IEC 61508 EXPERIENCE FOR THE DEVELOPMENT OF THE LHC FUNCTIONAL SAFETY SYSTEMS AND FUTURE PERSPECTIVES

P. Ninin, CERN, Geneva, Switzerland

Abstract

This paper summarizes the experience gained during the development of personal protection systems of the LHC, and more particularly the feedback from the application of the IEC 61508 functional safety standards. This paper also drafts guidelines for the development of future functional safety systems at CERN. After an introduction on the legal aspects and responsibility of the various stakeholders involved in the development of a safety system, this paper will then look at the functional safety life cycle applied and experience gained in each stage of the development process. Topics covered are the preliminary risk analysis, the definition of safety functions, the probabilistic analysis of the architecture which implements the safety functions, the verification and validation process, the maintenance strategy and the validation of the system by an external regulatory authority. The applicability of the new nuclear industry safety standard IEC 61513 to such systems is discussed.

RESPONSIBILITY & REGULATION

Fundamental questions before designing a safety system are "who is responsible in the event of accident involving the loss of human life, health and environmental consequences?" and "who is responsible when the safety systems are blamed or the safety procedures are judged insufficient?"

Europe has no criminal laws for environment protection issues; the question of legal responsibility is always settled within each country's own judicial system. In France there is a three-tiered system of responsibility:

- Criminal responsibility: the industrial criminal liability of the end-user. Two levels of liability are defined; the one of the industrial legal entity and the one of the person in charge of Safety. Consequences of criminal acts can be serious: a fine, a prison term and/or site closure,
- Civil responsibility: case brought by third party victims who demand to be awarded damages,
- Administrative responsibility: obligation to declare the incident, suspension, and definite suspension of activity.

The risk assessment for a site like CERN highlights the industrial risk and nuclear risk, each of which are supervised by a dedicated independent body.

In France, regulations for industrial sites date back to 1810, but only in the 1980 did the European Union take the lead by introducing stringent regulations following the 1976 Seveso accident in Italy (SEVESO regulation). EU has also established more basic regulations for industrial site management: the Integrated Pollution Prevention and Control Directives that should be applied in each country. Nuclear facilities in France are controlled by the Nuclear Safety Authority (ASN).

However rather than discussing sanctions, methods and practice for prevention and good risk management practice should be promoted.

LHC ACCESS SYSTEM

The LHC Access system has been designed using the IEC 61508 as a methodology framework. The IEC 61508 uses the probabilistic approach to quantify the risks and to check that the architecture proposed can cope with the severity defined for each safety function. To do so, it introduces the notion of Safety Integrity Level – SIL which is a qualitative measure of the safety. It is scaled from 0 to 4; the higher the SIL, the more stringent the implementation requirements become.

In order to deal with the functional safety aspects, the project strategy focused on the following aspects:

- the preliminary risk analysis,
- the specification of the safety functions and SIL level, for example, stopping the beam in case of intrusion has been evaluated to a SIL 3,
- the preliminary safety study based on a first version of the functional analysis of the architecture,
- the design and realisation of the system based on V formed lifecycle,
- the final safety study "as-built", verifying that the stated SIL of each safety function is actually achieved,
- the verification and validation of the system,
- the organisation of the operation and maintenance.

When designing the LHC personnel protection system, it was decided to separate the access control functionalities and the safety functions into two different systems [1]: the LHC access control system (LACS), and the LHC access safety system (LASS). The latter is an interlock system ensuring that no beam can circulate or be injected in case of access during operation, and that every intrusion detection during beam operation leads to an immediate stop of the accelerator. To achieve this, the LASS system controls the state of a number of Elements Important for Safety (EIS). We distinguish between EIS-access and EIS-beam. The EIS-access consists of the personnel and material access devices (air-locks), doors dividing the underground areas into a number of sectors, ladder-traps etc. The EIS-beam has been earmarked as one of the essential LHC components and can, in parallel to the LHC beam dump system, stop the circulation. This choice of EIS-beam allows a triple redundancy for each interlock

