FUNCTIONAL SAFETY: A TOTAL QUALITY APPROACH

L. Scibile, P. Ninin, S. Grau

Abstract

Many systems used by the CERN accelerators and the technical infrastructure have to respect stringent requirements in terms of reliability, safety, availability and maintainability either for operation, security, or legal aspects such as the one required by French Regulatory Authority: the INB (*Installations Nucléaires de Base*). The functional safety approach provides a structured method for achieving these requirements. In particular, the new IEC 61508 standards give guidance for system design and an effective and safe system exploitation. When designing new systems, it also sets out a generic approach for all the safety lifecycle activities that are the base for a total quality approach: requirements, design, realization, installation, operation, maintenance and even the decommissioning. This paper gives the results of the first attempts made at the CERN Technical Service division (ST) to use these standards and gives some suggestions on how to improve functional safety in a particle accelerator environment.

1 INTRODUCTION

As computer control becomes usual for many CERN accelerators and technical infrastructure applications, it becomes apparent that the failure of these systems is likely to have an impact on the operation and/or on the safety of the people and the equipment.

The risk of a failure with its consequences has given rise to stringent requirements in terms of Reliability, Availability, Maintainability and Safety (RAMS). Moreover, CERN must also comply with the safety requirements set out by the French Regulatory Authority: the INB (*Installations Nucléaires de Base*).

To increase the RAMS performance of a particle accelerator environment is a big challenge because it involves the management of the opposite requirements of safety and flexibility. The other challenging aspect is to organize the work processes to cope with the reduction of resources, the dynamics of the new computer control technologies and the CERN outsourcing policy [1].

The functional safety standard for Electrical/Electronic/Programmable Electronics (E/E/PE) systems IEC 61508 [2] has been used as a management guideline to structure the work on safety-related control systems. An overview of this approach and the IEC 61508 is given in Section 2. A comparison with the quality standard ISO 9001 [3] is also given in Section 2.

The benefits and the pitfalls of the practical application of this approach in the Technical Sector (ST) division are presented in Section 3.

2 FUNCTIONAL SAFETY AND TOTAL QUALITY

2.1 Description of functional safety

The definition of functional safety, or dependability, has been expressed by the J.-C Laprie [4] as:

"*The notion of* functional safety *(dependability) is defined as the trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers.*"

Consistent with this definition, functional safety has a two-fold objective: guaranteeing that systems work and that they work safely. Therefore, functional safety can be seen as a method for developing a system that attains the proprieties of reliability, availability, maintainability and safety. In addition, the application of an overall safety lifecycle guarantees that these proprieties are maintained from conception to decommissioning. Functional safety is based on three major axes: people, procedures and methods. And the results of a recent study by the HSE on the causes of accidents, shown in **Figure 1**, support this strategy that people, procedures and methods are capital for the reduction of faults and accidents.

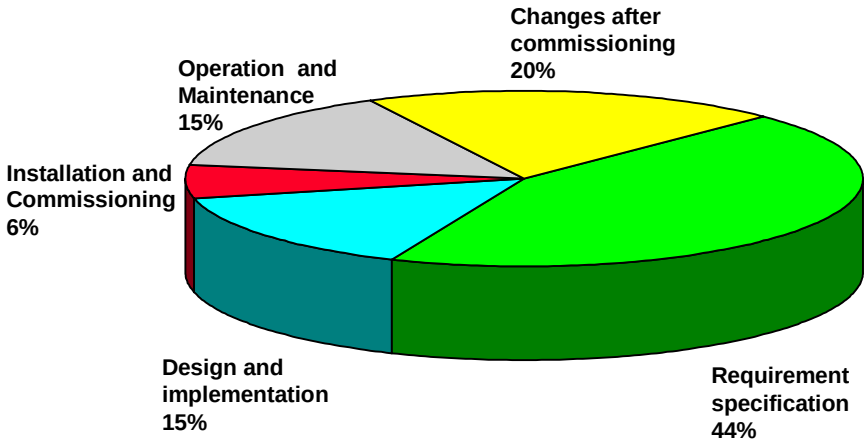

Figure 1 - HSE statistics on causes of accidents

In the field of computer controlled systems, the functional safety standard IEC 61508 defines a generic approach and a technical framework for dealing systematically with safety related activities. This methodology enables us to minimize system failures and optimize performance. 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. The standard also provides an overall safety lifecycle, shown in **Figure 2**, that focuses the attention on the safety aspects of each phase of the development process.

