROL SYSTEM PROJECT

The scope of the project is to procure, configure, test and install the HW/SW components in order to attain the following objectives:

- The new AD experimental area is equipped with an access control system and a machine interlock system to ensure access to secondary beams areas in accordance with specific access modes in the absence of beam.
- The system is composed of access points which are auto-controlled, linked to a redundant central interlock system, can be remotely controlled by a supervisor, and have an on-line help computer to facilitate the access operation and enhance the potential functionality of the access points.
- The system operates fail-safe, is modular, uses industrial controllers, communicates over a local fieldbus network, and uses available LANs for external communications.
- The system can be adapted to different experimental areas by hardware configuration links.
- The system is integrated with the AMS for the distribution of database information.

2.1 Project management

The AD Access Control System was launched as a Project and managed as a Project in accordance with the Goal Directed Project Management (GDPM) methodology. It is divided

into three phases: Feasibility Study, Prototyping and Production. At each phase it is associated a ‘milestone plan’ and each milestone is broken down into activities. As an example, the milestone plan for the prototyping phase is shown in Fig. 1.

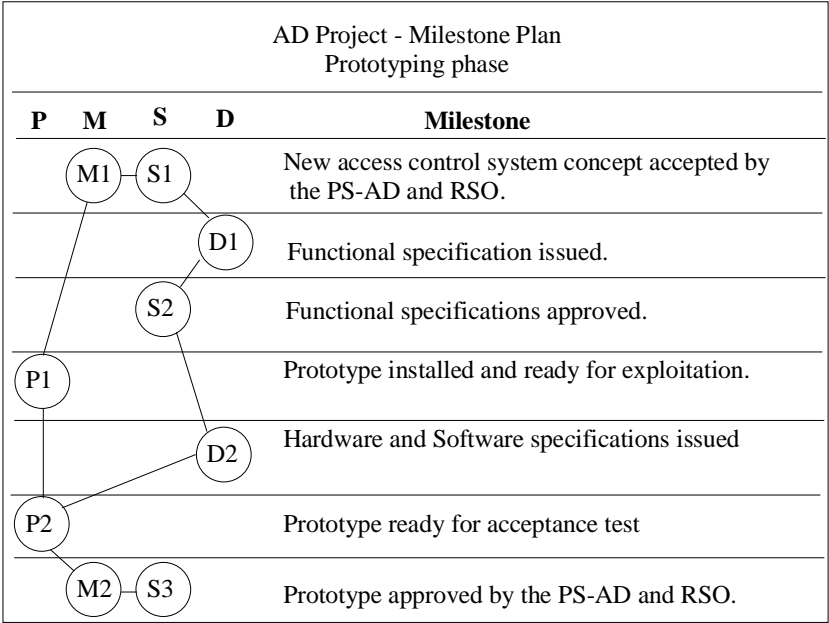


Figure. 1: AD Project – Milestone plan: Prototyping phase.

The Feasibility Study is intended as a basis for discussions during the design phase and it indicates the various options for the evolution of the project. The user requirements were identified and a summary is given in Table 1 based on the definitions and expectations of the stakeholders.

Table 1

Summary of the results of the User requirement study

Stakeholders	Expectations
Physicists	- A questionnaire was discussed with the Experiment coordinators and their expectations can be summarized in the desire for an access point that is easier to use and which provides more information.
Operators	- Supervisor Software integrated with database - Additional on-line help
Maintenance team	- Modular design - Store and database of spare parts - Minimum settings and no programming
Management	- Project completed on time and within given budget
Technical staff	- Good working conditions - Hands-on practical aspects - Application of new technologies
Project leader	- Project execution in line with the planning - Positive feedback from management - Meet the stakeholders’ expectations at the completion of the project

The Prototype phase was successfully completed on time with the approval of the AD installation. A prototype was assembled and used to test different configurations and architectures. It will be used to define and test the access procedures by the person responsible for security. The production phase is currently active. For the production phase, the team was divided into small working groups according to a list of activities; this has improved the allocation of resources and control of the execution of the project.

3 AD ACCESS CONTROL SYSTEM DESIGN: TECHNICAL SOLUTIONS

The general design concepts which fully incorporate those for future access control systems are: Standardization, Modularity and Integration.

Standardization is necessary in order to improve equipment management, to contain costs and development, and to optimize maintenance. Modularity is necessary in order to allow different configurations of the access points, to simplify installation and maintenance, to outsource single modules, and to optimize costs by using standard modules. Integration is necessary in order to share information with other systems (e.g. radiation level, beam status, etc.), to implement different modes of exploitation, and to access the AMS database.

The technical solutions for the AD access control system are a result of an accurate analysis of the present access control systems, project objectives, design concepts and the potential contribution of new technologies. Particular effort was given to the selection of appropriate HW/SW components and to the use of industrial products.

The solution is based on local a PROFIBUS network and standard industrial components (HP-UNIX, Siemens S7 PLC, Siemens Industrial PC, ELEX card reader and DORMA door locks). The system architecture was designed to make it open to both technological and structural evolution.

3.1 System architecture

The open redundant architecture solution, based on a PROFIBUS network and standard industrial components, guarantees reliability, safety and optimal integration. The system architecture is shown in Fig. 2.