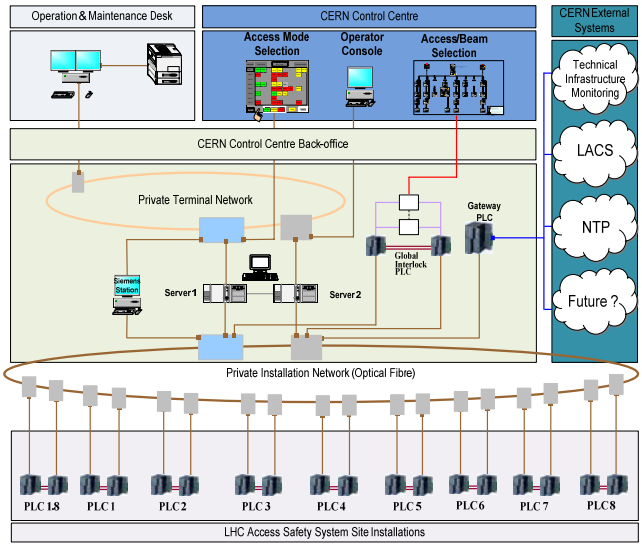

Figure 1: PLC based architecture.

both by geographical separation and by technological diversity.

As presented in Figure 1, the LASS-distributed architecture is based on the Siemens 400FH series failsafe Programmable Logic Controllers. At each of the LHC access points (8+1 in all), a local controller monitors the state of the point's all EIS and calculates the site resultant that is forwarded to the global controller. This global controller processes the information obtained from each of the nine local units and executes whatever safety actions necessary. Each local controller supervises about 150 EIS-access elements. This means mostly the monitoring of several double position contacts on each EIS. The contacts and actuators are cabled via redundant copper cables. The PLC units are linked via a self-healing fibre loop network located in the LHC tunnel. In case of a double network failure and loss of communication, each LHC point controller sets the points' EIS to a safe state, thus blocking both access and beam operation.

Experience

The scope of the system was limited to protect users from radiation hazards; nevertheless new operational needs quickly were raised, such as providing support for the specific access and safety conditions in the LHC powering test campaigns. In addition to the robust and failsafe LASS control system architecture based on SIL 3 components, the system has been reinforced by a hardwired loop to avoid a potential common mode of failure in the PLC's or an unacceptable delay in the execution of a safety function due to degradation in the system. The hardwired loop provides a technologically diversified redundant mechanism to stop the beam in case of intrusion through the external envelope of the accelerator. The final safety study of the hardware architecture which shows that the SIL 3 objective has achieved had to be completed using other strategies to guarantee the performance of the global system. Actually the safety study does not consider communication protocol, software, installation or test coverage aspects. The risk analysis, definition of the safety function, and safety study is a complex process that requires staff experienced with the use of the specific methods such as HAZOP or Bow Ties.

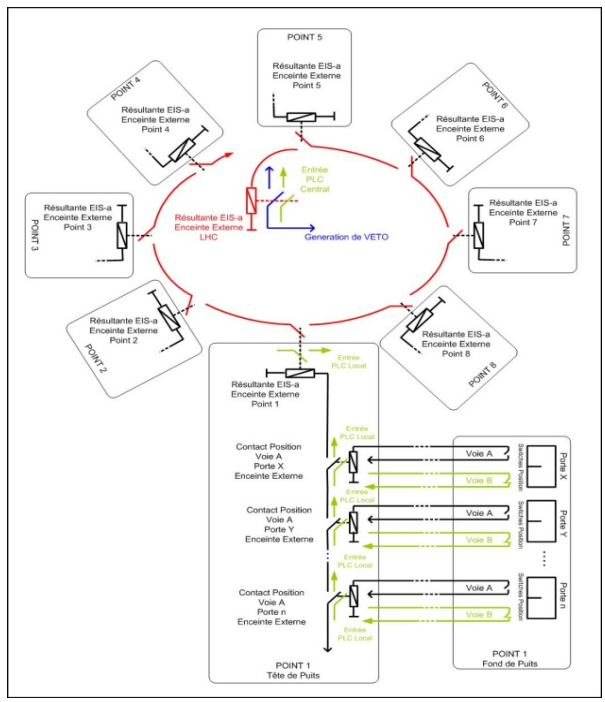

Figure 2: Hard-wired redundant loop.

A test and validation strategy had to be developed to ensure that the test coverage of the system is optimum at each stage of the project. The main testing stages were the validation on a large scale test platform, the local on-site validation, the global testing, and final validation by the CERN regulatory body [2]. The adopted strategy allowed the detection of all the software bugs or non-conformities on the test platform. The software deployed on the site was revealed to be stable and robust. The only significant problem encountered appeared when introducing an enhanced diagnostic functionality. This issue increased the data flow between each site PLC and the global controller, leading to the trigger of the safety time-out and leading to the No-Beam & No-Access fallback condition.