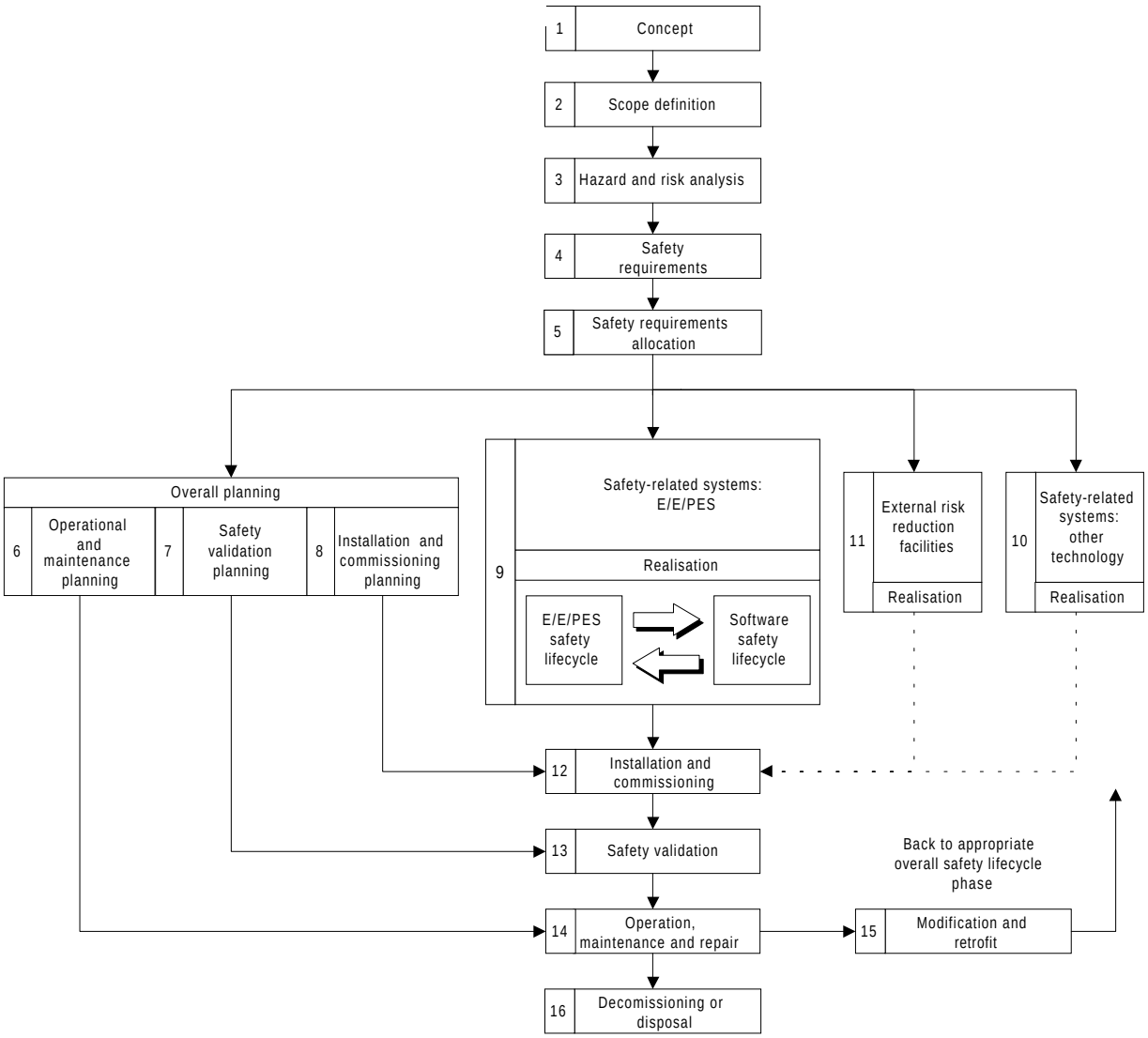

Figure 2 - IEC 61508 Overall Safety Lifecycle

2.2 Functional safety, quality and the standards

The functional safety approach addresses the issues of awareness, responsibility and commitment in the organization (or a project). In this mindset, special attention is given to the understanding and the evaluation of the real needs/expectations in terms of functional and safety requirements.

The IEC 61508 provides all the processes to build the understanding of the real needs/expectations in order to meet them. In addition, the standard explicitly addresses the issue of continuous process improvement (as found in the Capability Maturity Model developed by the Software Engineering Institute [5]). This mindset, with the processes for achieving it, is the basis for a total quality in safety-related control systems. And quality is of fundamental importance to safety because it relates to the ability of a system to meet its requirements.

In this respect, the IEC61508 has many common points in terms of quality and process management with other international standards like the ISO 9000. For example, the ISO 9000 quality system, defined as "*the organizational structure, responsibility, procedures, processes and resources for implementing quality management*", is implemented by the IEC 61508 clause which covers the management of functional safety.

Similarly, the model for quality assurance provided by the ISO 9001 which covers the conformity of a product throughout the entire development lifecycle, is implemented by the IEC 61508 clause 7 and clause 8 which provide the requirements for the overall safety lifecycle and the requirements for functional safety assessment respectively.

However, purely quality standards such as ISO 9000 typically provide little guidance on safety-related applications. According to the safety standard IEC 60601-1-4 [6], *"ISO 9000-3 alone does not provide sufficient validation confidence"*

On the other hand, in addition to providing the answer to the question "how much safety is enough?" in terms of Safety Integrity Levels (SIL), the IEC 61508 also provides a way to answering to the question "how much quality is enough?". Therefore, there is a multiple result by adopting a functional safety approach: the achievement of the required RAMS and the assignment of the sufficient effort in terms of design, realization, installation, operation and maintenance, management and quality.

