EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH
ORGANISATION EUROPÉENNE POUR LA RECHERCHE NUCLÉAIRE

CERN - ST Division

CERN-ST-2001-036
1st February 2001

RISK ANALYSIS: AN APPROACH FOR SAFETY-RELATED PROJECTS AT CERN

F. Balda

Abstract

In recent years Risk Analysis has become increasingly important for any kind of project for both personnel and equipment safety assessments. Many divisional projects must respect the rules imposed by the French regulatory authority (INB) and the requirements of applicable international standards. This document proposes a systematic approach for the setting up of a complete Risk Analysis, and it defines coherent steps to be undertaken in order to check the achievement of the project safety goals. Several techniques are discussed, and some ST projects to which they have been applied or are going to be applied are presented. The proposed Risk Analysis structure should be associated and adapted to the different stages of the design and allows the definition of safety requirements; it furthermore traces the guidelines for qualitative and quantitative assessments.

Presented at the 4th ST Workshop
Chamonix, France, 30 January - 2 February 2001

1 INTRODUCTION

Risk Analysis is a wide and complex field, which follows the development of a system from its conceptual birth to the end of its lifetime. It includes a number of techniques aiming to the establishment of the safety-related requirements of a system and the evaluation of the risk connected to the use of such system, keeping into account interactions with external systems and the possible accidents.

All components and systems have to comply with various international standards and rules imposed by the applicable norms (ISO, ASME, IEC, etc.), and all safety-related divisional and CERN projects must respect the INB regulations. Most times, these standards do not establish a fixed path for a safety analysis, or leave to the system developers a high number of degrees of freedom for what concerns this topic.

The scope of this paper is to propose a subdivision of the phases of a Risk Analysis, and a coherent set of techniques (sufficiently flexible to be adapted to different projects) that can allow the analyzer to assess the risk related to the system under study and point out both weak points and devices for risk reduction.

1.1 Applicability at CERN: some safety-related projects

Some groups in ST Division (ST/AA, ST/MO) have recently begun to develop a Risk Analysis process associated to the project of a system. In particular, the *Access Control & Machine Interlock Systems (ACS, MIS)* for LHC and SPS, as well as the *CERN Safety Alarm and Monitoring (CSAM) System* are willing to follow a common path and test the reliability of their architecture by means of such a process. This comes also out from the common applicability of the standard IEC-61508 (built up for safety-related electrical/electronic/programmable electronic systems).

Constraints and rules imposed by INB, given the recommendations (see [1]) concerning the LEP Access Control System, will include:

- Make sure that any inhibition of a VETO signal can be rapidly pointed out;
- Show that no mechanical or electrical failure (related to elements ensuring redundancy) can inhibit the locking of an access point or actions devoted to beam destruction after an intrusion;
- Show that no mechanical or electrical failure (related to elements ensuring redundancy) can inhibit the locking of the “safety-related machine equipment” and the related actions devoted to forbid access in the case of change of the state of one of this equipment;
- Ensure physically independent pathways for the safety signals;
- Use auto-controlled PLC and signal the “imminent beam”.

1.2 Acceptability of risk

Risk is mathematically defined as:

$$R = F \cdot C \,, \tag{1}$$

where:

- F = Frequency; it represents the number of times an event takes place during a certain period and is expressed in *[no. of occurrences/time]*.
- C = Consequence; it quantifies the effects of an accident according to the different aspects to be taken into account (people, equipment, money…) and can be expressed in *[damage/occurrence]*, “damage” being a quantification of any considered loss (loss of life, injuries, loss of money, downtime…).
- R = Risk; it can represent either a *collective* risk (expressed in *[damage/time]*) or an *individual* risk (expressed in *[damage/person/time]*), depending on the kind of consequence considered.

Risk perception is heavily subject to factors very difficult to be quantified, such as politics, society features, people's perception, history of accidental events, etc.

The *tolerable risk* is the accepted risk in a given context based on the current characteristics of society; it can be estimated by means of several methods (ALARP, limit curve, etc.), and should be clearly defined before starting the project. The risk associated to one or more accidents related to any system must be kept below the fixed threshold. [2],[3],[4]

2 OUTLINE OF THE ANALYSIS PROCESS

As a general statement, it is important to stress that Risk Analysis does not have a fixed layout, but must be modeled and adapted to the particular system under study. It is convenient to sub-divide the risk analysis process in three main phases, according to the state of the project (see Annex 1 and next sections): *Concept*, *PRA* and *Reliability analysis.*

2.1 Basic rules and guidelines

A Risk Analysis should be *systematic* and *flexible* to cover all aspects related to safety, *iterative* to ensure that the risk assessment evolves in parallel with changes in architecture or projects, and *conservative* to avoid under-estimation of consequences or probabilities of an accident.

