EMERGENCY PREPAREDNESS

E. Cennini, P. Doebbeling, P. Oortman Gerlings, CERN, Geneva, Switzerland.

Abstract

On September 19th 2008, a technical fault was at the centre of a sequence of events which hampered the performance of certain equipments of the LHC 3-4 sector. The behaviour of the CERN staff confronted with the situation is the domain of emergency response. This paper outlines emergency response as one step in a bigger model of emergency management, sometimes also referred to as risk management. Just as many other management processes, the emergency management process is cyclic as well as continuous; it attempts to control and improve the status quo. It starts with identifying hazards and ends with recovery after emergencies have happened [1].

More specifically this paper focuses on incidents and accidents with the CERN research facilities. What can go wrong here? And what should be the response to the various emergency situations? The main technical, organisational framework of the CERN emergency management will be recalled, highlighting the CERN risk management and risk control strategy.

THE HUMAN OPERATOR AS INTERFACE OF THE EMERGENCY MANAGEMENT PROCESS

During the operation of CERN research facilities, the CERN staff involved in beam operation and emergency management interfaces between two processes (see Fig.1).

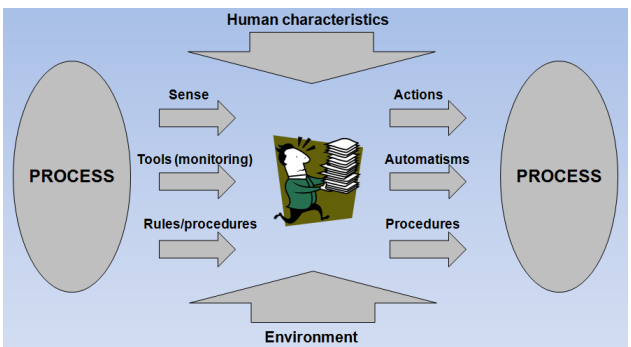

Figure 1: Layout of papers.

As interface he communicates through different means [2]:

- In reception: his 5 senses (her 6 senses?), the displays/instruments he/she reads, the procedures and instructions he/she knows or discovers.
- In emission: he/she acts, elaborates procedures and creates automatisms.

This communication takes place in a specific work environment and has typical human characteristics.

Human operator characteristics

The Human operator has some peculiar characteristics:

- He is mono-task, at least consciously.
- Unconsciously he can be multi-tasks but moving from one task to another may be difficult and disruptive.
- He needs information in order to operate and this information shall be evolving.
- When an emergency arises, he has difficulties to change from normal business to exceptional emergency handling with assessing the risk and the seriousness of the event. Therefore the information/instruction he receives during such situation, especially the initial alert information, shall be formalised, simple and clear.
- Typical errors of a Human operator are: perception errors, decoding errors, operating mode not respected (deliberately or not), missing decision in due time, and wrong sequence in the action performed.

Risks at the operator-process interfaces

The risk related to the information received from a process follows from the design of the monitoring tools and from the relevance of the displayed parameters.

Handling and decisions cannot be based on the operator experience since the occurrence of emergencies is relatively rare hence individual experience with such situation is usually small.

The risk related to the intervention/action from operators to a process depends on the quality of the relation between the actions and their expected effects and also how the different sequences of actions are managed.

Obviously correct wording (meaning) and common understanding between operators are essential assets.

EMERGENCY MANAGEMENT PROCESS

Emergency management is an eight steps process (see Table 1) i.e. it is not a once off exercise, but something that is done (more or less) continuously. It also means there are discrete steps in the process; the output of one step is the input to the next one. Being a managerial process it implies a system with feedback loops and allocation of responsibilities, which is designed, build and operated explicitly. .

Table 1: The 8 steps of the Emergency Management Process

Steps	Scope
1. Identify threats/Hazard	Generic identification of natural, technical or human caused issues that might cause the organization to fail relative to the given objectives