3 FUNCTIONAL SAFETY IN THE ST DIVISION

3.1 Why ?

In order to face the issues of quality, project management, operation & maintenance, safety and cost optimization for the concept phase of the CERN Safety Alarm Monitoring (CSAM) [7], the ST/MO group formed a team for functional safety. After a positive experience, functional safety is being extended to other safety-related or critical control systems.

Quality: As largely explained in this paper, the issue of quality is solved by adopting the overall safety lifecycle of the IEC 61508 with the adherence to the requirements for the management of the functional safety.

Project Management: Safety-related projects must cover additional management tasks. These also include the management of the safety requirements and their allocation, functional safety assessment and functional safety audits.

Operation and Maintenance: The standards provide an organizational framework for identifying and managing the operation and maintenance of safety-related systems. These include specific procedures for reducing the risk of accidents. The application of a systematic analysis of the operational constraints during maintenance and the definition of the preventive maintenance based on the required RAMS implies a maintenance plan with an overall cost estimation.

Safety and cost optimization: The functional safety approach brings to an overall estimation and optimization of the total life costs of a safety-related system because it implies the justification of the proposed solutions against measurable required safety performance and the optimization of the operation and maintenance procedures.

3.2 How ?

People are an essential element in the organization of functional safety. Therefore, special training was organized in order to increase the knowledge of the team, to raise the awareness of the risks associated to safety-related control systems, to create a common base of knowledge and to have a feedback from industrial experts.

The training objectives have been attained and the results have been applied during the preparation of the functional and safety requirements for the CSAM technical specifications [8].

The process of knowledge acquisition/sharing has continued by actively participating to specialist conferences and seminars and by making presentations at CERN working groups and workshops.

3.3 Where ?

The functional safety approach is being applied in different areas and problems as described in the following paragraphs:

Overall projects: For the CSAM project [7], functional safety has been setup from the very beginning. The IEC 61508 has been used as a canvas for the concept phase and for structuring the system lifecycle. The standards have eased the preparation of the technical specifications and the performance requirements for the CSAM invitation to tender. In particular, it has helped in the drawn up of clear and concise performance requirements for a result oriented contract; it has also been useful for the cost estimation of the system itself and of the long term operation and maintenance services.

Re-engineering: The execution of a systematic analysis for the SPS smoke removal control system is providing an essential overall understanding of the main safety functions executed by the system. The analysis has indicated functional priority and critical elements. The first phase has provided technical recommendations to guarantee that sufficient effort is invested in these functions.

Dependability analysis: As a quality commitment to continuos improvement, a functional safety approach was used for the dependability analysis of the Technical Data Server [9]. Even in this case, the execution of a systematic analysis has uncovered potential for improvement and has also identified and quantified the weak points of the current system.

Functional safety support: To Add value to a project, a functional safety engineer must be fully involved in the design team. Functional safety support was provided for the Water 2000 monitoring project. The main contributions have been an insight to the control system risks and a set of recommendations to mitigate or eliminate them.

4 CONCLUSIONS

This paper gives the results of the first attempts made at the CERN Technical Service division (ST) to use the IEC 61508 functional safety standards. It is shown that there is a close relationship between total quality and the functional safety even though safety-related application are better covered, or complemented, by the use of specific standard like the IEC 61508. After an initial investment in training and coaching, the functional safety approach is producing the expected confidence in the concerned projects and systems. In particular, the collaborative effort for the CSAM project has produced robust specifications and the tender offers resulted perfectly in line with the estimations. The use of systematic and methodical analysis has also helped identify other system deficiencies and inefficiencies and has provided means to avoid or eliminate them.

REFERENCES

[1] G. Kowalik, *Industrial Activity at CERN*, 3rd ST workshop Chamonix, February 2000.

[2] IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronics (E/E/PE) systems, Part 1, General Requirements*, Geneva: International Electrotechnical Commission.

[3] ISO 9001: *Quality Systems – Model for quality assurance in Design/Development, Production, Installation, and Servicing*, Geneva: International Organization for Standardization, 1994.

[4] J.-C Laprie, *Dependability: Basic Concepts and Terminology*, International Federation for Information Processing WG 10.4, (Ed.) Springer-Verlag, 1992

[5] M. C. Paulk, *Comparing ISO 9001 and the Capability Maturity Model for Software*, Software Quality Journal, Vol. 2, No. 4, December 1993, pp. 245-256.

[6] IEC 60601-1-4, *Medical electrical equipment - Part 1-4: General requirements for safety - Collateral Standard: Programmable electrical medical systems*, Geneva: International Electrotechnical Commission.

[7] S. Grau, P. Ninin, R. Nunes, L. Scibile, C. Soler, *CERN Safety Alarm monitoring Project*, 3rd ST workshop Chamonix, February 2000.

[8] S. Grau, L. Scibile, F. Balda, A. Chouvelon, *Application of risk management for control and monitoring systems*, This workshop.

[9] R. Bartolome, F. Havart, L. Scibile, S. Grau, *Achieving a "SIL 1" TCR monitoring system*, This workshop.