EXPERIENCE USING THE FUNCTIONAL SAFETY PRINCIPLES TO DESIGN THE CERN SAFETY ALARM MONITORING SYSTEM

L. Scibile[†], R. Bartolome, A. Chouvelon, S. Grau, P. Ninin, M. Trebulle
CERN, Geneva, Switzerland

Abstract

The CERN Safety Alarm Monitoring system (CSAM) is designed to monitor the safety alarms on all CERN premises, including accelerators and experiments. The project follows the Functional Safety approach documented in the IEC 61508 standards. The functional safety is characterized by the four following criteria: availability, reliability, maintainability and safety.

The IEC 61508 standards provide a structured method for system design and safe system exploitation. It sets out a generic approach for all the safety lifecycle activities; from requirements up to the decommissioning.

The IEC 61508 considers the functional safety from different but related perspectives: technology, procedures and human interventions on the systems.

This paper gives the results of the first attempts made at CERN to use these standards in the design and realization of the CERN Safety Alarm Monitoring system. As the system will be installed and tested on site during the summer 2003, it provides a feedback on the actual advantages and disadvantages of this approach. The paper gives also some suggestions on how to improve functional safety for remote monitoring in a particle accelerator environment.

1 INTRODUCTION

Control and monitoring systems are broadly used at CERN to help to safeguard equipment, accelerators, experiments and people's life. The CERN Safety Alarm Monitoring (CSAM) 0 belongs to this category. It acquires and transmits alarms produced by safety equipment (fire detection, gas detection, emergency stops, flooding detectors, blocked lift, emergency calls and others) from surface buildings (offices or laboratories), from the underground caverns and experiments, all the CERN sites, accelerators and experiments.

The performance and level of integrity of such systems has to be maintained over many years of operation, including the changing environments and technologies, maintenance and tests periods.

In order to take into account these multiple requirements, the functional safety standard IEC 61508 0 has been used as a management guideline to structure the work on the CSAM 0. An overview of this approach and the IEC 61508 is given in Section 2.

The benefits and the pitfalls of the practical application are presented in Section 3.

2. APPLICATION OF THE IEC 61508 TO THE CSAM

2.1 CSAM description

The CSAM system acquires and transmits safety alarms to the CERN fire brigade control room to ensure a quick and efficient intervention. The system provides the firemen with the detailed information necessary to identify without ambiguity the nature of the problem and its exact location in a very peculiar environment.

The main characteristics of the system are:

- 24h/365d non-interruptible dedicated alarm monitoring system for the Fire Brigade, generation of inhibit/maintenance and test reports, human computer interface with geographical and text alarm information, exact information for efficient intervention, real-time availability monitoring,
- Flexible system architecture for the integration of the existing CERN-wide safety alarms and with the capacity for the future alarms of new accelerator and experiments with software and hardware integration capabilities,
- Modular distributed safety alarms controller based on standard industrial equipment,

The system was designed to guarantee a continuity of service 99.8% of the operational time in continuous non-interruptible mode. And this includes the maintenance interventions and other alarm operations, such as the introduction, modification and elimination of alarms.

2.2 Application of the IEC 61508

In line with the IEC 61508, the first project phases included the setup of the functional safety management 0, a detailed analysis of the system requirements and the allocation of the Safety Integrity Levels (SIL classification is given in the IEC 61508. A SIL level indicates, at the same time, a level of reliability, availability, maintainability and safety for the system under consideration and the safety lifecycle activities that guarantee that these proprieties are maintained from conception to decommissioning. A higher SIL classification (1 to 4) indicates higher safety integrity) 0.

The Management of Functional Safety was formally set-up and this implied the formalisation of the policy and the strategy for achieving functional safety. In particular, the following actions were undertaken:

- Organisation of the CSAM Project, that included all the planning activities: Quality Assurance Plan, Project Management Plan, Safety Plan, Development Plan, Configuration Management Plan, Maintenance and Operation Plan.

- Definition and training of the project team.
- Selection of measures and techniques to meet the fixed requirements.
- Definition of the functional safety assessment activities for the different project phases.

As the realisation was contracted to an industrial partner, detailed technical specifications for the tendering process were prepared. These included also the identification of a certain number of safety functions and the allocation of safety integrity level. The maximum SIL was fixed to SIL2. The levels were included as a contractual engagement on the system performance.