2. Assess risk - Probability - Consequences	Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. The identified threats and hazards become risks when they have a certain probability and measurable consequences on people or the organization
3. Analyse potential impact and define preventive measures	Preventive and protective measures influence the probability and the consequences in order to prevent losses and reduce the seriousness e.g. alarm systems, emergency stops, safety valves, periodical maintenance, fire compartments, automatic extinguish systems. The preventive measures are iterations between step 2 and 3 and reduces the residual risk at the end of the iterative evaluation process
4. Accept residual risk	In spite of control systems and preventive measures there is always a probability that things go wrong. The residual risk has to be identified, evaluated to be within the legal boundaries and to be accepted by the management
5. Organise preparedness	Emergency preparedness and incident response has to cover the residual risk. These measures have to be organized, planned and trained before the emergency occurs. Typical example are not only the preparedness of Fire Brigade and Medical Service, but also is there a high importance of the departmental emergency plans coping with the risks identified in 2,3 and 4
6. Respond to emergencies and mitigate effects	In this step an incident/emergency has occurred and the situation needs to be brought under control by emergency services. This is done with organization schemes according to the level of seriousness e.g. as described in IS 51
7. Ensure continuity	Continuity is the capability of an organization to operate under exceptional circumstances and situations in order to continue operations at an acceptable minimum level. e.g. continuity of safety systems, power supply, cooling and ventilation, access system, etc...
8. Plan recovery	Recovery is the reinstallation of normal operation conditions of the organization. A fully fledged emergency management system sets levels (finance, manpower, delivery time) within which it is expected to recover completely

Threats identification

The CERN safety policy imposes the obligation to identify risks. During the design phase of specific LHC personnel and machine protection systems, functional safety studies have been performed to steer the design process. Before the start of LHC, audits have been carried out to supervise this threat identification.

The CERN's levels of seriousness as well as the implemented Safety Alarm levels, the different kind of management and some worst cases of accident are recalled and illustrated in Fig. 2.

Risk assessment

Once the threats are identified, they have to be referenced with reasonable scenarios in order to get the possible impact of an incident/accident. This is the risk assessment process. Today standards give support on how to evaluate risks in structured ways. Sometimes there is the need to do a quantitative, in other occasions a qualitative analysis however sometimes a ranking of risks is sufficient. There is always the weighing of probability and gravity resulting in serious yet credible scenarios with the current setup. If these scenarios are deemed to have unacceptable risks, reduction measures are taken.

Impact analysis

The outcome of the risk assessment is used to design and operate the installation safely in normal situations and to prevent dangerous incidents as best as possible. However, it is also used to define the potential impact: what can still go wrong in spite of the proactive measures taken? And what is the response of the Organisation? What resources should be available? What procedures are needed for such situations? Such questions are answered in this step.

Residual risk

At the end of the iterative process of risk assessment, impact analysis and risk reduction by preventive measures there should be an evaluation of the residual risks that face the Organisation. These risks have to be compared with legal obligations and accepted by the management, potentially covered by insurances and treated in the emergency preparedness to mitigate the effects.

Residual risks that cannot be evaluated by clear limits may be treated with the ALARA concept.