The following general safety-related features should characterize a system (electrical, electronic, network, mechanical, etc.):

- *Redundancy:* more than one path (electronic, mechanical…) should be available for the most important (or safety-related) exchanged fluxes (electrical signals, fluids/gases, protocols…);
- *Physical independence:* the most important communication ways, redundant paths (pipes, cables, networks, power supplies, etc.) or elements (racks, gas containers, etc.) should be physically located in remote places, in order to avoid or minimize common-cause failures and "domino-effects" (i.e. the propagation of an accident to adjacent elements);
- *Passivity:* whenever possible, the safety systems should act in a passive way, i.e. they play their role without the need for an intervention of other systems or the undertaking of other actions, which may be affected by their own failures;
- *Fail-safe technology:* any failure and, wherever possible, any chain of faults should result in a safe situation, avoiding the evolution of the accident in a worse scenario.

3 CONCEPT PHASE

This is perhaps the most delicate phase of the project. From how the system is basically conceived and from which functions it is demanded to satisfy, it depends a big percentage of a good result in the final product.

During this phase, the general capabilities, functions and main objectives of the system are decided and linked together. Therefore, *at this stage no quantitative estimations of the risk are possible*.

3.1 Objectives and expected results

The main objectives of this phase mostly concern the functional point of view, as a definitive architecture has not been fixed yet.

In this context, the operational modes of the system must be specified, as well as the links between the modes and the relationships with other systems. Once a functional scheme of the system is established, the safety-related functions should be pointed out, these being the zones in which highest care must be taken while designing the architecture. Finally, a list of safety requirements should complete the preliminary part of the study and prepare the path for the following phase.

An External Functional Analysis (FA) and an application of the ALARP model for Safety Integrity Level (SIL) allocation and Undesired Event prevision (see 3.2 and 3.3) has been performed for the CSAM system ([4],[5]). A similar study will be realized for the ACS-MIS systems of LHC.

3.2 Functional Analysis

The Functional Analysis (FA) allows clarifying system's functions and links with other systems. It is also useful to point out the "borders" of the system (what can be considered inside/outside, what is under its control, what is influenced…). The FA is divided into *External* and *Internal* FA, and depends on the foreseen operational modes of the system.

One of the possible methods for the *External* FA is the MISME (see [5] and [6]), which points out the connections (*main functions* or *constraints*) between the system and external elements. The *Internal* FA allows a finer system specification and helps in pointing out the *technical functions*, that is to say those describing in details the *main* functions identified in the External FA. This approach also allows the definition of interfaces and fluxes exchanged between the single parts of the system.

3.3 Safety requirements

The safety requirements should summarize the information achieved during the whole Concept Phase and establish a list of safety-related conditions the system (or its sub-parts) should respect. Their major scope is to trace limits and thresholds not to be exceeded.

It is convenient to individuate "a priori" the *Undesired Events* (UE, accidents or main degradations which may affect the system during its lifetime), estimate their consequences and therefore assess an acceptable frequency (probability of occurrence per time) so that the associated risk becomes tolerable, following the ALARP model ("As Low As Reasonably Practicable", see [3],[4],[5],[7],[8]).

Alternatively or for completeness, a similar technique can be applied to safety functions of Electrical/Electronic/Programmable Electronic systems (following the International Standard IEC – 61508). The method consists in negating the function (thus degrading the system), estimate the consequences and find out the *Safety Integrity Level* (SIL, see [4] and [7]), that is to say the failure probability per units of time or per demand, required for that function. SIL 1 indicates low-availability systems, SIL 4 refers to strongly reliable systems.

As great uncertainty affects safety considerations at this stage, very conservative assumptions must be made. In particular, when estimating the consequences of an accident related to the system, both local effects and those *on the whole process* (i.e. on LHC, the tunnel, the experiences, the personnel, the environment…) should be considered.

4 "PRA" PHASE

The Preliminary Risk Assessment (PRA) is a phase in which all of the remaining safety-related information from the *qualitative* point of view must be provided. The techniques described below require either a precise functional architecture of the system (thus a Functional Analysis, realized in the previous phase, becomes very useful), or a component-like scheme.

4.1 Objectives and expected results

The main objectives of this phase are still related to a qualitative approach, but add much more detail than what has been gained in the Concept Phase.

