EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH
ORGANISATION EUROPÉENNE POUR LA RECHERCHE NUCLÉAIRE

CERN - ST Division

CERN-ST-2001-044
1st February 2001

APPLICATION OF RISK MANAGEMENT FOR CONTROL AND MONITORING SYSTEMS

S. Grau, L. Scibile, F. Balda, A. Chouvelon

Abstract

This paper presents an application of the state of the art and new trends for risk management of safety-related control and monitoring systems, currently applied in the industry. These techniques not only enable to manage *safety* and *reliability* issues but they also help in the control of quality and economic factors affected by the *availability* and *maintenance* of the system. The method includes an unambiguous definition of the system in terms of functions and a systematic analysis of hazardous situations, undesired events and possible malfunctions. It also includes the identification and quantification of the risk associated to the system. The required risk reduction is specified in terms of safety integrity levels. The safety integrity level results in requirements, preventive measures, possible improvements and recommendations to assure the satisfactory management of the risk.

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

1. INTEREST OF USING RISK MANAGEMENT TECHNIQUES

Control and monitoring systems are broadly used in the ST division to help to safeguard equipment, accelerators, experiments and people's life. The performance and level of integrity of such systems shall be maintained over many years of operation, even though those systems will likely face with changing environments and technologies, maintenance and tests periods. Risk oriented approaches are well suited to assure the required level of integrity of those systems over their lifecycle.

This paper presents an application of risk oriented approaches for the specification phase of an alarm monitoring system, the *CERN Safety Alarm Monitoring (CSAM)* system. The paper describes the methodology used for this application, it analyses the obtained results, and it concludes with main benefits, required manpower and applicability of such methods.

Risk oriented approaches are currently used in the industry and summarized in different standards such as the IEC 61508 (for references on IEC61508 refer to [1], [2], [3]). These techniques not only enable to manage *safety* and *reliability* issues but they also help in the control of quality and economic factors affected by the *availability* and *maintenance* of those system.

A recent study was made to identify the principal causes of failure of control and monitoring systems. The results showed that failures are mostly caused by unclear specification of the system [2].

2. RISK MANAGEMENT APPLICATION

In view of the complexity and dimensions of the CSAM system, a very simplified version of it will be analyzed in this paper. Note that the paper does not pretend to be exhaustive, but it provides an overview of the methodology and its applicability. The detailed analysis can be found in the references.

For this application, the *system* under study is the future safety alarm transmission and supervision system. The CSAM system will help to safeguard a *process*, which in this case consist of all CERN premises in the LHC era (experiments, accelerators, etc.) [3]. Concretely, it will help to safeguard property, equipment, people's life as well as to maximise physics up time.

To achieve this objective the system shall minimise the consequences of any incident, arising at CERN premises, by informing as soon as possible the CERN Fire Brigade for an immediate intervention. Those incidents will be signalled at the Safety Control Room (SCR) by *alarms* arising mainly from: smoke (fire) detectors, flammable gas detectors signalling serious leaks, red telephones, actuation of general emergency stop, oxygen concentration detectors, water leak (flooding) detectors, actuation of local evacuation signals, blocked lift with trapped occupants and “deadman” devices.

2.1 STEP 1: Unambiguous definition of the system and its environment

The first step on risk management techniques is to define as unambiguous as possible the system under study, its environments and the service to be provided by the system to the different users [3].

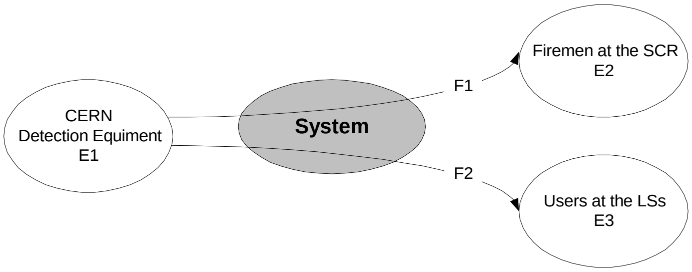


Figure 1: System, environments and functions definition

In the simplified version of the CSAM system (see Figure 1), three *environments* are identified. First, the detection equipment (E1), which generates, in case of an incident, the mentioned alarms. Second, the firemen at the SCR (E2) and third, the local users at the different Local Synoptics (LSs) (E3) distributed over the CERN, where alarms are displayed.

Those three environments delimit our system. Indeed, our system goes from the acquisition of alarms at the interface with the detection equipment, up to the alarm display at the SCR and LSs. Note that the display includes all process required to present a complete and reliable information to assure quick firemen interventions.

