Journal of Hazardous Materials 181 (2010) 324–334

Contents lists available at ScienceDirect

Journal of Hazardous Materials

journal homepage: www.elsevier.com/locate/jhazmat

Industrial emergency planning modeling: A first step toward a robustness analysis tool

Georgios-Marios Karagiannis[a,*], Eric Piatyszek[a], Jean-Marie Flaus[b]

[a] Ecole Nationale Supérieure des Mines de Saint-Etienne, 158, cours Fauriel 42023 Saint-Etienne cedex 02, France
[b] Institut National Polytechnique de Grenoble, 46, avenue Felix Viallet 38031 Grenoble cedex 1, France

ARTICLE INFO

Article history:
Received 27 January 2010
Received in revised form 30 April 2010
Accepted 4 May 2010
Available online 11 May 2010

Keywords:
Industrial emergency plan
Robustness
Lessons learned
Model-based risk analysis
Risk assessment

ABSTRACT

The purpose of this paper is to present a model-based approach to the analysis of the robustness of industrial emergency plans, established by the European Union SEVESO II Directive. Robustness is defined in terms of the capacity of the mechanism to respond to deteriorated conditions. Analysis of emergency plans has been so far based mainly upon lessons learned from past major accidents or exercises, which do not allow for an integral analysis of the response mechanism. The proposed methodology is based upon a systemic, hierarchical and generic model of an internal or external industrial emergency plan, using the FIS modeling approach. The process generally found within an industrial emergency plan is identified through the model. Potential failures are estimated through an *a priori* analysis of the plan model and an *a posteriori* analysis of lessons learned from exercises and past accidents. Assessment of the plan's functions is carried out via assessment checklists, structured via the systemic model for each of the plan's process. This approach can hence be used as a toolbox both for the assessment of existing plans and the development of industrial emergency plans.

1. Introduction

The European Union 96/82/CE Directive, also known as the "Seveso II" Directive, sets the framework for emergency management of industrial accidents involving hazardous substances in the European Union Member States. It defines two risk levels for industrial establishments, depending on the quantity and nature of hazardous substances present in the establishment. The Directive then imposes a number of measures to Member States and industrial facility operators aimed at preventing, mitigating and preparing for industrial accidents, including, but not limited to, development of safety management systems, internal and external emergency plans, land-use planning, information of the public, accident reporting, and safety inspections.

The operator of an industrial facility falling into the scope of Article 9 of the Seveso II Directive is required to prepare an internal emergency plan, which describes the measures to be taken inside the establishment in case of a major industrial accident. The respective public authorities are required to prepare an external emergency plan, which describes the action taken outside the establishment. The objectives of both internal and external emergency plans include containing the incident, protecting people, property and the environment, communicating the necessary information to the public and public authorities, and providing for the restoration of the environment after the accident. Under the Seveso II Directive, European Union Member States (and hence industrial facility operators) are required to put in place without delay the emergency plans if a major industrial accident occurs or is reasonably expected to occur.

The objective of this paper is to present a model-based approach to industrial emergency plan robustness analysis. Indeed, emergency plans can suffer a number of dysfunctions, including, but not limited to, absence of critical personnel or failures of technical equipment. The approach is based on an *a priori* identification of these failures using a functional model of the emergency response mechanism established by the plan. This analysis is subsequently confirmed and/or modified through information obtained by lessons learned from past industrial major accidents. The knowledge produced as a result from these combined tasks is then capitalized upon and organized through the creation of assessment checklists derived from the identified potential failures. These checklists are then used to analyze the mechanism's operation under deteriorated circumstances. This analysis can have a twofold utility. First, it may be used during the design stage of an industrial emergency plan, to facilitate planning by highlighting failures that can potentially occur at the emergency response phase (that is, during the application of the plan). Second, this structured

* Corresponding author. Tel.: +33 04 77 42 66 67; fax: +33477426633.
E-mail addresses: karagiannis@emse.fr (G.-M. Karagiannis), piatyszek@emse.fr (E. Piatyszek), jean-marie.flaus@inpg.fr (J.-M. Flaus).

0304-3894/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2010.05.014

analysis can be used for the assessment of existing plans, by identifying potential pitfalls in the emergency response mechanism.

This paper is organized as follows: Section 2 outlines the proposed methodology for iterative modeling of industrial emergency plans. This section includes an attempt to define robustness in terms of industrial emergency planning, the concept of model-based risk analysis applied to industrial emergency plans, the basic ideas of experience feedback on industrial emergency plans by structuro-functional models of these plans, and finally a description of the method proposed. The results of the application of this methodology to Internal Emergency Plans are given as an example on Section 3 of this paper. An overview of the Internal Emergency Plan model created using the FIS approach, a report of the experience feedback supporting this research and an example of an audit checklist are presented in this section. Finally, conclusions drawn and possible perspectives are presented in Section 4.

2. Methodology for iterative modeling of industrial emergency plans and their failures

2.1. Robustness of industrial emergency plans

There is not a globally agreed definition of robustness, and the apprehension of this term is further complicated by its relationship to resilience and stability. *Robustness is intuitively defined as the capacity of a system to adapt its behavior to unforeseen situations, such as a perturbation in the environment, or to internal dysfunctions in the organization of the system* [1]. However, this definition does not clearly differentiate between the notions of robustness or resilience. According to Harding et al. [2], r*esilience represents the capacity of a physical or biological environment, a society, an organization or a person to go through a stressful experience, while minimizing its impact or utilizing the adversity to improve their development organization*.

Furthermore, in the context of emergency and crisis management, Wybo [3] defines resilience as the ability of the organization (at any level) to keep achieving its tasks by adapting its functioning to hazardous situations, uncertainty, time pressure and threats. Robustness is defined as the ability of the organization to survive and stay under control by the emergence of new organizational patterns.

With regard to an industrial accident response mechanism, such as the ones established through internal and external industrial emergency plans under the Seveso II Directive, robustness can be defined in terms of the capacity of the emergency response system (or mechanism) to maintain an effective level of operational response to the emergency (that is, to survive and remain under control of the emergency situation) when the condition of the elements of the system becomes deteriorated or under unforeseen situations. Such circumstances may arise for example as a result of failures of technical resources necessary to response operations, lack of competence of response personnel, or problems inherent in the emergency procedures themselves. As an example, robustness may include the capacity to ensure all communications-related functions of an internal emergency plan in the absence of part of the communications personnel in the command post or while a part of the emergency contacts reference is not accessible. In other terms, one can define robustness of industrial emergency plans as the efficiency of the industrial emergency response system or its ability to perform according to plan and fulfill the result based requirements defined in the plan under deteriorated circumstances or unforeseen situations.

For the purposes of this study, we have centered our focus on the first component of robustness (deteriorated circumstances). Thus, in order to analyze the robustness of an emergency plan in terms of the expected results, we have chosen a model-based approach: first we identify the main functions of the plan and the associated resources. Then we use this model to identify the possible failures and to structure the experience feedback. This approach allows an analysis of the critical points of the plan and is presented in the following section.

2.2. Model-based risk analysis

An *a priori* analysis of emergency plans may help identify failures that can potentially occur within an industrial accident response mechanism. In this study, this *a priori* analysis is performed using a structuro-functional model of a typical emergency plan.

Industrial emergency plans are often outlined by flow diagrams, which serve the purpose of facilitating the plan's comprehension [4]. While this representation is quite didactical and illustrates the sequence of the plan's main functions, it does not prominently display the operational aspects of the mechanism established through the plan, the resources used to perform each function, or the interactions among these functions and resources. On the other side, a functional model of the industrial emergency plan can illustrate the relationship between the various functions in the form of interactions between them, but also the assignment of resources to functions (i.e. what is needed to perform each action). Thus, a structuro-functional model allows for a better study of the emergency response mechanism.