The preparation of detailed system and maintenance documentation for the French Nuclear Regulatory Authorities is a long-lasting quality process that suffered somewhat by a lack of guidelines. Here, the new norm IEC 61513 offers a very valuable framework. For large scale architecture like the LASS, the regulatory authorities preferred a safety demonstration based on the respect of the Common Cause of Failure – CCF, diversity, redundancy, single failure criterion rather than a demonstration based on a probabilistic approach. Other details of the experience gained in the design, testing and operation of the LHC Access system are given in the reference [3].

The environmental conditions that the system is required

to support had to be also carefully considered (eg. radiation exposure of equipment, flooding, humidity, vandalism, electromagnetic interference, seismic events, chemical influences, as well as cabling and power supply aspects). In the first year of operation, the system has been exposed to several of these factors such as the large magnetic fields of the LHC experiments or condensation due to the vicinity of the cryogenic installation.

FUTURE PERSPECTIVE

The IEC 61508 as a global standard appeared for the first time in 2000. It has been completed in four different fields of activities by specific norms:

- the IEC 61511 for the process industry (2004) [4]
- the IEC 62061 for machines,
- the IEC 61513 for the nuclear sector, [5]
- the EN50126 for train transport.

IEC 61511

The IEC 61511 describes the management of the instrumented safety functions over the full lifecycle of the project: specification, design, realisation, maintenance, modification and dismantling.

It describes the expectations of the hardware and software according to the criticality of the safety functions. The norm proposes also a methodology to realise the risks analysis and to ensure the performance of the instrumented safety functions.

Amongst all the new concepts of these methods, the principle of risk reduction with protection layers and the safety lifecycle are worth being highlighted.

The norm identifies several layers to perform risk reduction (Layer of Protection Analysis – LOPA):

- the process conception,
- the control system including diagnostic and alarm,
- the prevention; with definition of instrumented safety systems and mechanical protection,
- the attenuation of the gravity of the accident and consequences with instrumented safety systems and mechanical mitigation systems,
- the emergency procedures of the installation,
- the global emergency procedure, eg. firemen.

The IEC61511 lifecycle defines the following stages:

- the preliminary risk and danger analysis, the definition of safety functions and SIL,
- the safety functions allocated to the various protection layers,
- the safety instrumented systems specification,
- the design and the realisation of the SIS,
- the installation, commissioning, and validation,
- the operation and maintenance aspects,
- the management of the modification,
- the dismantling of the system.

Another improvement brought about by the IEC 61511 is the introduction of training and competency official certification.

IEC 61513

The IEC 61513 proposes a different lifecycle; currently the process of categorisation of safety functions is part of the power plant design (IEC 61226).

The standard does not use the SIL concept but categorises safety functions according to their severity (A, B, C) and defines a system class (1, 2, 3) that depends on the level of the safety function that it has to execute. Instead of layer of protection, it uses the notion of physical barrier.

It covers in detail specific software aspects such as configuration, management, computer security, testing, man-machine interface, and data communication.

Constraints such as cabling, EMC, internal and external hazards like flooding, ice, lightning, electromagnetic interference, earthquakes, explosions, chemical influences, etc. are also covered

In addition a quality assurance program covers aspects such as data security and integrity, modification, integration and commissioning, operation, and maintenance.

The IEC 61513 recommends the diversity of means to achieve the safety objectives and to minimise common causes of failure. This can be achieved by a strategic analysis of the extent to which the computers are used versus hard-wired systems and human actions.

The IEC 61513 provides a guideline for the audit Nuclear Authorities.

CONCLUSIONS

The engineering of personnel safety systems for particle accelerators has to deal with the industrial and nuclear risk. The IEC 61511, with its complete lifecycle and pragmatic quantification of the risks and architecture, provides a valuable framework for the safety engineer to perform his or her tasks. The IEC 61513, which is specific for instrumentation and control of nuclear power plants, gives other perspectives on design and maintenance of the system. Furthermore in France this standard now sets the regulations that are used by the authorities to audit the system, and to grant the authorisation to go into operation.

ACKNOWLEDGEMENT

To T. Ladzinski, F. Valentini, C. Delamare, S. Di Luca, S. Grau, T. Hakulinen, L. Hammouti, F. Havart, J-F Juget, R. Nunes, T. Pettersson, E. Sanchez-Corral Mena, G. Smith, F. Schmitt.

REFERENCES

[1] P. Ninin, & all “LHC Access System: From Design To Operation”, EPAC’08.
[2] F. Valentini & all, “Safety Testing for the LHC Access System”, EPAC’08.
[3] T. Ladzinski & all “The LHC Access System”, ICALEPCS 09.
[4] EN 61511 « Guide d’application de la norme ».
[5] IEC 61513 “Nuclear power plants ...”.