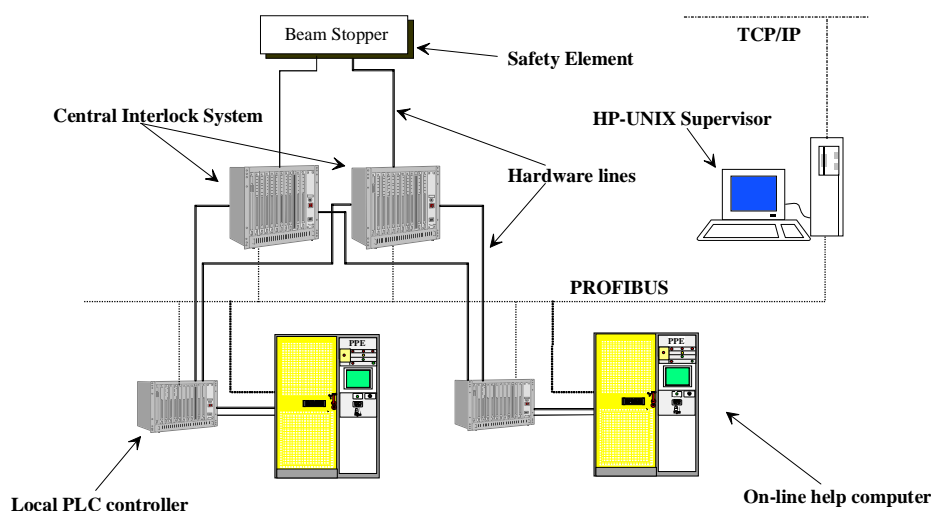


Figure. 2: AD Project – Milestone plan: Prototyping phase.

The system is composed of a local PLC controller and an on-line help computer for each access point, a central interlock system, and an HP-UNIX supervisor. The local PLC controller processes the data from the door's equipment, the on-line help computer, the central interlock system, and the HP-UNIX supervisor. An on-line help computer acts as a control panel to check/change the zone status and to manage the AMS operations. The central interlock system is a redundant system which processes the safe/unsafe conditions from the access equipment and from the safety elements (e.g. the beam stopper). The HP-UNIX supervisor has two main functions: the supervision, by means of mimics, and the communication with the external world via TCP/IP (e.g. communication with the AMS server). The safety data are transmitted on redundant hardware links whilst other data are sent over a PROFIBUS network.

The choice of a local PROFIBUS has the benefit of an open industrial deterministic fieldbus with transmission security and high transmission speed. The shortfall is that long distances can be a problem and repeaters would therefore be required in an environment as big as CERN.

Siemens S7 PLCs have been selected for the local PLC controller and the central interlock system. The new S7 series provides a very well integrated development environment with state-of-the-art configuration and debugging utilities. The PLC stations can be programmed remotely via PROFIBUS thus eliminating the need to connect the programming station directly to the PLC. There is also a powerful program for the management of the PROFIBUS network which includes diagnostic capabilities.

The on-line help computer runs a LabView application which manages the mimics, the card readers, and the AMS database. It is connected to the PROFIBUS network with an APPLICOM card and it communicates with the local PLC controller and with the HP-UNIX supervisor. The communications between the PC and the PLC use the S7 protocol. This allows direct access to the PLC memory, avoiding complicated transmission protocols.

The HP-UNIX supervisor runs a Dataviews application which manages the mimics, the communications with all the stations (PLC and PC) on the PROFIBUS network (using an APPLICOM card), and the communications with the AMS server (Ethernet network).

Each module is designed with an open interface and is configurable; it can be scaled and used in different set-ups. This involves additional costs which are balanced by the benefits of modularity and standardization.

3.2 Safety system

The study of the safety related aspects of the design of the AD access control system are based on the international standards IEC 61508 [6], [7] and on the recommendations of the '*Instances françaises des Installations Nucléaires de Base*'.

With respect to safety, this new access control system is an evolution of the existing ones [8]. The concept of a redundant system has been extended to a totally redundant central interlock system. This is obtained by having two independent PLC systems with dedicated, and not shared, hardware links and by doubling the safety relevant sensors. This configuration is primarily used to improve reliability.

With identified faults the system has been designed to be fault tolerant. This comprises the operation in degraded mode (e.g. network problems, sub-item faults, etc.). In the case of

failure the system has been designed to terminate in such a way that safe conditions for the people are guaranteed.

The modularity of the system also allows the implementation of different levels of security which can be adapted to different machines.

New technologies introduce greater hardware safety integrity thus increasing the level of security.

4 CONCLUSION

The adoption of new technologies and techniques result in an overall improvement in engineering solutions, cost reduction, management and organization and also in the optimization of resources. As this project includes all the elements for the industrial evolution of present access control systems it is an ideal test bed for future access systems, in particular the LHC.

Acknowledgements

I would like to acknowledge the support and invaluable contributions given by all members of the AD project Team. A special thanks goes to P. Ciriani for giving me the opportunity to carry out this work with the necessary resources and encouragement.

References

- [1] P. Ciriani, *Trends in industrial control systems in ST Division and at CERN*, Proceedings 1st ST Workshop, Chamonix, France, 1998.
- [2] S. Andersen, K.V. Grude, T. Haug, *Goal Directed Project Management* (Coopers & Lybrand, London second edition, 1995).
- [3] M. Vanden, P. Ninin, *Project Management as a Breakthrough at CERN*, Proc. ICALEPCS '97, Beijing, China.
- [4] S. Maury, *Design study of the Antiproton Deceleration AD*, CERN report, 1997.
- [5] U. Epting, *AMS-AC (Authorization Management System) and databases for access control*, Proc. 1st ST Workshop, Chamonix, France, 1998.
- [6] International Standards CEI/IEC 61508-4:1998.
- [7] International Standards CEI/IEC 61508-5:1998.
- [8] C. Jacot, *Politique CERN pour le contrôle d'accès à son domaine et la description de l'implantation en cours*, Proc. 1st ST Workshop, Chamonix, France, 1998.