Another advantage of using an explicit model to describe an industrial emergency plan lies in the capacity to represent each function as a separate entity. Then, resources, interactions (inputs, outputs and supports) and other attributes are associated to each entity, in order to complete the representation. A "package" consisting of the function, its resources, its interactions and other attributes is hence created for each function. The entire plan can hence be represented as an assembly of these "packages". This modular approach enhances the flexibility in the design and analysis of an industrial emergency plan, and allows the designer (and/or analyst) to focus their attention to specific parts of the plan.

Furthermore, by representing an industrial emergency plan by a functional model, one can decompose this complex system into autonomous and independently functional sub-systems. In cognitive psychology, externalization and structural decomposition are regarded as the main strategies in complex problem solving, and are often applied by analysts in different fields [5]. Industrial emergency plans are real world systems; therefore any attempt to analyze them must take into account a large number of components, which creates a consequently large number of interactions. It has been highlighted in the literature [6] that this complexity in modeling can be managed by a hierarchic model strategy in risk management. In such a hierarchic approach, progressively more detailed models of the system can be created by applying a sequence of structural decomposition which breaks up the system by decomposing it into less abstract components. The components can then be analyzed separately, and the results integrated into the analysis, while maintaining the global model of the system being studied. This helps increase the level of depth of the analysis, while making scale economies in overall analysis time [7].

However, the structural decomposition of a complex system must not be an end in itself, or it can easily become a waste of energy. The time and resources needed to fully decompose every all sub-systems of a system down to the elementary level can quickly overwhelm the analyst's capacity. On the other hand, abstraction gives flexibility in the analysis, and allows for completeness and accuracy [8]. The costs and benefits of the process of structural decomposition may be balanced by a partial abstraction. By selecting a particular level of abstraction, only the necessary level of detail is revealed. By decomposing only the necessary sub-systems

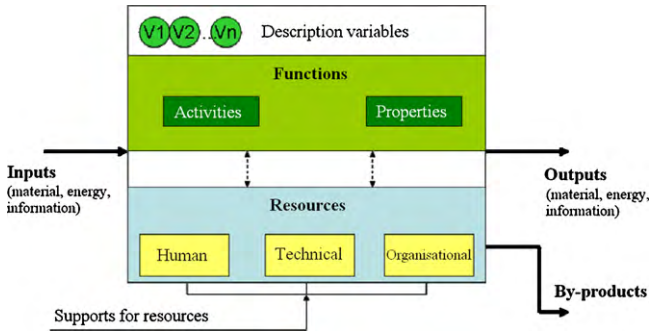

Fig. 1. Process model diagram in the FIS method. Adapted from Flaus [6].

of a larger system, the analysis can focus on these aspects that are necessary to the investigation.

In this paper, the FIS (Functions–Interactions–Structure) approach is used to create a structure-functional model of the plan. The FIS [6] modeling approach has been implemented in order to create a generic model of a typical internal emergency plan. FIS is a hierarchic process modeling method designed for systematic risk analysis. It is based on the SIPOC (Supplier–Input–Process–Output–Customer) approach. The scope of the SIPOC approach is further enlarged to include both the interactions between processes (described in functional and material terms) and the internal structure of the process, whose functions and necessary resources are analyzed [9]. Thus, each system is represented as a set of interacting processes. Each process is modeled using the process model diagram depicted in Fig. 1. XRISK is a software application that has been developed for carrying out structural-functional systemic modeling and risk analysis using the FIS approach [10].

A process is defined in the ISO 9001 standard as "an organized system of activities which uses resources (machines, people, methods, materials...) to transform inputs into outputs". In every case, inputs are turned into outputs because some kind of work, activity, or function is carried out. Processes can be administrative, industrial, agricultural, governmental, chemical, mechanical electrical etc. Resources are used to carry out the activity defined within the process, and supports are the functions required to ensure resources operate as expected. These elements of the process model diagram (resources, functions, inputs/outputs, supports and input/output constraints) are defined in Flaus [6].

Any system that is too complex and/or requires a more detailed analysis may be decomposed into sub-systems, by assigning each function of the system to one sub-system. Each function of the new systems can subsequently be assigned to one sub-system and decomposed. The analyst can thus create as many decomposition levels as the analysis requires. The analysis effort can hence be channeled in studying a specific part of the system, and then integrating the results of the analysis to that of the entire system. This feature helps an integral but also detailed analysis of the failures that can occur in the system.

Thus, the FIS method can be utilized to construct a generic, structural, functional and hierarchic model of the emergency response mechanisms established by the internal and external emergency plan of an industrial facility. This model can then be instantiated to a specific industrial facility, in order to produce a model of this facility's emergency response to major industrial accidents mechanism. However, this modeling is a dynamic process. The model is built according an iterative approach and can be enriched by progressively adding new elements. Thus, a new failure mode, a corresponding function or a missing resource may be added, once identified through research and experience feedback activities.

Experience feedback is an essential aspect of any emergency response system. It helps to ensure the continuous improvement of the system, thus enhancing its robustness, as described in the following section.

2.3. Experience feedback and analysis of industrial emergency plans

Industrial emergency response calls for precise and effective action, which in turn requires a proper organization. The circumstances during the response phase do not allow for the time necessary to improvise this organization, which should therefore be established and tested before the emergency occurs. Emergency plans are used to establish a response system to various emergencies; they set up the organization and identify human and technical resources necessary for the tasks that must be undertaken in order to save lives and reduce damage when an emergency event is immediately imminent or immediately after an emergency occurs.

National emergency management and/or civil protection authorities of many countries or specialized organizations often publish emergency planning guides, designed to assist the work of emergency planners. Examples include the U.S. Federal Emergency Management Agency [11,12], the Civil Protection Direction of the French Ministry of Interior [13–16], but also the Oil and Chemical Industries Safety Studies Group in France (in French: *Groupe d'Etudes de Sécurité des Industries Pétrolières et Chimiques—GESIP*) [17,18]. These guides are based on lessons learned from past natural and technological emergencies and disasters, and represent current knowledge and practice on emergency planning.

Experience feedback (often referred to as "lessons learned") is an important information source for the analysis of emergency planning, including industrial emergency plans. Lessons learned are often a part of operational mechanisms, including of those related to industrial emergency response. The process of experience feedback calls for the identification of any parameters of the plan that may have worked well or not every time an operational mechanism is activated, such as in exercises or for responses to real accidents. Whereas the latter are the only real test of any emergency response system, exercises can also serve the purpose of assessing part or all of the operational mechanism established through an emergency plan. This assessment can then be used to improve the response system.

By nature, the process of experience feedback identifies efficient elements of the plans well as failures or faults that have already occurred when emergency plans are put into action, but does not allow a systemic and exhaustive analysis of the emergency plans studied [19,20]. This process can often be significantly enhanced by a structural method of analysis of the robustness of emergency plans. Several authors have already highlighted the need for a systemic analysis of emergency plans [19,21–24].

In this study, the structure-functional model of the industrial emergency response mechanism is used to organize the information obtained through experience feedback. Failures in emergency response plans may be represented by event trees and analyzed using risk analysis methods, such as the Failure Mode and Effects Analysis [25,26], making lessons learned more readily associated to the different elements of the plan. Hence, emergency planners will find it more practical to integrate experience feedback into future planning endeavors. It will then be easier to use this information during the concept phases of emergency planning, but also for analysis of existing plans. This approach can also take into account the propagation of failures within the functions of the emergency response mechanism, but also enables integrating *a priori* with *a posteriori* analyses of the plans, as described in the next section.