In particular, the hazards (or major accidents) related to deviations to process, bad working of a function, functional unit or to the failure of a component should be pointed out. These techniques allow finding out *which* are the accidents that may most likely affect the system and *where* they are probably going to be located, in such way that any weak point is immediately detected. A list of "Initiating Events" (single failures or events which, after a chain of other events, may lead to a hazard) should also be prepared. At the end, a series of safety recommendations should already be able to significantly improve the system and fix the major problems. If, after the PRA, no suitable technical architecture is envisaged, structural changes should be applied to the project from the very beginning (functional architecture), thus iterating the process.

A PRA study (probably a HazOp, see 4.2) will be performed for the ACS-MIS systems of LHC.

4.2 Techniques for preliminary assessments

HazOp (Hazard and Operability analysis) is a systematic technique aiming to analyze the system from a functional point of view. It is also possible to sub-divide the system in units (i.e. gas supply unit, ventilation, transmission…) and then apply the technique, given that the parameters exchanged between the units are known (see also 3.2). A list of so-called "key words" referring to abnormal working ("No", "Less of", "More of", "Other than", etc.) is applied to the detected parameters in order to inspect the behavior of the system. Causes and consequences, both locals, on the whole plant and on other connected systems are analyzed.

A qualitative evaluation of risk (by means of previously tables such as described in [3],[4],[5],[7] or [8]) is suggested or required, thus three columns (Frequency, Consequence and Risk) are usually added on the right of the HazOp table. The technique must be repeated for each sub-zone (if any) and for each foreseen operational mode of the system.

FMECA (Failure Mode Effects and Criticality Analysis) is based on the same conceptual idea as HazOp, but checks the system from the point of view of components, thus needing a technical architecture description. The functional units of HazOp are replaced by the single components, and the "keywords" are replaced by the failure modes of each component.

HazOp and FMECA are "single-failure" techniques, that is to say they suppose that only the considered deviation to process occurs, and do not analyze the consequences of multiple simultaneous faults, but are "systematic" as they consider all of the possible deviations from normal working. These two methods are complementary, but usually only one of them is required for a PRA. [2],[3]

5 RELIABILITY ANALYSIS

This last phase can be considered as the inner core of the whole safety process. It is during this period that the possible accidents are deeply analyzed, consequences are estimated as precisely as possible ("deterministic" analysis), and probabilities or frequencies are quantified in order to make the calculation of associated risk possible.

5.1 Objectives and expected results

The objective of this phase is to give a validation to the system from a safety point of view, thus ensuring that both all the safety functions are implemented and the risk associated to accidents is acceptable. An iterative process will allow the implementation of necessary changes and corrections.

Such work includes a quantitative estimation of the probability of the occurrence of a certain accident, or of the failure of a system. This can represent the unavailability or unreliability of such system, depending on the mathematical method used. A quantitative estimation of the frequency of a series of accidental sequences starting from a certain class of Initiating Events would also be useful (thus using the Event Trees), as well as an dynamic analysis on the possible states and transitions of the system (Markov Graphs, Petri Nets, see 5.3).

A Fault Tree – method (see 5.2) will be adopted for the ACS-MIS systems for LHC. The possibility of coupling it to Event Trees, as well as of applying a Markov graphs/Petri nets study, as well as will be investigated.

5.2 Fault Trees and Event Trees

The *Fault Trees* (FT) are probably the most known quantitative method for Risk Analysis. They are a deductive, systematic technique that allows the splitting up of a systemic event into basic, elementary events whose reliability characteristics and data are known. In this way, it becomes possible to estimate the probability of the so-called "Top Event" (TE, usually the negation of one of the system's/sub-system's functions). The technique refers to single systems and components and aims to get numerical data.

The FT makes use of logic gates (OR, AND, etc.) and the basic requisite for its validity is that the undeveloped events at which the splitting up stops must be *independent* one from the other. This is a *static* technique, that is to say does not allow the analysis of the transition between one state and another, but is also *multiple-failure*, allowing the inspection of various degraded configurations of the system. If coupled with the Event Trees, the FT can be considered as a *dynamic* technique.

The *Event Trees* (ET) are a logical technique which allows pointing out the possible accidental sequences starting from a certain Initiating Event (IE), practically describing the evolution of a single accident depending on the good working or failure of the foreseen protection systems. Before the realization of the ET, the analyzer should group the IEs into separate class, putting together those that are likely to give rise to the same accidental sequences. Given certain conditions (see [2]), to each branch of an ET a Fault Tree concerning a system or safety/redundant sub-system can be attached ("Fault Tree Linking").

