EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH
ORGANISATION EUROPÉENE POUR LA RECHERCHE NUCLÉAIRE

CERN - ST Division

CERN-ST-2000-016
February, 2000

CERN SAFETY ALARM MONITORING PROJECT

S. Grau, P. Ninin, R. Nunes, L. Scibile, C. Soler

Abstract

The CERN Safety Alarm Monitoring (CSAM) system is the alarm transmission and supervision system for all CERN premises in the LHC era. Its objective is to help safeguard human life, property and the environment. The CSAM system consists of the acquisition, transmission, supervision and management of alarm-related data using state-of-the-art technology. It also includes some automatic safety actions to reduce hazardous events. As this is a large and multidisciplinary project a strategy based on three main issues was defined. First, the safety standards provide us with a technical framework for dealing systematically with safety-related activities in order to minimize system failures, optimize performance and obtain homogeneity with LHC site installations, maintenance and operation. Second, a rapid prototyping methodology leads to the best technical solutions; and, finally, we consider the commercial aspects required for a tendering procedure.

Presented at the 3rd ST Workshop
Chamonix, France, January 25 - 28, 2000

1 INTRODUCTION

The CSAM system gathers information generated by equipment such as fire and gas-leak detectors, emergency stops and other safety-related systems, which are located in both surface and underground areas. This information has to be transmitted as a high priority and in a diversely redundant way to the Safety Control Room (SCR) for immediate intervention by the CERN Fire Brigade (FB). Forty years of experience has demonstrated that the quality and accuracy of the information provided by the monitoring system is crucial to ensure a quick and efficient intervention by the FB. This information should be 100% reliable and 100% available. Therefore, the system must provide users with the necessary information to identify without ambiguity the nature of the problem and its exact location, 24 hours a day.

The information captured by the detectors is also sent to the Technical Control Room (TCR) and to other control rooms and systems requiring this information. In fact, the TCR has a double back-up function with respect to safety alarms: Firstly, it could be used by the FB if their SCR was not operational; and secondly, it could complement the FB's safety actions with possible technical actions. Moreover, the system has to cope with the upgrading of existing safety-alarm systems for all CERN sites to obtain homogeneity with LHC site installations, maintenance and operation.

The CSAM project is under the responsibility of the ST division. Because of the importance of this project, the two group leaders of the Alarm and Access systems (ST/AA) and the Monitoring and Operation (ST/MO) agreed to pool resources and skills to tackle this task together. Furthermore, since the CSAM development will be contracted to an external company, a large participation from the SPL division is required to deal with commercial aspects.

2 BACKGROUND

The current alarm transmission system was designed for the LEP accelerator in the late 1980s. Alarms and safety-related data are transmitted via two communication systems. One of them is a computerized system that provides the SCR with detailed information (type of alarm, location, description, etc.). It includes data handling systems, such as the Central Alarm Server (CAS) and the Technical Data Server (TDS), that manage the alarms. The computerized system is backed up by a hard-wired system permitting lower-grade operation in the event of failure of the main system.

However the current alarm system does not fulfil some of the safety requirements for the LHC project. It has limitations such as insufficiently detailed information, alarms occasionally arriving with unacceptable delays, incompletely redundant paths, and heavy procedures required to update the system. It is in this context that the need of the CSAM project arose.

3 STRATEGY

As this project is so broad, including aspects such as diversely redundant transmission paths, state-of-the-art technologies, many system interfaces, compatibility with existing systems, management of safety aspects, etc, a strategy had to be defined. This strategy focuses on three main issues: standards that summarize expertise and experience in the field of safety, a rapid prototyping methodology to find the best technical solutions, and the commercial aspects required for a tendering procedure.

3.1 Standards

We have chosen two safety standards to guide us.

- European Norm EN 50136: '*Alarm systems-Alarm transmission systems and equipment*'. This standard provides guidance on the safety requirement [2] and the acceptance test definition.
- International Standard IEC 61508: '*Functional safety electrical/electronic/programmable electronic safety-related systems*'. This standard defines a generic approach and a technical framework for dealing systematically with safety-related activities. This methodology enables us to minimize system failures, optimize performance of the CSAM and obtain homogeneity with LHC site installations, maintenance and operation.