2.4. Proposed methodology

The industrial emergency plan modeling method proposed is funded upon an iterative evolution of a base model. An initial elementary model ("base" model) of an industrial emergency plan is created, using planning guidelines (e.g. from national authorities or international bodies or organizations) and existing plans of the same type. This model needs to represent the functions generally included in the plans of the type under study, but also to take into account territorially related aspects of each plan (which are by definition different in every occasion) by providing for a progressive decomposition of the main functions into sub-functions, until a satisfactory level of detail is attained. In other words, the industrial emergency plan model needs to be functional, generic, and hierarchical.

This base model can be further continuously improved as soon as experience feedback, research or critical thinking reveal new potential failures, missed functions or supplemental resources. This process is iterative, and follows the Plan–Do–Check–Act principle (often referred to as "Deming wheel") [27], hence leading to continuous improvement of the model. The objective is to achieve a model that represents the situation as best as possible, through a process of inserting new elements or modifying existing ones, with a view to adapting the model to new information, for example a new failure identified in one plan. The modification of the model is followed by a validation of the model. In the above example, validation would include an assessment of whether this failure can be recurring to other types of emergency plans as well, and eventually consultation with experts in the field of industrial safety and emergency response. Any differences identified are analyzed to determine the causes before any changes in the model are applied.

An industrial emergency plan concept guide can be created as through this modeling process. The functions, interactions, resources, and supports of the model can be used to point out the basic elements of an industrial emergency plan. For example, an industrial internal emergency plan under the EU "Seveso II" directive shall contain the following general functions:

- Incident detection and plan implementation.
- Emergency self-protection actions.
- Activation of the internal emergency response mechanism.
- Protection of people and property.
- Emergency response and crisis management.

Furthermore, the following resource categories are necessary to the emergency response:

- Human resources
  - ◯ Facility on site personnel.
  - ◯ Emergency operations personnel.
  - ◯ Operations coordination personnel.
- Technical resources
  - ◯ Communications equipment.
  - ◯ Emergency response equipment.
  - ◯ Information management equipment.
  - ◯ Facilities.
  - ◯ Safety at work equipment (work PPE, work emergency equipment etc.).
- Organizational resources
  - ◯ Emergency plan procedures.
  - ◯ Support documents (decision aids, checklists, contact lists etc.).

Each of these resource categories may include other subcategories of individual resource types. For example, the "Emergency Operations" human resource category includes firefighters (professional and/or volunteer), first responders or emergency medical technicians, operations support personnel and security personnel. The "Emergency Response Equipment" technical resource category shall include firefighting, emergency medical care and hazardous materials response equipment. Each of these resources has a defined set of support functions. For example, all technical resources need proper maintenance to work optimally or at all.

Once the model is set up, a process of identifying potential critical points or failures is initiated. This process is based both on an *a priori* and an *a posteriori* analysis of the model. The *a priori* analysis aims at identifying potential failures of the plan through an examination of the model at resource and function levels. The emergency plan model contains a defined set of resources for each function. Failures of the plan's functions are caused by failures of one or more of their resources, or of one or more of their inputs. A fault tree is built at function level, representing the logical combination of events leading to the failure of the function. The base events of this fault tree are the failures of the function's resources and the absence/failure of the function's inputs. Potential failures of resources result in turn from the lack or failures of their respective support functions. Hence, another fault tree is built for each resource, representing the logical combination of events that can lead to the failure of the resource. The events at the top of each resource fault tree are the base events of the function fault tree, while the base events are the failures of the resource's support functions. This analysis is enhanced by the experience feedback activities that comprise the *a posteriori* analysis. Lessons learned are used to update the model and identify potential failures or critical points that may have been missed by the *a priori* analysis.

One or more assessment questions are associated to each elementary or intermediate event in the function fault tree. Emergency plan audit/assessment checklists can hence be created through this process, and generated after the generic model of the industrial emergency plan. These checklists can evaluate the degree to which potential failures in the emergency response mechanism have been taken into account in the planning process and acted upon.

In this section we have described the methodology of progressive/iterative modeling of industrial emergency plans and their failures. In the next section, we will present the results of the application of the above methodology in the case of Internal Emergency Plans (under the EU Seveso II Directive).

3. Results

3.1. Internal Emergency Plan generic, functional, hierarchic model

The initial internal emergency plan model shall be presented in this paragraph. This "base model" can further be edited through research and lessons learned from industrial accidents and emergency response exercises in industrial installations. In using the FIS approach to model industrial emergency plans, a system shall be considered as an organized entity, made out of unit elements each being only defined with regard to their place in this entity. In this paper, a part of the Internal Emergency Plan shall be presented as an example.

The structure-functional-generic model of the Internal Emergency Plan has been created through consultation with industrial operators. Hence, the basis of the model includes several emergency plan guides [11,12,14–18] and 3 existing Internal Emergency Plans of chemical and petrochemical industrial installations. In modeling an industrial emergency plan through the FIS approach, each generic action that is (or should be) defined by the plan is represented by a process. The structure is subsequently constructed by setting out the interactions between processes. Then, the resources

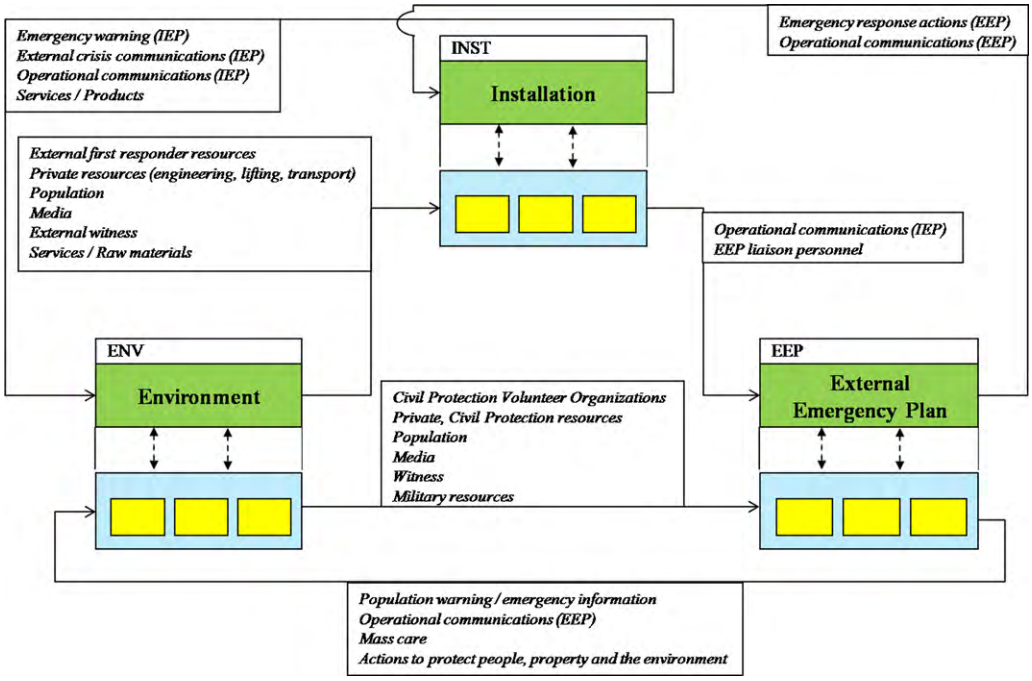

Fig. 2. Generic functional model of response to industrial emergencies.

necessary for implementing each function and their corresponding supports are identified and added to the model.