The *service* to be provided by system is defined by the interactions between the system and the environments. Every interaction is called *function* and it has associated a description (see Table 1) and an arrow in Figure1. For this application, the system shall provide a complete and correct display at the SCR and LSs of the alarms generated at the detection level, to assure quick firemen interventions.

Table 1
Functions definition

Function identifier	Relation between environments	Function Description
F1	E1 → E2	Display complete and correct information for each incoming alarm at the SCR to assure a quick Fire Brigade intervention
F2	E1 → E3	Display the complete and correct information for each incoming alarm at the LSs to assure a quick Fire Brigade intervention

2.2 STEP 2: Identification of what is the Tolerable Risk for this application

Next step is the identification and quantification of the risk this system shall protect. In other words the specification of the *risk reduction* this system shall provide. Many parameters need be identified for the risk reduction, being the first one the *tolerable risk* for this application.

The *risk* is generally defined as the product of *frequency* of an accident, multiplied by its *consequences*. However, risk is heavily subject to factors very difficult to be quantified, such as politics, people's perception, and society characteristics. In particular, the tolerable risk, which is the accepted risk in a given context, is based on the current values of the society [3]. It is for this reason that the safety representatives of CERN (TIS Division) were required to identify the tolerable risk for the CSAM system.

The tolerable risk assignment is made to *undesired events* (UE) determined "a priori", by means of expert judgement of the current alarm system and on the foreseen capabilities of the new one. The undesired events are events that the users of the system want to avoid. For example, the loss of alarms or the incorrect display of alarm information (see Table 6). To carry out the assignment, pre-defined ranges of frequencies, consequences and risks need to be defined (see Tables 2-3-4-5).

Table 2
Risk class

Risk class	Interpretation
I	Intolerable risk
II	Undesired risk, and tolerable only if risk reduction is impractible or if the costs are grossly disproportionate to the improvement
III	Tolerable risk if the cost of risk reduction would exceed the improvement gained
IV	Negligible risk

Table 3
Frequency categories

Category	Description	Indicative frequency level (per year)
Frequent	Events which are very likely to occur in the facility during its lifetime	>1
Probable	Events that are likely to occur in the facility during its lifetime	0.1 -1
Occasional	Events which are possible and expected to occur in the facility during its lifetime	0.01-0.1
Remote	Events which are possible but not expected to occur in the facility during its lifetime	0.001-0.01
Improbable	Events which are unlikely to occur in the facility during the lifetime	0.0001-0.001
Negligible	Events which are extremely unlikely to occur in the facility during its lifetime	<0.0001

Table 2 defines four risk classes. Table 3 defines six frequency categories of any *event* or incident. Table 4 presents the consequence categories used to classify the severity of an accident for the process. They are essentially based on two criteria: injury to personnel and damage to equipment.

Table 4
Consequence categories

Category	Injury to personnel		Damage to equipment	
	Critiria	N. fatalities	CHF loss	Downtime
Catastrophic	Events capable of resulting in multiple fatalities	>1	> 100 MCHF	> 3 months
Major	Events capable of resulting in a fatality	1	1 MCHF - 100 MCHF	1 week - 3 months
Severe	Event which may lead to serious, but not fatal, injury	0.1	10 KCHF- 1 MCHF	4 hours - 1 week
Minor	Events which may lead to minor injuries	0.01	0- 10 KCHF	< 4 hours

Finally a *Risk Matrix* can be drawn out in order to identify the risk associated with an undesired event. In this way it becomes possible to decide whether this risk is intolerable, acceptable or negligible, and if it is necessary to undertake preventive measures or not.

Table 5
Risk Matrix classification of accidents

	Consequence			
Frequency	**Catastrophic**	**Major**	**Severe**	**Minor**
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Negligible	IV	IV	IV	IV

By means of Table 4 and with the judgement of experts, the consequences for every undesired event are identified. This refers to the impact that the UE may have on the whole process the system is protecting. As seen in Table 6, the UE defined for this particular application can have ‘catastrophic’, ‘major’ or ‘severe’ consequences.

Then, the threshold for tolerable risk is determined by means of Table 5. The risk is generally acceptable if all the efforts have been done to reduce it at the minimum and if any other financial effort is disproportionate to the improvement gained. Thus the maximum allowable frequency is determined in order the risk to be classified with the index ‘II’. The meaning of such a frequency is explained in Table 3.

For example, to make the risk tolerable for a ‘catastrophic’ UE, the frequency of occurrence shall be lower than ‘remote’. However, given that it is a common use to require that the frequency is at least one or two orders of magnitude lower than the threshold, the effective *Tolerable frequency* is ‘negligible’ as indicated between brackets in Table 6.