At the end, quantitative results (unavailability, unreliability, expected number of failures, etc.) can be output, if some basic data are introduced (failure rates, repair rates, etc.). [2],[3],[9]

5.3 Importance analysis and other techniques

The *Importance* or *Criticality* analysis is one of the most useful methods to inspect a system and decide which zones need an improvement. The most critical components are those for which a little improvement brings great benefits on the reliability/availability of the whole system. The method basically consists in calculating an index for each component, depending on its reliability parameters, and comparing all indices. Higher values indicate a higher criticality, thus meaning where an intervention should be undertaken. [2],[3]

A number of other techniques are available for quantitative Risk Analysis. In recent years, great importance has been given to dynamic techniques (such as *Markov Graphs* and *Petri Nets*), that is to say methods capable of representing the behavior of a system as time goes by, and of simulating its transitions from a state to another. [2],[3],[9]

5.4 Software tools

A large number of software tools are available for each step of a Risk Analysis. For its simplicity and completeness, one of the most interesting is *Stars Studio 2000* (JRC Ispra, Italy). It allows the creation of taxonomies and graphics, and contains tools for HazOp, FMECA, Fault Trees and Event Trees. All of the tools contain user-friendly commands and links.

Other software tools, even more complete but generally more complicate (often containing cost estimation, Monte Carlo simulations, databases, etc.) are for example *Risk Spectrum's PSA Professional* (Sweden), *Item Software*'s various tools (UK-USA), *SOFIA* (Sofreten, France), *Aralia Workshop* and *GRIF* (Ixi, France).

The cost of a software package containing a set of Risk Analysis tools generally oscillates between 10 and 40 kEuro, with an annual maintenance cost of 15-50% of the total license cost.

6 CONCLUSIONS

A Risk Analysis approach such as the one proposed by this paper can ensure the respect of international rules and norms like INB constraints, given the degrees of freedom in choosing the most suitable method for the system under study. Given the experience in the LEP Access Control System safety assessment, and providing that enough information on the system and proper software are available, the effort necessary for a complete study of the LHC Access Control System is estimated to fall in a range in between one and two man-years.

The number of components, architectural complexity and scope of the system should turn analyzers towards a certain set of techniques in spite of others. For example, the more the system is complex, the more grouping sets of components into functional blocks will avoid (especially during the PRA) dispersive or time-wasting cataloguing work. Generally speaking, a good conceptual study or Functional Analysis, a HazOp or FMECA and a FT (if necessary, coupled with ET) technique can guarantee a reasonably good result for a Risk Analysis.

It is for this reason that the group ST/AA has chosen to organize such a process in parallel with the development of the Access Control & Machine Interlock Systems, both for LHC and SPS.

REFERENCES

[1] E. Cennini, C. Jacot – Système de contrôle d’accès et système de verrouillage des faisceaux du LEP: compte-rendu de l’étude de défaillance – Access Control Section, October 1997

[2] A. Carpignano – “Sicurezza e Analisi di Rischio: Metodologie di analisi” – Politecnico di Torino, Aprile 1997

[3] F. Balda – “Short guide to Risk Analysis” – *in course of preparation*

[4] S. Grau, L. Scibile, F. Balda, A. Chauvelon – “Application of risk management for control and monitoring systems” – 4th Chamonix Workshop, 2001

[5] CERN Safety Alarm Monitoring System – Functional and Safety Requirements Document – CERN – IT-2694/ST, August 2000

[6] “Méthode d'Inventaire Systématique des Milieux Environnants” (MISME) – NF X 50-153

[7] International Standard CEI/IEC 61508 (n. 1-7):1998

[8] Principia-EQE – “Executive summary of findings arising from preliminary risk assessment” – Report n. 296-03-R-05 - 29th September 1998

[9] T. Aven – “Reliability and risk analysis” – Elsevier Applied Science, London and New York, 1992