Three major systems are considered in the FIS generic model of response to industrial emergencies by putting into action industrial emergency plans defined by the SEVESO II Directive (Fig. 2). Each of these three systems (corresponding to the industrial installation, its environment and the external emergency plan respectively) is further decomposed into sub-systems, according to the FIS decomposition principle. Inputs and outputs represent the flow of information (communications), key persons to the response, or actions on an entity (e.g. emergency response actions).

The "ENVIRONMENT" system represents the physical environment of the facility. It is a "buffer" system that contains all the people, property and natural environment around the facility, but the neighboring industrial facilities, the local territories, and any special elements at risk as well. The environment of the facility plays a critical role in crisis management, as it defines the theatre of emergency operations, the communications necessary to implement the plan, and any secondary hazards (e.g. domino effects, or an explosion causing a landslide).

The "EXTERNAL EMERGENCY PLAN" system represents the civil protection mechanism put in place in order to respond to emergencies originating from the facility. It is activated once the effects of an industrial accident extend, or are reasonably anticipated to extend, beyond the physical limits of the industrial facility. Since, for simplicity, the example model presented in this article is that of the Internal Emergency Plan, this system will not be presented in further detail here.

The "INSTALLATION" system represents the industrial facility itself. The facility's main objective is to produce chemical substances in various quantities and forms. This system is decomposed into two sub-systems (Fig. 3):

- The "PRODUCTION SYSTEMS" sub-system corresponds to the production of substances and/or services in the facility,
- The "INTERNAL EMERGENCY PLAN" system represents the mechanism put in place internally to deal with industrial accidents.

This decomposition serves a twofold purpose. First, the analysis is focused on the Internal Emergency Plan, without totally neglecting the production activities of the industrial installation. Since the objective of this analysis is to assess the robustness of the emergency plan based response, only the "INTERNAL EMERGENCY PLAN" system is further decomposed. The 5 sub-systems into which the above system is decomposed correspond to the generic functions that any industrial internal emergency plan is called to fulfill. These sub-systems and their interactions are depicted in Fig. 4. The second purpose of the decomposition of the "INSTALLATION" system is to illustrate the interactions between the production activities of the installation and the mechanism put in place by the Internal Emergency Plan. For example, industrial emergencies often call for a modified operation mode or even shut-down of part or all of the plant's activities. Therefore, the necessary information (orders) needs to be given from the industrial site Emergency Operations Center (EOC) to the respective activity centers (i.e. plant workshops), in order to ensure effective plant control. This information flow is a typical example of the interaction between these two sub-systems.

The system named "INCIDENT SURVEILLANCE" represents the detection of the occurrence of a hazardous event, presenting a risk to people, property, and the environment. A pool fire and a leak of a toxic material are two examples of such hazardous events. One or more technological systems may be used for detection, for example an array of fire detecting devices or a real-time monitoring device for a chemical reactor. Furthermore, hazardous events may be detected by witnesses, usually workers of the facility, or security personnel (especially during non-working hours/days). A combination of these two mechanisms is usually put into place by industrial facility operators. This function contains the determination of the incident's location and an assessment of its intensity and possibly of the area affected. If the detection is performed by a technological system, more precise information on the physical and chemical parameters of the hazardous event (pressure, temperature etc.) will be known. If the hazardous event is detected by a witness and/or a visual surveillance system (e.g. a CCTV security system), then additional information on the numbers and intensity

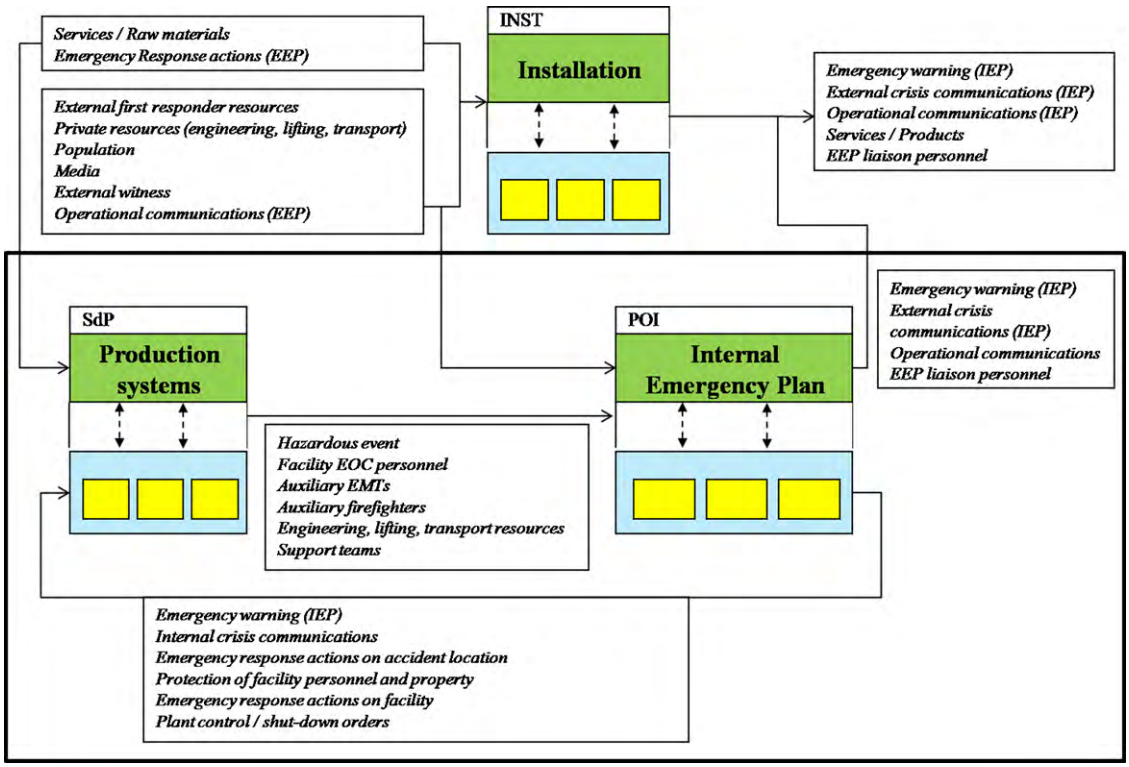

Fig. 3. Functional decomposition of the "INSTALLATION" system into two sub-systems.

of damage, as well as on people immediately affected (wounded, deceased) may also be available. This function is part of the internal emergency plan alert and precedes the plan's activation.

Once a hazardous event is detected and identified as such, on site personnel will attempt to mitigate its immediate effects by taking emergency measures to ensure their own safety. These may be simple actions aiming to avoid propagation of the accident (e.g. closing off a control valve, shutting down a circuit, putting out a small fire using portable fire extinguishers), but may also include evacuation and isolation of the area exposed to the hazard, if the risk level and the incident speed of onset justify these actions. As soon as the workers are safe, they may take action to secure the affected