- It is particularly interesting because it defines the skills needed to deal with safety, the required procedures to be defined and carried out, as well as the kind of development methodologies to be used.

3.2 Prototype

The purpose of the rapid prototyping strategy is to clarify the user and safety requirements of the system, to test state-of-the-art technologies, and to test integration with existing systems. The experience gained will be used to define the technical specifications for the tendering procedure. The basic prototype architecture is described in Section 4.3.

3.3 Commercial aspects

Since the CSAM system will be developed and installed by an external company, a market survey will be conducted to select firms for fulfilling the requirements of the project. A call-for-tender procedure will finally provide the name of the selected company.

The quality of the project is dependent on the quality of the technical specifications. We believe that the key to a successful implementation is to provide a precise definition of the desired system, leaving no ambiguities to the selected company. This is crucial to avoid misunderstandings and common pitfalls difficult to correct once the system is under development. Therefore, special care has been taken in collecting, analysing and defining the user requirements and standards, which will be a valuable guide in writing the technical specifications. Experience gained from the prototype will be used to define as accurately as possible the system to be developed.

4 ARCHITECTURE

4.1 CSAM functional requirements

The first step towards defining the system architecture was the identification of the system functional requirements, based on an analysis of the user requirements [2]. The result of this study is presented in the CSAM functional diagram (see Fig. 1).

Imposed by French regulations[1], two diversely **redundant transmission paths** have to be implemented to ensure a high availability of the CSAM system. One of the paths will probably be based on the existing TDS middleware. The other transmission path points to Industrial Ethernet and fieldbuses, Programmable Logic Controllers (PLCs), Supervisory Control And Data Acquisition (SCADA) systems, and web servers. This is to ensure vendor-independent solutions, as well as easy and cost-effective maintenance.

The **Safety Alarm Detection Interface** gathers information from fire and gas detection panels, emergency-stop devices, red telephones, deadman and flood detectors. The interface to this equipment for both transmission paths will be made via a highly available PLC. Among the detection equipment, one must distinguish between old and new systems (for the LHC). The first ones will be connected to the PLC via hard-wired contacts or non-standard communication protocols, most of them not providing the exact type and location of the alarm. The second ones will interface via hard-wired contacts and standard communication protocols, all providing the exact type and location of the alarms. Other non-safety data will be acquired via the **Technical Data Interface**.

Another required function of the system is to be able to trigger pre-programmed automatic **Safety Actions** to reduce hazardous events, e.g. gas leak *Alarm-of-Level-3* will trigger a signal to close the gas valve.

In order to achieve the required homogeneity and avoid data incoherence between the two transmission systems, the system requires a common **Reference Database (configuration)** for storing and configuring all information related to alarms as well as any equipment or interfaces. Furthermore, it requires a global **supervision** manager to monitor the correct functioning of both transmission paths.

---

[1] INB: Installations Nucléaires de Base.

Imposed by safety standards and French regulations, the system shall also have a common **Event Logging System** where alarm information for post-mortem and historic analysis is logged.

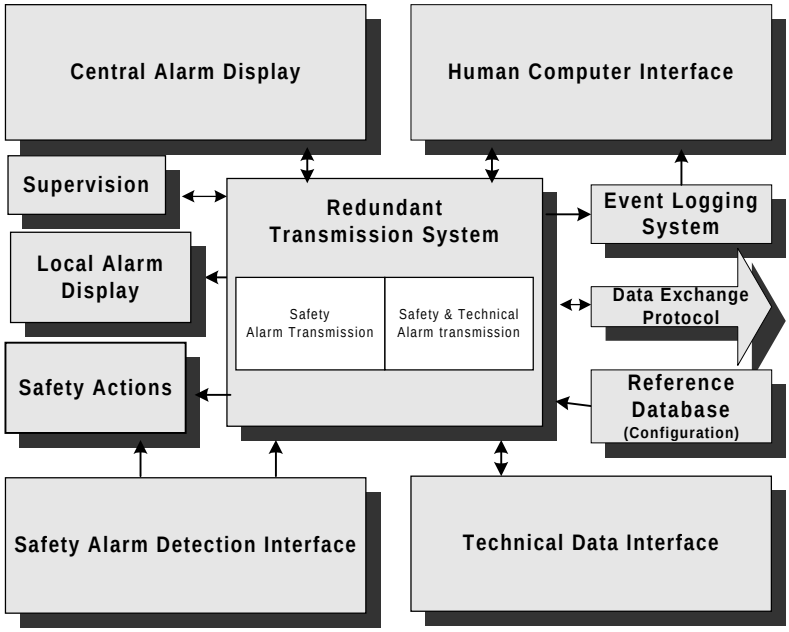

Figure 1: CSAM functional diagram.