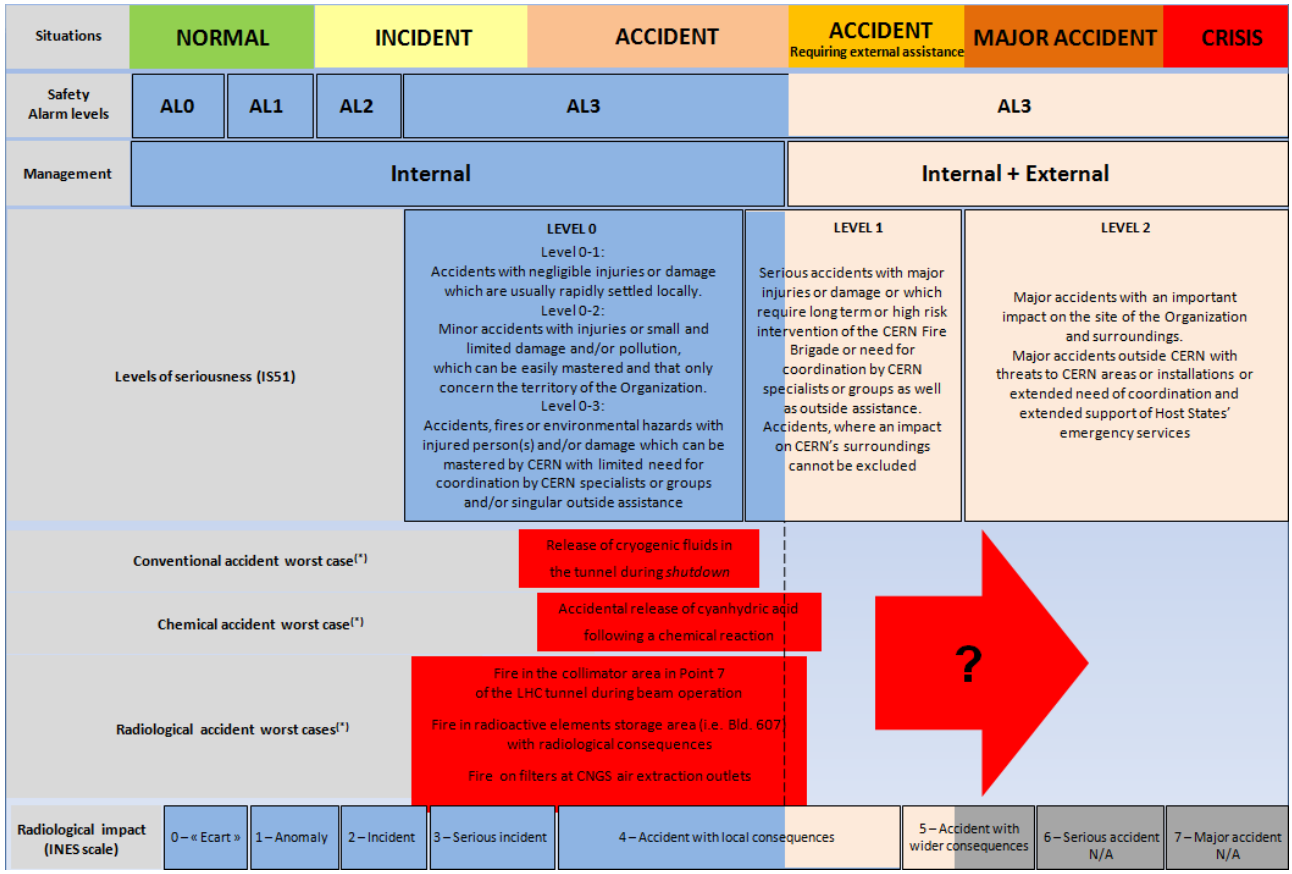

Figure 2: CERN Safety Alarms and seriousness levels' definition.

The outcome of defining the potential impact is used in two directions. Firstly, a set of things to do and secondly, considering the risks which are acceptable even if it is very sensitive. Logically it is easy to see that to avoid all negative consequences of CERN operations requires a large sum to control the risks. Socially and emotionally this is less straightforward.

Incident preparedness

In this step the question "What do we do when things go wrong?" is answered.

The incident preparedness includes emergency planning with defining and implementation an overall CERN emergency organisation in accordance with the emergency organisation of the host states, defining internal roles and responsibilities of CERN Departments, Experiments and Groups, developing emergency procedures and instructions of internal emergency services, provide sufficient and effective equipment for emergency services. Also coordinated reaction plans of the different control rooms and cooperation agreements with the host states and private contractors for emergency support and media information procedures are part of the preparedness. A recommended Safety documentation structure is illustrated in Fig. 3.

Good incident preparedness uses lessons learnt from former incidents, accidents and near misses. Training, full exercises and table top exercises are mandatory.

Emergency response and mitigation

The objective is to combat the emergency and bring the situation under control as fast and as best as possible. This should not only include the physical dangers, but also the information about what happened. (What and how to tell relatives of victims, neighbouring citizens and the press?).

Continuity

Continuity has the objective to ensure the best continuity of business, to maintain operations and services and to fulfil the key deliverables and obligations during and after an emergency has stopped the normal work. How can the organisation operate and survive if major parts of its assets are not operational is the main question. The crisis management organisation should define those parts of the Organisation's business that may be stooped for some time and those to which priorities for continuity are given e.g. priorities for power supply, cryogenics, civil engineering, personnel, experts, finance. Continuity should identify equipment, supplies, and supply chain interactions that support the critical activities. Strategies to secure operation of safety systems, maintenance and research facilities should be implemented.

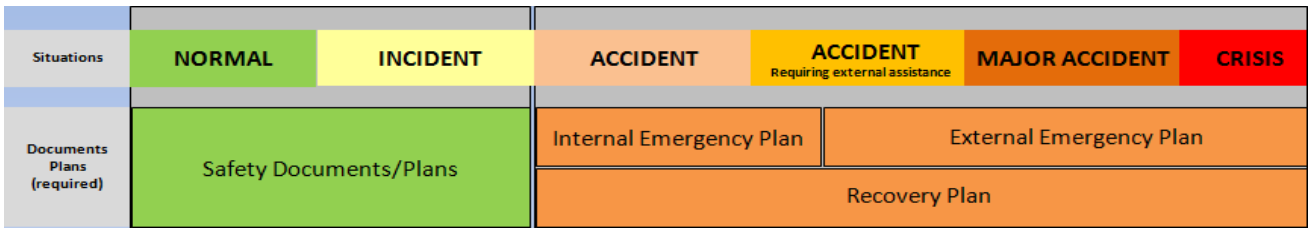

Figure 3: Recommended Safety Documentation Structure.