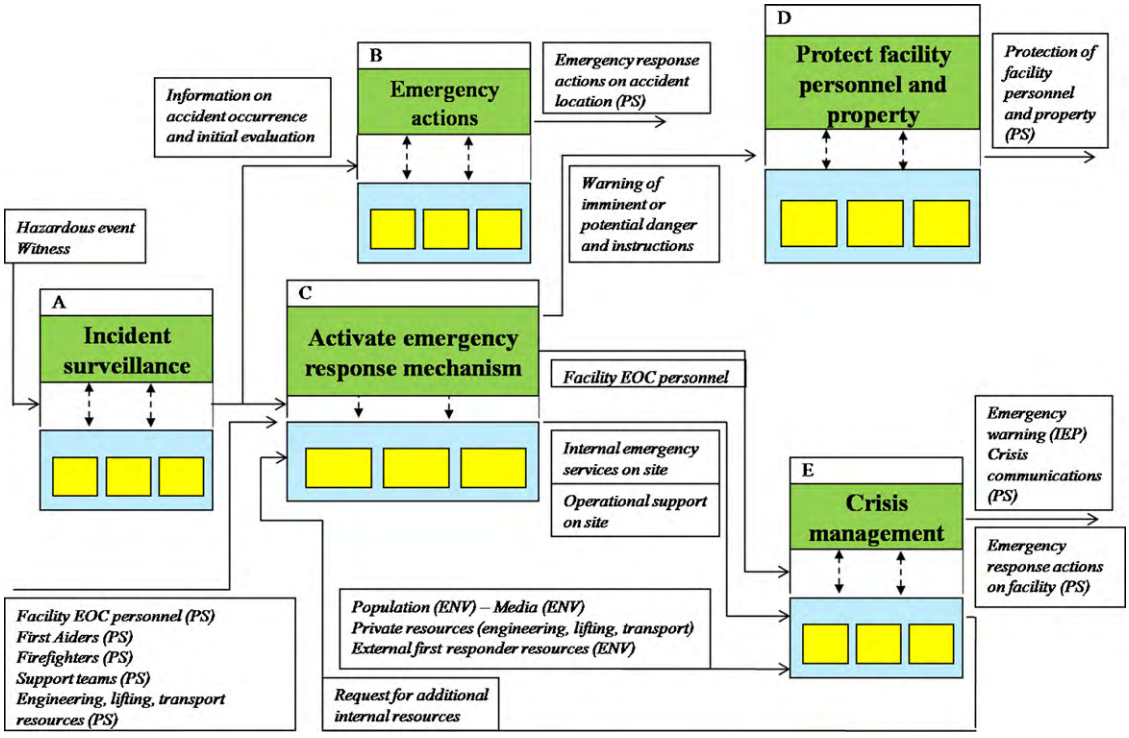

Fig. 4. Functional-generic model of an Internal Emergency Plan.

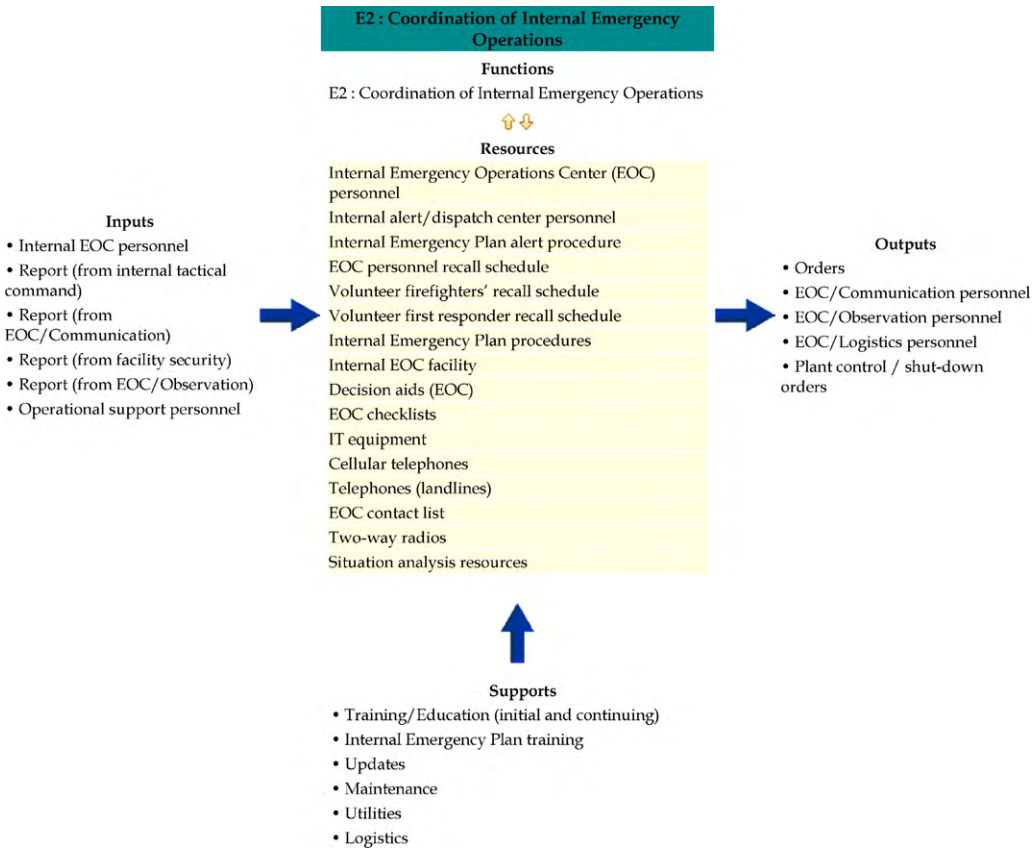

Fig. 5. "Box model" of system E2: Coordination of Internal Emergency Operations.

area and assist the internal emergency services, for example by directing the fire engines to the accident scene. These actions are taken into account in the model and are represented by the system called "EMERGENCY ACTIONS".

For the emergency response to begin, the resources identified in the internal emergency plan must be mobilized. This task is the object of the "ACTIVATE EMERGENCY RESPONSE MECHANISM" system. This function is essential to the internal emergency operations, since it defines the resources that will be assigned to various actions needed to effectively respond to the accident. It includes the reception and treatment of the call to the facility's emergency number, and the mobilization of the internal emergency services, facility emergency operations center personnel, and any operational support resources. It also includes the emergency warning of any person within the facility that may be exposed to either the hazard that caused the accident in the first place, or one of the associated or secondary hazards. Warning is usually followed by instructions to be followed by all receptors of the message.

By warning the people inside the facility, they can take action to protect themselves against chemical or other hazards. Major industrial accidents often have a rapid onset: for example, a toxic gas cloud can reach an entire facility within a few minutes. Therefore, some internal emergency plans prescribe the emergency warning of all personnel within the installation by default. In most cases of major industrial accidents, there are two solutions for the protection of people: shelter in place or evacuation. Evacuation is safest if it can be completed before the danger reaches the evacuation routes. If evacuation is not an option or if a short passage of a toxic cloud is anticipated, then people are instructed to shelter in place and take protective measures (e.g. close all ventilations, stay away from openings, remain in an interior room within a strong structure etc.). Chemical or other processes are also often stopped as a precautionary measure or in order to avoid any secondary effects. All these actions correspond to the "PROTECT FACILITY PERSONNEL AND PROPERTY" system.

The last sub-system of "INTERNAL EMERGENCY PLAN" is "CRISIS MANAGEMENT". This system represents all the action taken by the facility mechanism to respond to the incident internally. It is the internal emergency plan's most complex function, and it includes internal emergency operations (firefighting, hazardous materials response, search and rescue, emergency medical care, incident command), as well as action taken to manage the overall response, communicate, secure the facility, and maintain a record of the incident and incident management.

As presented above, resources, interactions and supports are assigned to each system. The FIS approach calls for a graphic representation ("box model") of each system. The representation of the COORDINATION OF EMERGENCY OPERATIONS" sub-system of the "CRISIS MANAGEMENT" system is included here as an example (Fig. 5).

Therefore, the entire model includes five generations of systems and functions. At the lowest level of decomposition, the model includes a total of 26 functions. Each system has its own resources and interactions with other systems. The model includes more than 150 human, technical and organizational resources, organized into 63 types of resources.