Table 6
Undesired Events (UE)

Identifier	Description		Specification	Consequences	Tolerable Frequency [y-1]
UE-1	Partial loss of the system at the SCR (one or more alarms)	-	CSAM internal fault	Catastrophic	Remote (Negli.)
		-	Alarms inhibition	Catastrophic	Remote (Negli.)
UE-2	Alarm not in a correct form	-	Not complete	Major	Occasion. (Impro.)
		-	Confuse/Redundant	Severe	Occasion. (Impro.)

The tolerable risk is then specified when Table 6 is completed.

2.3 STEP 3: Determination of Safety Functions

Next step towards the specification of the required risk reduction is the identification of the functions actively participating to protect the process. In other words, to identify the functions which can lead to UE in case of malfunctioning. These functions are called *safety functions* to distinguish them from normal functions.

For our particular application, both functions in Table 1 shall be considered as safety functions because they can lead to the UE-1 or UE-2 in case of failure.

2.4 STEP 4: Estimation of Event Likelihood

In the determination of the required risk reduction, the *event likelihood* is an important factor. In this case the event likelihood is the probability of occurrence of any real initiating event triggering an alarm in the mentioned detection equipment. For example, the higher ‘catastrophic’ fire or gas leak likelihood we have, the more risk reduction is required to maintain a tolerable risk for the process.

To estimate this event likelihood, the event likelihood for LEP period is calculated and then extrapolated to the LHC era. Considering only fire events for this simplified application, the following event likelihood were obtained for the LEP period: 5 ‘minor’ fires/year (‘frequent’) (Example: fire in an electrical rack), 1 ‘severe’ fire/year (‘probable’) (Example: fire in a power converter or a magnet), 2 ‘major’ fires/5 years (‘probable’) (Example: fire in BA3) and no ‘catastrophic’ fires (Example: experiment burned). For the last case, the ‘remote’ frequency is considered instead.

Then, the following conservative hypothesis is made to extrapolate to the LHC era: fire event likelihood for the LHC are 10 times higher than the expected for the LEP. Therefore, for a ‘minor’ incident for example, the estimated frequency of occurrence is ‘frequent’ (50 Fires/Year).

2.5 STEP 5: Other Safety-Related Systems helping to safeguard the process

Another factor taking part in the determination of the required risk reduction is the total number of independent safety-related systems helping to safeguard our process.

For the LHC era there will be many different systems. However, not all of them are independent or protect the same risks. Some systems will help to reduce risk by reducing the frequency of initiating events. This is the case of detectors and accelerators control systems. Some systems help to reduce risk by reducing the consequence of initiating event. For example the CSAM system, the Access controls and Interlock system, extinguishers, smoke removal systems in the tunnels etc.

A detailed analysis of those systems concluded that the combination of all this system together is equivalent to have two fully independent safety-related systems performing the mentioned safety functions. In case of ‘catastrophic’ or ‘major’ incidents, a third system is also available.

2.6 STEP 6: Determination of the Required Risk Reduction for this application

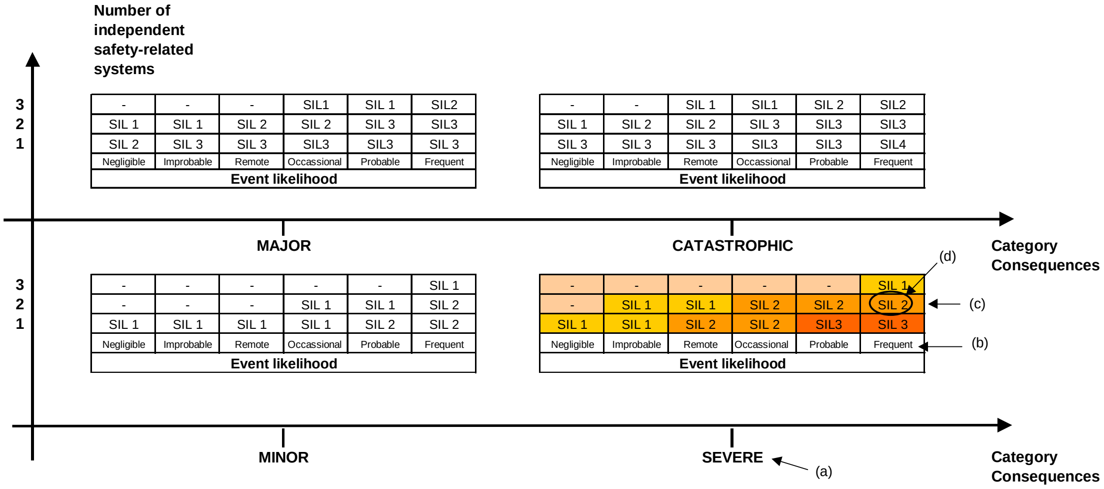
The IEC61508 proposes to determine the required risk reduction by identifying the required *Safety Integrity Levels* or SIL associated to every safety function and to the whole system (see Table 7) [3].