Recovery

After an incident with operational interruption or disruptions, the normal situation must be re-established. A recovery plan based on the risk and impact analysis as well as the residual risk should define a general estimation about the time table for restoration of operation according to the identified main risks, identify installations and operations that cannot potentially be restored with reasonable delay and total or partial suspension of operations not urgently needed.

Recovery needs also pre-emptive decisions on keeping on stock a minimum number of critical spare parts. Additional technical and human resources required from outside by co-operation agreements with partners to contribute to the recovery and procedures for financial consideration (insurances, stakeholders) and pre-emptive planning based on lessons learned should be prepared.

APPLYING THE MODEL TO POST 19 SEPTEMBER 2008 CERN

Identification of threats

Threats identification related to damage to equipment and further worst case scenarios shall be investigated and shall update the respective lists.

Are there threats that are new compared to the former threat identification?

Assessment of risks

Several risk assessment reports have to be updated (RPS 1.7, Safety Design Criteria, Interfaces between systems have to be eventually refined, defined and tested). Moreover, the integration of the various systems into an overall risk assessment is missing. Also the risk assessments of other facilities have to be reviewed in view of the findings of similar (in consequences) incident especially the systems and equipment belonging to the accelerator chain carrying and preparing the LHC beams.

The processes of elaborating systematically Safety Files for new facilities and continuously updating the existing ones from the lessons learned from incident accidents (requiring an incident and accident logging/analysis tool) are compulsory.

Define potential impact/consequences

As bad as the incident was, it did not exceed the worst case scenarios. The various alarm systems (about a dozen) worked as designed. And - because nobody was nearby in the tunnel, there was no threat to life. However, there is a clear lesson to define a policy on reliability, availability, maintainability and safety of these safety systems in order to have them working when needed in the future and fine tune the risk assessment.

The lessons learned from the incident will help to improve the knowledge and therefore the procedures related to the use of protective/preventive means on the following aspects:

- The mechanical risk/hazard.
- The rapid reduction of Oxygen within few minutes in the whole sector.
- The intervention organisation.
- The stabilisation work under critical safety conditions.

Organise preparedness

Preparedness can be organised through the following aspects:

- Level 2 Alarms monitoring and follow up
- Near misses analysis
- Procedures/instructions in case of incident/accident
- Education and training of all players (Management, departments, control rooms, emergency services)
- Full exercises as well as table top exercises
- Appropriate Equipment for intervention and Command & Control.

The emergency preparedness documentation shall foresee the following (obvious) characteristics:

- In line with the rules and regulations in force.
- Clear responsibilities.
- Available where needed.
- Adapted to the circumstances (from normal situation up to crisis situation).
- Simple wording.
- Use of pictograms instead of sentences.
- Managed through a Documentation Management System.
- Harmonised templates
- Grows in effectiveness and efficiency by real life experience and exercises

Emergency response

The main steps of the CERN emergency warning outline are illustrated in Fig. 4.

The handling of the incident went smoothly thanks to the alertness and competence of the operators.

The emergency planning and the intervention concept of the fire brigade has worked well but can be improved furthermore with the lessons learnt from the incident.