3.2. Experience feedback used

The FIS modeling approach has allowed a functional analysis of industrial emergency plans. The *a posteriori* identification of failures was evidence based: it included the analysis of data from databases and lessons learned from exercises of emergency response to indus-

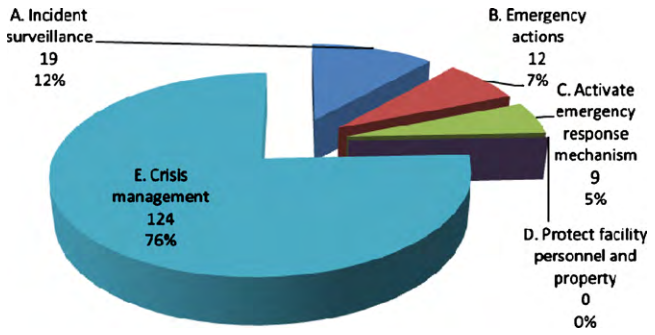

Fig. 6. Failures in industrial emergency response mechanisms established by Internal Emergency Plans, as identified through emergency response exercises or analysis of accident reports.

trial accidents. The purpose of this task is to identify failures to the plan functions in terms of the accomplishment of the functions' activities or near-misses, i.e. events that could have led to failures of one or more functions of the plan but this was eventually avoided.

The ARIA (Analysis, Research and Information on Accidents) database of the French Ministry of Ecology and Sustainable Development was the first source of information used. This database lists all the technological accidents (both industrial and related to hazardous materials transport) that have had a real or potential impact on public health and safety, the agriculture, or the natural environment. It has been developed by the Bureau of Industrial Risk and Pollution Analysis of the French Ministry of Sustainable Development. On October 2009, the ARIA database included more than 30.000 short reports of accidents having occurred in France or abroad. A report is added for every new accident, and the database is entirely accessible on the Internet. A small number of accidents (159 on November 2008) have been selected due to their serious consequences or for their value of lessons learned, and are the object of longer reports. These reports are listed under 13 categories (based on the industrial activity concerned) including, but not limited to, chemical, explosive, plastics, refineries, metallurgy etc. An analysis of these reports has revealed failures of critical points in Internal and/or External Emergency Plans in 64 out of 159 accidents. In total, 83 critical points have been identified in the application of Internal Emergency Plans, and 23 in the case of External Emergency Plans.

The other part of the research for evidence base on critical points in industrial emergency plans included following industrial emergency response exercises in the facilities whose Internal and/or External Emergency Plans have been used for the development of the Emergency Plan model described above. These exercises, being monthly or yearly in frequency, have revealed more critical points in the application of industrial emergency plans. In total, 22 Internal Emergency Plan exercises and 2 External Emergency Plan Exercises were followed from January 2008 to October 2009. An "after action" report was written after every exercise. These exercises revealed 13 more critical points in the application of Internal Emergency Plans and 9 in the case of External Emergency Plans.

These failures/critical points are used as a feedback to the plan model. They have been classified in tabular form, including the failure type and the function(s), resource(s) and support(s) associated, following the formalization described in Section 3.1. This table has been used to assign frequencies to each failure type. The cumulative frequencies of these failures (by main function of the Internal Emergency Plan) are represented in Fig. 6. The critical points that stand out in terms of highest frequency are presented on Table 1. No near-miss events were identified in the experience feedback activity performed, perhaps due to the poor documentation of such events in generic experience feedback reports. However, such near-miss events identified by industrial operators and/or civil protection authorities during exercises or real incidents can be used to improve the emergency response system.

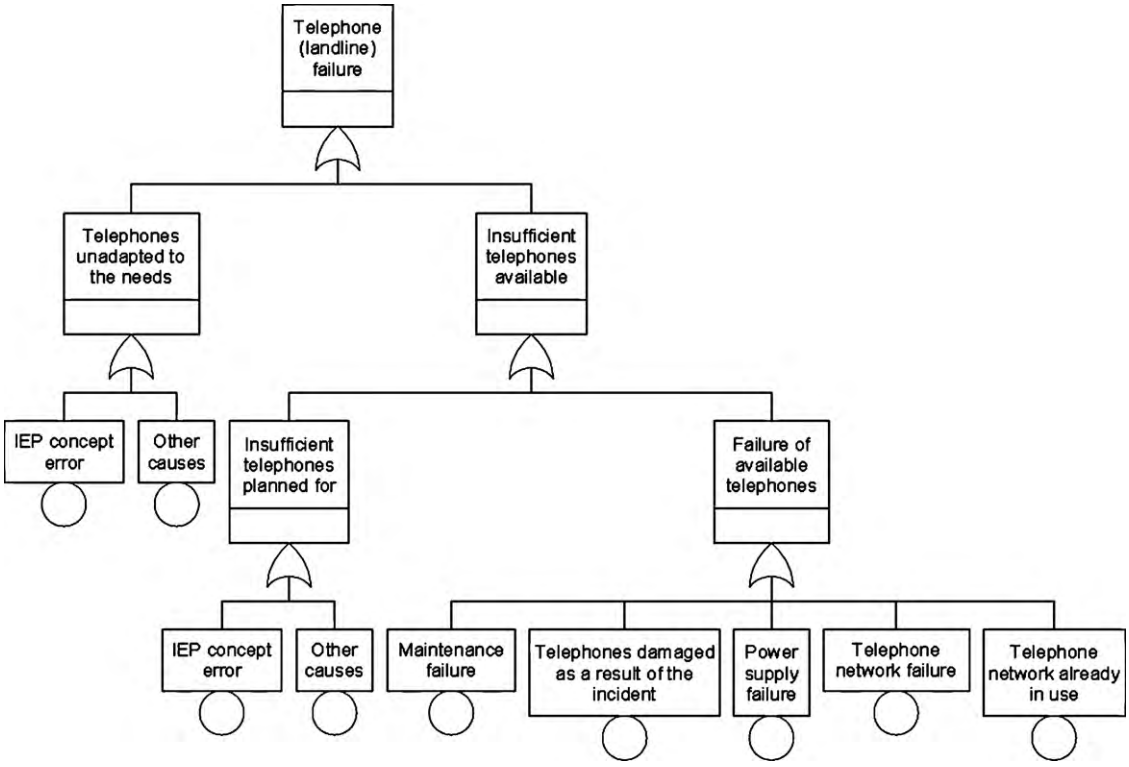

Fig. 7. Fault tree for the "Telephones (landlines)" resource.

Table 1
Frequency of observation of critical points identified through emergency response exercises (2008–2009) or analysis of accident reports. Numbers in parentheses indicate percentage to the total number of critical points identified.

Critical point designation	Function involved	Frequency
Failures of the emergency response equipment	E	39
Difficulty in the acquisition of Internal Emergency Plan (IEP) procedures by Internal Emergency Operations Centre (EOC) personnel	E	24
Delay in personnel mobilization and/or recall	C	8
Problems in the communication between the Internal EOC and Emergency Response Teams	E	6
Delay in activating the IEP	E	4
Difficulty in using the equipment in the Internal EOC	E	3