Finally, data is exchanged with all Experiment Control Rooms through the **Data Exchange Protocol**.

4.2 LHC communication infrastructure

The LHC Communication Infrastructure working group is seeking common solutions for voice, video and data transmission. This infrastructure represents a potential solution for the CSAM system as a **redundant transmission network** (Fig. 1).

The proposed design aims at a very high level of information availability. This means 99.999% of network availability (5 min/year of downtime). The system would be based on advanced telecommunication technologies (GBEthernet) with several channels working at rates of 2 Gbit/s. As a communication media, fibre-optic cables (FO) will be used, each of them being multiplexed in different channels and wavelengths providing several dedicated transmission paths to the different users (controls, safety, etc.). An FO will be dedicated to the safety systems requiring data transmission using additional safety features (48 V supply, redundant paths, etc.).

The communication system is divided into sectors centralizing the information at a common communication centre (CC). Each sector consists of six service points and the CC, covering surface and underground areas where equipment is connected. In every sector, information travels in both directions (full duplex) so even if the FO is cut at one point, the service will be assured for the whole sector. This concept provides dynamic redundancy at the communication media level. For the CSAM project, if data were transmitted on both the control (safety & technical data transmission path) and safety (safety transmission path) networks, there would be four transmission paths.

4.3 Prototype

We are using a rapid prototyping methodology to clarify the main aspects of the system design. At the moment the prototype is in development but the basic architecture is already defined. This is described below and represented in Fig. 2:

- The interface between detection equipment and transmission systems is via a PLC. On the detection side, the PLC gathers alarms either from a detection panel or from hard-wired contacts.

On the transmission side, these PLCs have two communication cards, one for every transmission path.

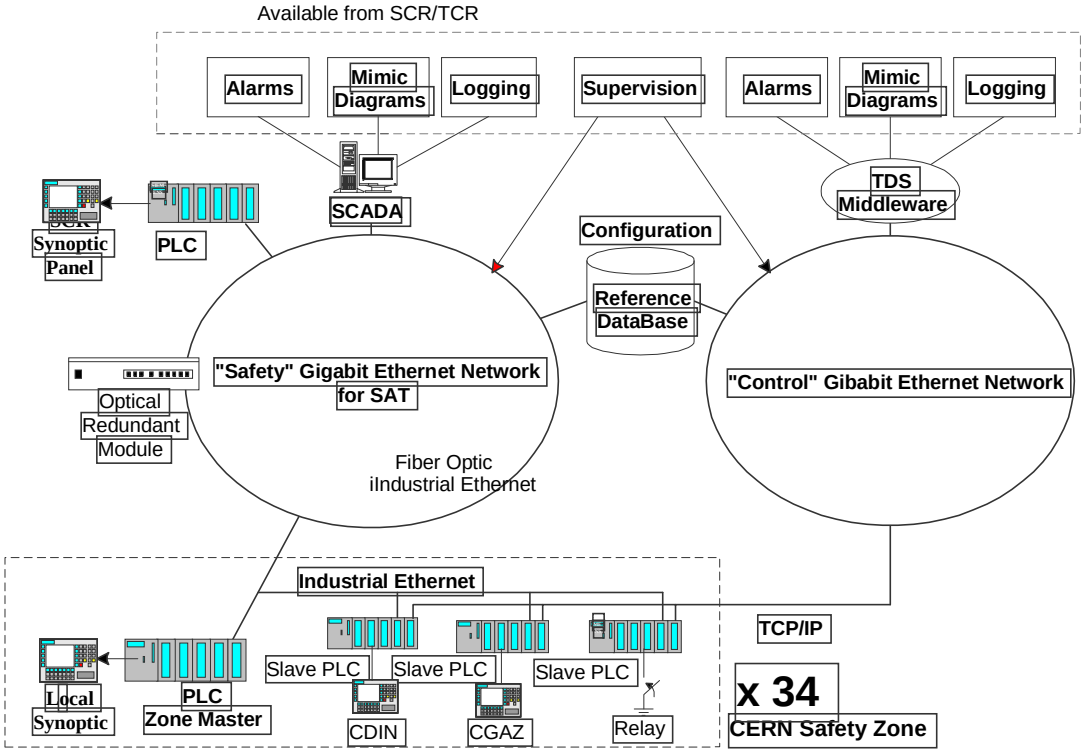

Figure 2: Prototype architecture.