The safety and development lifecycle activities were setup as shown in Table 1. Review and control activities were also setup based on the Quality Assurance Plan and the Project Management Plan.

Table 1: Lifecycle activities

Activities	
Development	**Safety**
Detailed specifications	
System architecture design	Internal & external functional analysis
	Preliminary risk calculation
Sub-system architecture design	HAZard and OPeration analysis
	Failure Modes and Effects Analysis
	Software Errors and Effects Analysis
HW/SW design	Quantitative risk analysis
	Time petri nets
Final Design	

2.3 CSAM Design

The design focused on two main objectives: functional performance and safety integrity levels.

The system was decomposed in various sub-systems that were allocated the various functions. An overview of the physical architecture is given in Figure 1. The safety integrity level associated to the relative functions determined the architecture. For the functions requiring a SIL2 level, a redundant 1oo2 architecture was designed from alarm acquisition to alarm display. As the system is distributed over a large area, CERN has defined 33 safety zones that geographically identify areas for an efficient fire brigade intervention. For each safety zone, a Local Safety Alarm Controller (LSAC) was designed to guarantee the alarm acquisition and the local alarm display. All the alarms are transmitted to a Safety Alarm Monitoring Centre (SAMC) that processes and stores the alarms and acts as a server for the Human Computer Interfaces (HCI) in the fire brigade control room (SCR) and in the Technical Control Room (TCR) for backup. In parallel to the SAMC, a Central Safety Alarm Controller (CSAC) acquires and displays via a mural synoptic the presence of at least one alarm in a safety zone. The communication with external systems is done by the Safety Alarm Gateway with External Systems (SAGES) that is directly connected to the SAMC and implements the required communication protocols. The overall system is configured and managed via the CSAM Supervision and Maintenance Manages (CSMM).

The details of the different subsystems are given below:

- LSAC: for the alarm acquisition the solution is based on two redundant PLC with independent alarm acquisition and a real-time diagnostic cross check. Each PLC is connected on a different TCP/IP network and the presence of an alarm in each of them is processed 1oo2 and is transmitted via one hardwired connection to the CSAC.
- LSAC: for the local alarm display, there are two independent ways to see the presence of an alarm: a PC and a PLC text display. The PC is equipped with a touch screen that allows the interaction of the firemen in the different safety zones (there are 33 different safety zones). A SCADA client is implemented in the PC displaying the same views of the operators in the SCR. The text display is directly connected to the PLC and forms a redundant and independent way to visualise the alarms present in a safety zone.
- CSAC: this sub-system is based on a redundant PLC is connected to the two TCP/IP networks and to each LSAC with a point-to-point hardwired link. It processes the inputs and displays the 1oo3 result on two large mural panels one located in the SCR and one in the TCR. In the background, a 2oo3 result is used for diagnostic purposes.
- SAMC: this sub-system is based on a SCADA solution distributed on redundant servers and connected over redundant TCP/IP networks. It receives all the safety alarms and animates all the HCI as well as the SCADA clients in the LSAC.
- SAGES: this sub-system integrates all the functionalities for all interfaces with external systems. It also implements a standard OPC.
- CSMM: this sub-system is based on the same SCADA as the SAMC and integrates all the functionalities for the system supervision (acquisition and processing of all diagnostic data) for system configuration.

The use of a distributed SCADA allows to have the same views visible both from the safety zones and the control room. Updates are deployed without stopping the system operation.

3. BENEFITS AND PITFALLS

3.1 Benefits

The training on the IEC61508 provided a common language between the contractor and CERN, and defined a very clear objective for the contractor: achieve a SIL2 system and maintain it.

The safety activities carried out during the specification phase provide us with: a global overview of CERN risks, the part of risks covered by the CSAM system, the acceptable risk for CERN, and the existing risk barriers.

The safety analysis carried out during the system design and development guided us on the hardware and software choices to achieve the SIL 2. For example: Petri nets were used to verify the availability of the alarm transmission networks and the connectivity used, Reliability Block diagrams showed that the SAGES required a redundant fan to achieve the required SIL, and that a PC was not enough for displaying information for the Fire Brigade at the LSAC level, therefore a PC and a Text Display solution was chosen.

The safety analysis provided us with the comprehension of the CSAM operational modes (normal operation, maintenance, failure, stop) and the transitions from one another, as well as the on-line availability and transmission times calculations for the system. These calculations are used to trace the evolution of the system in time and verify that the SIL level is maintained.