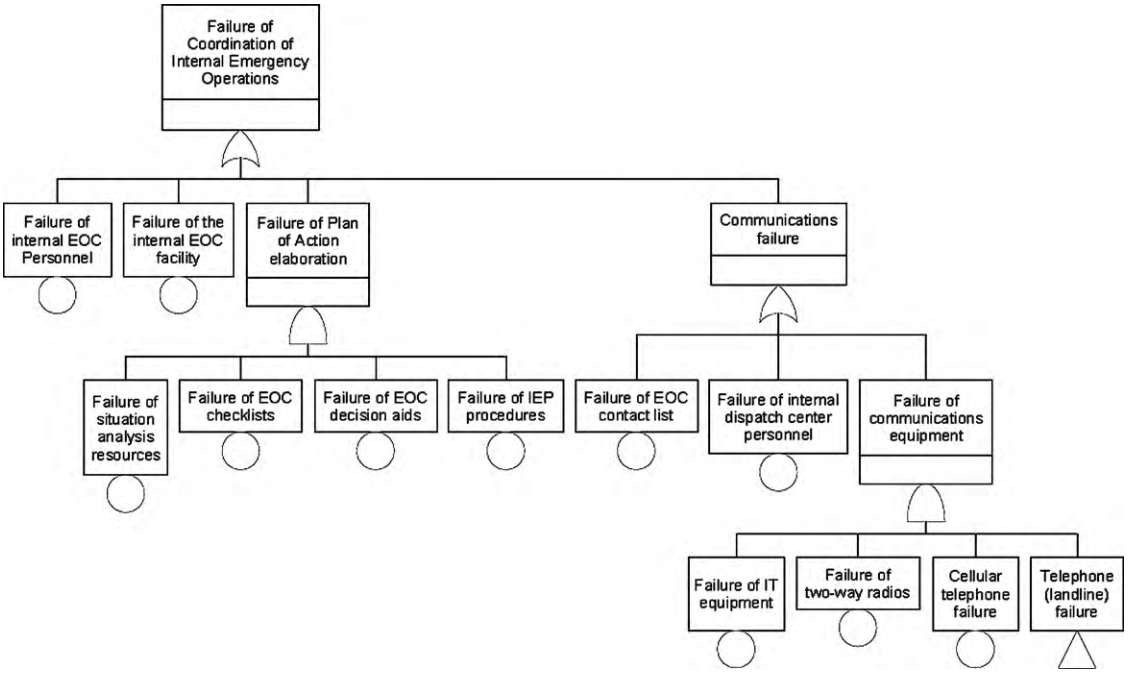

Fig. 8. Fault tree for the E2: Coordination of Internal Emergency Operations function.

3.3. A checklist example

The critical points identified by the above presented *a priori* and *a posteriori* analyses of the failures of industrial emergency plans are combined to create fault trees for each of the functions, which represent the logical combinations of events leading to function failure. Questions are then assigned to assessment checklists. Each checklist refers to one function, including all its associated resources, supports and interactions.

As an example, the fault tree of the function E2: Coordination of Internal Emergency Operations is given in Fig. 7 below. This fault tree contains the logical combination of events leading to the failure of the function. The base events of this fault tree are the failures of its resources and the inputs of this function. Other fault trees are built for each one of the resources identified in the function. As an example, the fault tree of the resource "Telephones (landlines)" is given in Fig. 8. The top event of this fault tree and the corresponding base event of the function fault tree are the same. The resource fault tree represents the logical combination of events that may lead to the failure of this resource. Hence, the complete function fault tree is created by "assembling" the fault tree of Fig. 7 with the resource fault trees of all this function's resources (such as the one in Fig. 8).

One or more assessment questions are generated after each base or intermediate event of the function's fault tree. The sum of these questions constitutes the function's checklist. The checklist of the function E2: Coordination of Internal Emergency Operations is given in the appendix as an example.

The checklist of each function is derived through a logical procedure from the failure modes and fault tree of the corresponding function. The failure modes of a function include the failure modes of all the resources necessary to the function and the failure modes corresponding to the inputs to the process. At this stage, the checklist of every function can only allow a qualitative analysis of the function. A method to quantify the checklists is currently being developed, which could help to associate a failure probability to each of the plan's functions.

4. Conclusion

A functional-generic model has been used so far to facilitate an iterative risk analysis approach for the assessment of the robustness of industrial emergency plans. This approach is based on the identification of the potential failures during the application of the plan. These failures have been in turn identified using an *a priori* analysis of the plan model and an *a posteriori* analysis of lessons learned from industrial accidents and emergency response exercises. The sum of these potential failures is then transformed into assessment checklists that can be used for the evaluation of the robustness of the plan.

This method provides for an assessment of the functions and the structure of an industrial emergency plan. By its nature, it can assist in the management of protection objectives. However, it questions neither the safety reports of an installation nor the decision making process during a crisis. For example, in the activation of the

external emergency plan, this method can help the facility operator identify problems in the structure of the function responsible for this decision. Nevertheless, it will not assess the criteria upon which this decision is taken (which are based on the analysis of consequences of industrial accidents and as such are contained in the facility's safety reports) nor the decision making process in times of crisis, which is site and time-specific and cannot be criticized as such.

The perspectives in the development of the methodology include two features, both of which are the focus of our current work. First, it was established that the functional-generic plan model includes a great number of functions, resources and interactions, which makes its practical exploitation rather difficult. This is why an explicit specification of the functions and resources is necessary in order to ensure knowledge transfer. Therefore, an ontological approach [28,29] is currently being used to formalize the description of functions and resources included in the industrial emergency plan model, in order to facilitate knowledge transfer. The second question pertains to the quantification (or deterministic definition) of the robustness of an industrial emergency plan. The checklists defined in Sections 2.4 and 3.3 above shall be used, in conjunction with the resource fault trees, for example Fig. 7, to generate an indicator of the robustness of each resource. Once an indicator is defined for each resource, these shall be combined to generate the indicator of the function through the logical combination of the indicators of all the resources included in the function, using the function fault trees (for example Fig. 8). A global robustness indicator for the plan is then generated through the logical combination of the indicators of the functions (after the plan model structure).

This approach can be developed and used to produce a decision making assistant tool, that could be used in the assessment of the robustness of an existing industrial emergency plan (internal or external). Nevertheless, the methodology is also applicable during the plan development phase, and can lead to the creation of a more robust industrial emergency plan. In the latter case, an iterative analysis of the various functions of the plan is performed as the plan is being developed, which progressively increases the robustness of the final product.

Appendix A.

1. Is this function included in the emergency response mechanism?
2. Is there a mechanism to ensure the quality of situation reports received?
3. Are Internal EOC Personnel trained in Internal Emergency Plan features?
4. Are Internal EOC Personnel trained in emergency management?
5. Is the number of available EOC Personnel sufficient for EOC operation, according to the needs anticipated in the Internal Emergency Plan?
6. Do EOC Personnel have other roles (within the Internal Emergency Plan or not) that could interfere with their availability in case of emergency?
7. Are Internal Dispatch Center Personnel trained in the Internal Emergency Plan features relative to their duties?
8. Is the number of available Internal Dispatch Center Personnel sufficient for Internal Dispatch Center operation, according to the needs anticipated in the Internal Emergency Plan?
9. Do Internal Dispatch Center Personnel have other roles (within the Internal Emergency Plan or not) that could interfere with their availability in case of emergency?
10. Does the Internal Emergency Plan alert procedure cover the emergency management needs identified within the Internal Emergency Plan?
11. Is the Internal Emergency Plan alert procedure updated on a regular basis?
12. Is the EOC personnel recall schedule well fitted to the needs identified within the Internal Emergency Plan?
13. Is the EOC personnel recall schedule updated on a regular basis?
14. Is the Volunteer Firefighters' recall schedule well fitted to the needs identified within the Internal Emergency Plan?
15. Is the Volunteer Firefighters' recall schedule updated on a regular basis?
16. Is the Volunteer First Responder recall schedule well fitted to the needs identified within the Internal Emergency Plan?
17. Is the Volunteer First Responder recall schedule updated on a regular basis?
18. Do the Internal Emergency Plan operations procedures cover the emergency management needs identified within the Internal Emergency Plan?
19. Are the Internal Emergency Plan operations procedures updated on a regular basis?
20. Is the Internal EOC facility well suited for use within the Internal Emergency Plan system framework?
21. Does the Internal EOC facility location provide protection in case of a major industrial accident?
22. Do (EOC) decision aids correspond to the operational needs identified within the Internal Emergency Plan?
23. Are (EOC) decision aids updated on a regular basis?
24. Is a sufficient number of (EOC) decision aid copies readily available?
25. Do EOC checklists correspond to the operational needs identified within the Internal Emergency Plan?
26. Are EOC checklists updated on a regular basis?
27. Is a sufficient number of EOC checklist copies readily available?
28. Is IT equipment well adapted to the needs of EOC operation?
29. Is IT equipment sufficient?
30. Is IT equipment used only for emergency response?
31. Is IT equipment subject to maintenance according to the manufacturer's instructions?
32. Is there an appropriate electrical supply for the IT equipment?
33. Is there redundant communications equipment available for use in the Internal EOC?
34. Are cellular telephones appropriate for use within the Internal Emergency Plan framework?
35. Is there a sufficient number of cellular telephones available?
36. Are cellular telephones maintained according to the manufacturer's instructions?
37. Are cellular telephones readily available in case of an emergency?
38. Is there an appropriate electrical supply (batteries) available for the cellular telephones?
39. Are telephones (landlines) appropriate for use within the Internal Emergency Plan framework?
40. Is there a sufficient number of telephones (landlines) available?
41. Are telephones (landlines) maintained according to the manufacturer's instructions?
42. Are telephones (landlines) readily available in case of an emergency?
43. Is there an appropriate electrical supply available for the telephones (landlines)?
44. Are two-way radios appropriate for use within the Internal Emergency Plan framework?
45. Is there a sufficient number of two-way radios available?
46. Are two-way radios maintained according to the manufacturer's instructions?