Table 7
Safety Integrity Levels

SIL	**Low demand mode of operation** (Average probability of failure to perform its design function on demand)	**High demand or continuous mode of operation** **(**Probability of a dangerous failure per hour)
SIL 1	10^{-1}	10^{-5}
SIL 2	10^{-2}	10^{-6}
SIL 3	10^{-3}	10^{-7}
SIL 4	10^{-4}	10^{-8}

There exist four SIL values linked to numerical *Target Failure Measure* for both low demand and high demand or continuous mode of operation systems. For a low demand system, a SIL1 means that a system with 1 chance over 10 of failure is acceptable. For a continuous mode of operation, a SIL1 means that a system with a probability of a dangerous failure per hour of 10^{-5} is acceptable.

To determine the SIL of our system, which will provide us the required risk reduction, the *Hazardous Event Severity Matrix* is used. This matrix is presented in Figure 2. The SIL is first determined for every safety function and then extended to the whole system.



MAJOR

3	-	-	-	SIL1	SIL 1	SIL2
2	SIL 1	SIL 1	SIL 2	SIL 2	SIL 3	SIL3
1	SIL 2	SIL 3	SIL 3	SIL3	SIL3	SIL 3
	Negligible	Improbable	Remote	Occassional	Probable	Frequent
	Event likelihood					

CATASTROPHIC

3	-	-	SIL 1	SIL1	SIL 2	SIL2
2	SIL 1	SIL 2	SIL 2	SIL 3	SIL3	SIL3
1	SIL 3	SIL 3	SIL 3	SIL3	SIL3	SIL4
	Negligible	Improbable	Remote	Occassional	Probable	Frequent
	Event likelihood					

MINOR

3	-	-	-	-	-	SIL 1
2	-	-	-	SIL 1	SIL 1	SIL 2
1	SIL 1	SIL 1	SIL 1	SIL 1	SIL 2	SIL 2
	Negligible	Improbable	Remote	Occassional	Probable	Frequent
	Event likelihood					

SEVERE

3	-	-	-	-	-	SIL 1
2	-	SIL 1	SIL 1	SIL 2	SIL 2	SIL 2
1	SIL 1	SIL 1	SIL 2	SIL 2	SIL3	SIL 3
	Negligible	Improbable	Remote	Occassional	Probable	Frequent
	Event likelihood					

Figure 2: CSAM Hazardous Event severity matrix

Let us consider function F1. From step 3 we know that if this function fails it can lead to a ‘severe’ UE like the loss an alarm. We are then in the bottom-right rectangular of Figure 2 (a). From step 4, we know that the event likelihood for ‘severe’ fires is ‘frequent’ (b). From step 5, we know that two different safety-related systems are available (c). Therefore, the safety function F1 shall be at least SIL 2 (d). To determine the SIL of the system the same procedure shall be applied to every safety function and to every category consequence that the UE can lead to. We would take then the more conservative SIL number. At this stage we can affirm that the system shall be at least SIL2.

The objective is then achieved. With this method, we are capable of determining the required risk reduction for our system to have a tolerable risk for the process, given a certain environment of event likelihood and other safety-related system available.

3. CONCLUSIONS

The methodology described in this paper can be used to specify any other control and monitoring systems. The same methodology is being used to guide the re-engineering of existing systems [2].

The main benefit of determining the SIL is that this value defines the required framework to maintain the specified integrity level over the lifecycle of the system: from the concept to the dismantling phase. 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 [2].

Furthermore, once the SIL is determined, the following 4 parameters are fixed as well: *Reliability*, *Availability*, *Maintenance* and *Safety*. For example, the acceptance of a SIL 1 means that the level of hazard or economic risk is sufficiently low and that a system with 10% of chance of failure (90% availability) is acceptable for low demand systems.

An order of magnitude of the effort required to perform such analysis for a system like CSAM is between 1-3 man*month.

REFERENCES

[1] F. Balda , Risk Analysis: An approach for safety-related projects, 4st WS Chamonix, 2001.

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

[3] CSAM team, *CSAM Functional and Safety Requirements*, CERN, 2000