The safety analysis was also used for the traceability of important decisions.

3.2 Pitfalls

Functional safety implies traceability of decisions and planning of works. This immediately leads to non-negligible amount of documentation. The ratio between documentation value vs. required work is not always satisfactory. As always, time/cost and safety are antagonist characteristics. It has been important to find always compromises between those two characteristics, to achieve the required SIL level by minimising the impact in terms of time and cost in the project.

4. CONCLUSIONS

The main benefit of applying the functional safety approach is the definition of the required framework to maintain a specified integrity level over the lifecycle of the system. It defines the skills of the people to deal with safety, the different techniques to be used for the implementation of the system and the procedures to be defined and carried out. These guidelines are very useful also for the relationship with the subcontractors because they allow for an unambiguous definition of the required system and safety performances. The application of the standard in the design has improved the understanding of the system performance as well as of its limitations. Given the novelty in the application of the IEC 61508, the required effort was underestimated and additional resources were required to minimise the delays during the design and the realisation. The testing and validation activities represented around 10% of the total team effort.

5 REFERENCES

[1] S. Grau, L. Scibile et alt., *CERN Safety Alarm monitoring Project*, 3rd WST Chamonix, 2000.

[2] IEC 61508, Part 1, General Requirements, Geneva: International Electrotechnical Commission.

[3] L.Scibile, P.Ninin, S.Grau, *Functional Safety: a Total Quality Approach*, 4st WST Chamonix, 2001.

[4] S. Grau, L. Scibile, F. Balda, A. Chouvelon, *Application of risk management for control and monitoring systems*, 4st WST Chamonix, 2001.

[5] J.-C Laprie, *Dependability: Basic Concepts and Terminology*, Springer-Verlag, 1992

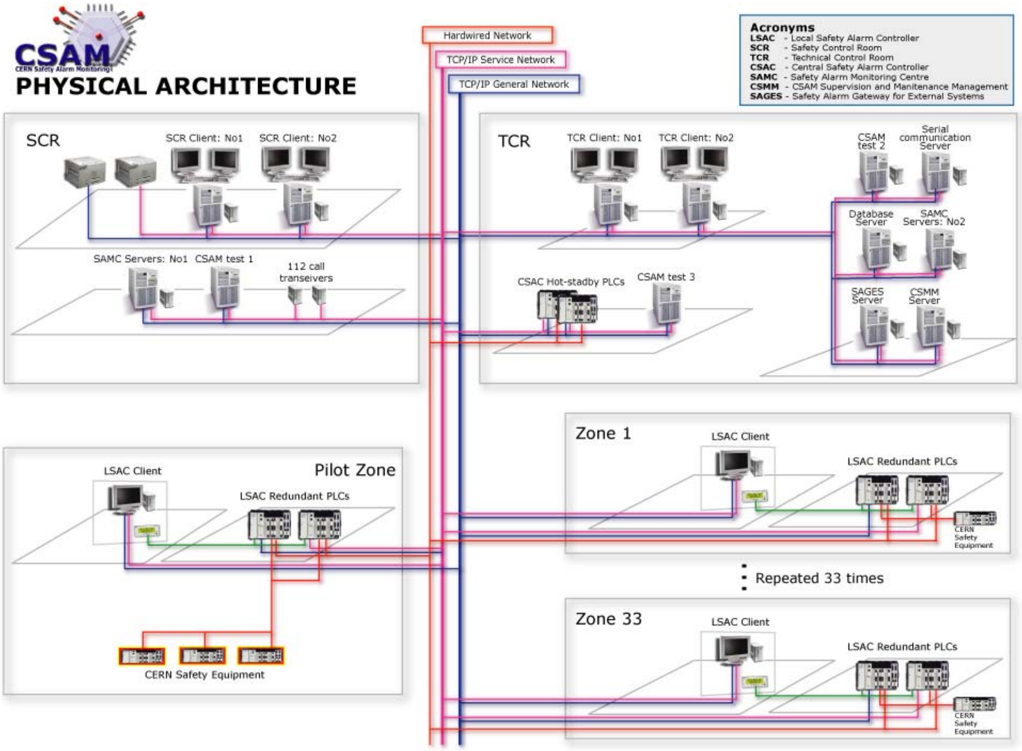

Figure 1: CSAM physical architecture