ANNEX 1

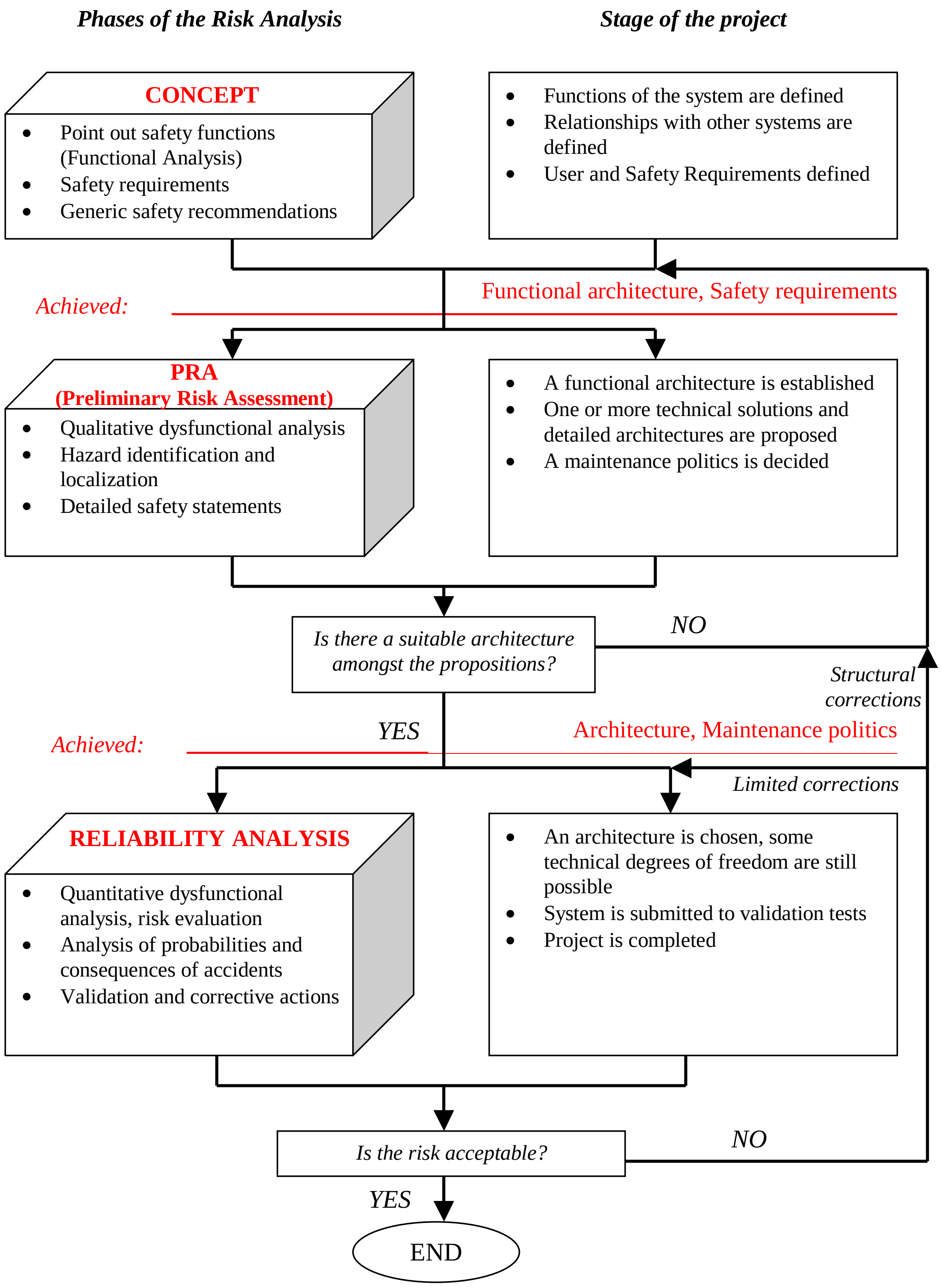
Phases of the Risk Analysis
Stage of the project
CONCEPT
Point out safety functions (Functional Analysis)
Safety requirements
Generic safety recommendations
Functions of the system are defined
Relationships with other systems are defined
User and Safety Requirements defined
Achieved:
Functional architecture, Safety requirements
PRA
(Preliminary Risk Assessment)
Qualitative dysfunctional analysis
Hazard identification and localization
Detailed safety statements
A functional architecture is established
One or more technical solutions and detailed architectures are proposed
A maintenance politics is decided
Is there a suitable architecture amongst the propositions?
NO
Structural corrections
YES
Achieved:
Architecture, Maintenance politics
Limited corrections
RELIABILITY ANALYSIS
Quantitative dysfunctional analysis, risk evaluation
Analysis of probabilities and consequences of accidents
Validation and corrective actions
An architecture is chosen, some technical degrees of freedom are still possible
System is submitted to validation tests
Project is completed
Is the risk acceptable?
NO
YES
END

Figure 1: Layout of the Risk Analysis process with respect to system development