47. Are two-way radios readily available in case of an emergency?
48. Is there an appropriate electrical supply (batteries) available for the two-way radios?
49. Does the EOC contact list correspond to the operational needs of the EOC?
50. Is the EOC contact list updated on a regular basis?
51. Is a sufficient number of the EOC contact list readily available?
52. Are the situation analysis resources well adapted to the needs identified within the Internal Emergency Plan?
53. Are the situation analysis resources used only for emergency response?
54. Are the situation analysis resources subject to maintenance according to the manufacturer's instructions?

References

[1] B. Pavard, J. Dugdale, N.B. Saoud, S. Darcy, P. Salembier, Design of robust socio-technical systems, 2nd Symposium on Resilience Engineering, Juan-les-Pins, France, 2006, http://www.resilience-engineering.org/proceedings.htm.
[2] T.W. Harding et al., Management des risques majeurs: des disciplines à l'interdisciplinarité (French), programme plurifacultaire du Rectorat MRM, Université de Genève, 2001.
[3] J.L. Wybo, The role of simulation exercises in the assessment of robustness and resilience of private or public organizations, in: H.S. Pasman, I.A. Kirillov (Eds.), Resilience of Cities to Terrorist and other Threats, Springer, 2008, pp. 491–507.
[4] C. Ramsay, Protecting your business: from emergency planning to crisis management, J. Hazard. Mater. 65 (1999) 131–149.
[5] R.J. Heuer, Psychology of Intelligence Analysis, Center for the Study of Intelligence, U.S. Central Intelligence Agency, 1999.
[6] J.M. Flaus, A model-based approach for systematic risk analysis, Proc. IMechE 222 (2008) 79–93.
[7] F. Baiardi, C. Telmon, D. Sgandurra, Hierarchical, model-based risk management of critical infrastructures, Rel. Eng. Syst. Saf. 64 (2009) 1403–1415.
[8] H. Simon, The Sciences of the Artificial, 2nd ed., MIT Press, 1981.
[9] J.M. Flaus, Méthodologie FISE, Internal Document G-SCOP/Institut National Polytechnique de Grenoble, 2007 (French).
[10] XRISK software tool website: http://www.xrisk.fr.
[11] Federal Emergency Management Agency, Developing and Maintaining State, Territorial, Tribal and Local Government Emergency Plans, Comprehensive Preparedness Guide (CPG), vol. 101, 2009, http://www.fema.gov/pdf/about/divisions/npd/cpg_101_layout.pdf.
[12] Federal Emergency Management Agency, Guide for All-Hazard Emergency Operations Planning, State and Local Guide (SLG), vol. 101, 1996, http://www.fema.gov/pdf/plan/slg101.pdf.
[13] Direction de la Défense et de la Sécurité Civiles, Guide ORSEC Départemental – Méthode générale, Tome G.1, 2006 (French), http://www.interieur.gouv.fr.
[14] Direction de la Défense et de la Sécurité Civiles, ORSEC Départemental – Disposition Spécifique – Plan Particulier d'Intervention – PPI) – Etablissements SEVESO «seuil haut», Guide, Tome S.1.2, 2007 (French), http://www.interieur.gouv.fr.
[15] Direction de la Défense et de la Sécurité Civiles, ORSEC Départemental – Disposition Spécifique – Plan Particulier d'Intervention (PPI) – Etablissements SEVESO «seuil haut», Mémento, Tome S.1.1, 2007 (French), http://www.interieur.gouv.fr.
[16] Direction de la Défense et de la Sécurité Civiles, Guide d'élaboration d'un Plan d'Opération Interne, Paris, 1985, ISBN: 2-905015r-r16-0 (French).
[17] Groupe d'Etudes de Sécurité des Industries Pétrolières et Chimiques, Guide méthodologique du GESIP pour l'élaboration du P.O.I. d'un site industriel, usine chimique, complexe pétrochimique – Rapport GESIP 96/01, 1996 (in French).
[18] Groupe d'Etudes de Sécurité des Industries Pétrolières et Chimiques, Guide méthodologique du GESIP pour l'élaboration du Plan d'Opération Interne d'un établissement de stockage de produits inflammables (dépôt) ou d'un petit établissement industriel – Rapport n° 96/02, 2001 (French).
[19] B. Jackson, The Problem of Measuring Emergency Preparedness—The Need for Assessing "Response Reliability" as Part of Homeland Security Planning, Rand Corporation, 2008, http://www.rand.org.
[20] P. Lagadec, Katrina: Examen des rapports d'enquête, Tomes 1 et 2, Ecole Polytechnique – Centre National de la Recherche Scientifique, 2007 (French), http://ceco.polytechnique.fr.
[21] D. Alexander, Principles of Emergency Planning and Management, Terra Publishing, 2002.
[22] D. Alexander, Towards the development of a standard in emergency planning, Dis. Prev. Mgmt. 14 (2005) 158–175.
[23] T. Kanno, K. Furuta, Resilience of Emergency Response Systems, 2nd Symposium on Resilience Engineering, Juan-les-Pins, France, 2006, http://www.resilience-engineering.org/proceedings.htm.
[24] H. Mayer, First Responder Readiness: A systems approach to readiness assessment using model based vulnerability analysis techniques, Master Thesis, Naval Postgraduate School, 2005.
[25] A. Villemeur, Sûreté de fonctionnement des systèmes industriels, Editions Eyrolles, 1988 (French).
[26] U.S. Department of Defense, Military Standard—Procedures for Performing a Failure Mode, Effects and Criticality Analysis, MIL-STD-1629A, 1980.
[27] W.E. Deming, Out of the Crisis, MIT Press, 1986.
[28] F. Bénaben, C. Hanachi, L. Lauras, P. Couget, V. Chapurlat, A metamodel and its ontology to guide crisis characterization and its collaborative management, in: Proceedings of the 5th International ISCRAM Conference, Washington D.C., USA, 2008.
[29] T. Gruber, A translation approach to portable ontology specifications, Knowl. Acquis. 5 (1993) 199–220.