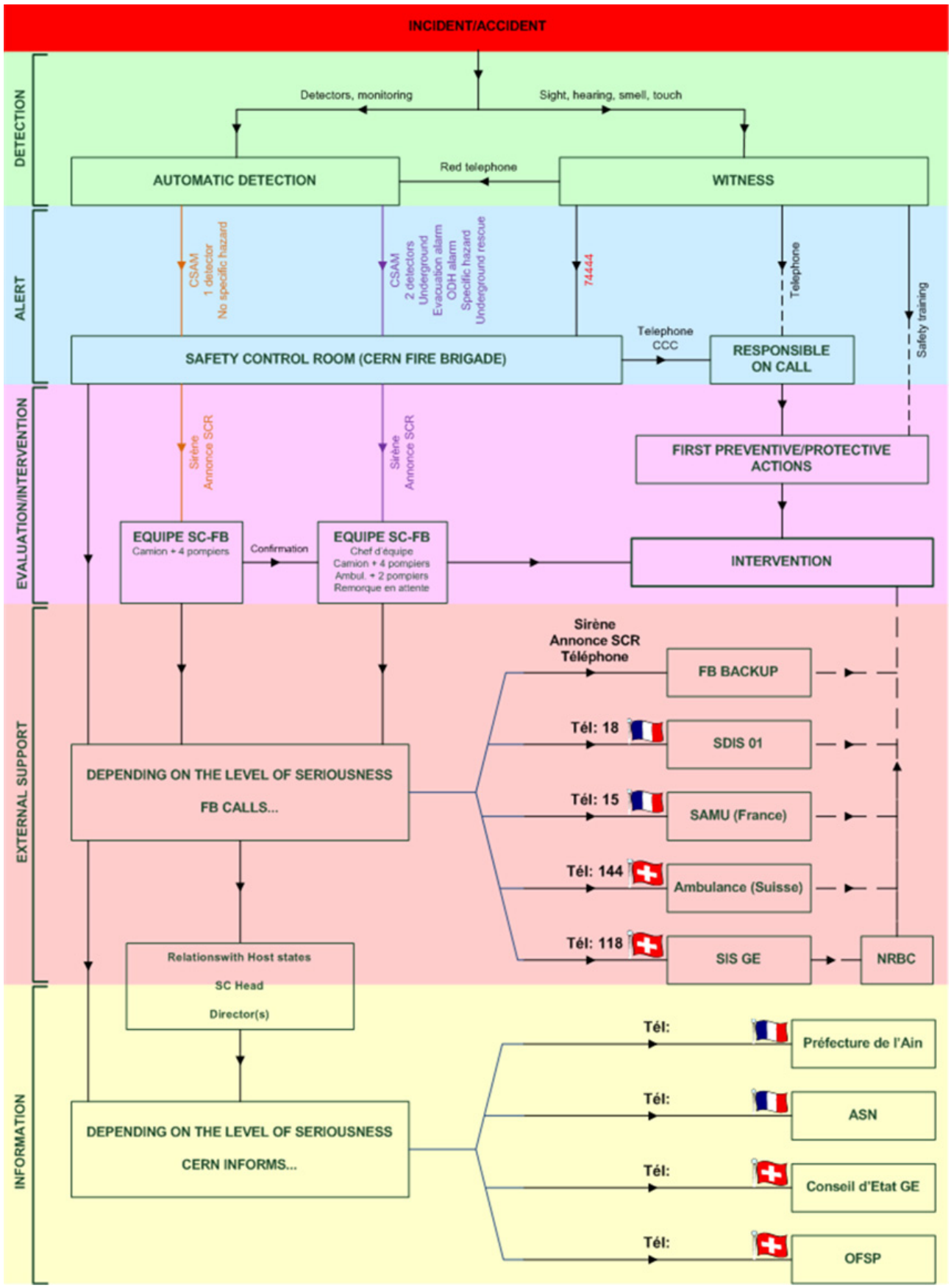

Figure 4: CERN emergency warning outline.

However, there was no clear crisis organisation set up and a need for better coordination between the various parties (control room operators, people in the field, emergency services, communication to various stakeholders, tasks and roles of Management) was identified. The roles and responsibilities have to be defined, clarified and implemented through exercises and instructions. Then everybody knows what he is (not) supposed to do in case of a future incident. The documentation must be made available (on paper or electronically) to the right people and kept up to date.

Continuity and recovery

The impact of the 19 September incident is sufficiently known. But are we prepared for continuity and recovery of other serious incidents? For example the (partial) losses of a ventilation system or electricity supply? How will it affect operations and research programs? How can these impacts be minimized? Which risks can be insured? What threatens the long-run continuity of the Organisation? Clearly there is here large room for improvement.

CONCLUDING REMARKS

The 19 September incident has shown –despite all damage- also a positive side. No one was injured and the safety risks after the incidents have been managed professionally and in a short time. The return of experience enabled us to identify and remedy weak points.

A systematic comparison of the event and a simple model has given us two benefits. First, it will make recurrence of disastrous events less likely. Secondly it enabled us to be better prepared for such events and thus reduce their impact effectively.

The overall CERN Safety documentation recalled in Fig. 3 needs to be urgently updated, revised and implemented with procedures, training and exercises.

REFERENCES

[1] ISO31000.

[2] Y. Metayer, L. Hirsch, “Premiers pas dans le management des risques”, AFNOR, 2007.