- Following the division of CERN in safety zones, PLCs of the same safety zone are slaves connected to a master zone PLC that provides inputs to the local display for that zone.
- Two transmission technologies are currently being tested: Industrial Ethernet and Profibus.
- SCADA systems such as BridgeView, Panorama, and Iconics32 are being tested to collect tag information from all the master zone PLCs. They also provide input to the Human Computer Interface. In parallel with this a team member investigates the solutions proposed by the SCADA Working Group.
- Another innovative alternative to traditional SCADA systems is being tested for the mimic diagrams. It is based on new communication cards for PLCs that can act as web servers. Web pages residing in the master zone PLCs contain the mimic diagrams for the corresponding safety zone. With this system, synoptics are decentralized and accessible remotely from the network (with a simple web browser), making it easier to retrieve alarms and update mimics.

5 CURRENT STATUS

From the commercial point of view, the user requirements have been collected, analysed and specified in the user requirements document [2]. They are almost finished and ready for final approval by TIS/FB and GLIMOS. The market survey has been launched.

At the prototype, one transmission path has already been set up and configured, from the PLC at the detection interface up to the SCADA system. Different hardware and software configurations are being tested, such as the distributed web server for information of the mimic. The second transmission path is going to be integrated soon.

Regarding standards, we are defining the required training in IEC 61508, to ensure the competence of people having responsibilities in the field of safety.

However, there are some open issues to be resolved:

- The proposal from the LHC communication structure only covers the LHC machine and not the Meyrin and Prévessin sites. If an extension to these areas is not possible, an alternative solution will have to be studied.
- In this proposal a common mode of failure at the CC is possible. A special design to avoid this is foreseen, but not yet defined.
- In order to use this proposed system, it might be necessary to build an FO ring to send information from the Prévessin Control Room, where the CC is placed, to the SCR and TCR, where the main users of the CSAM are working.

6 FUTURE

The time schedule for the CSAM project is described below. The CSAM team will continue to develop the prototype: testing technical solutions, the infrastructure communication proposal and the requirements. In fact, if this proposal is accepted, the infrastructure would be ready at the end of 2002, although tests with equipment could start at the beginning of 2000.

Also, at the beginning of 2000, the CSAM team will be trained on the safety standards, focusing on functional and preliminary risk analysis. After that, the CSAM specifications will be written for the call for tender. By January 2001, the contract with the selected company should be signed and the required manpower to integrate the alarms in all zones will be available. Once the CSAM design is defined, the first installation will be used as a pilot for validation. Furthermore, the functionality of the system will require the approval of the INB.

After the installation and commissioning, the safety validation of the CSAM system will take place. We expect the system to be ready by June 2003, when the first LHC beam will be tested.

7 CONCLUSIONS

The CSAM is an ambitious and complex project that will provide CERN with a highly reliable, homogeneous and state-of-the-art safety-alarm system for the LHC era. The main challenges of the project are the constraints of integrating a wide range of old systems with new ones into the same safety concept, the reliability and availability requirements and the large area to be covered.

ACKNOWLEDGEMENTS

We would like to thank the CSAM team for their dedication to this project, competence, continuous encouragement and positive attitude towards problems.

REFERENCES

[1] H. Laeger, LHC and CERN Safety Alarm System project launch, CERN, 1999.

[2] R. Nunes, C. Soler, CSAM User Requirements Document, October 1999.

[3] P. Ciriani, L. Henny, P. Ninin, Safety Alarms at CERN, First ST Workshop, Chamonix, 1998.

[4] H. Laeger et al., Recommendations for the LHC Safety Alarm System, CERN, 1998.

[5] P. Ninin, R. Parker, Options for LHC safety alarm transmission, CERN, 1998.