Robustness analysis of industrial emergency plans: a model-based methodology

G. M. Karagiannis[1], E. Piatyszek[1] & J. M. Flaus[2]
[1]*Ecole Nationale Supérieure des Mines de Saint-Etienne, France*
[2]*Institut National Polytechnique de Grenoble, France*

Abstract

The purpose of this paper is to present a methodology for the analysis of the robustness of industrial internal and external emergency plans, established by the European Union SEVESO II Directive. This methodology is based upon a systemic, hierarchical and generic model of an internal or external industrial emergency plan. The process generally found within an internal and/or external industrial emergency plan is identified through the model, thus allowing for a modular representation of the plan. Each process integrates the functions/activities performed, the resources necessary for performing these functions/activities, the resources generated or affected by these functions, the supports required for each resource and the interactions (inputs and outputs) of each process. An explicit specification of these elements for a generic plan was provided through an ontological approach. An analysis of the plan model is performed to estimate *a priori* the failures that can potentially occur in the emergency response phase, when the plan is put into action. An extensive experience feedback analysis has also been performed to identify *a posteriori* the failures that have already occurred during the application of the plan. Some 160 accident reports have been consulted, and 31 internal and external emergency plan exercises were followed. This double analysis (*a priori* and *a posteriori*) has led to putting in place assessment checklists, structured via the systemic model for each of the plan's process. Each checklist provides an indicator of the level of accomplishment (performance indicator) for the respective function. The logical combination of the function performance indicators results in a comprehensive assessment of the robustness of the industrial emergency plan. This methodology can hence be used as a toolbox, both for the assessment of existing plans and also for the iterative development of industrial emergency plans.

Keywords: industrial emergency planning, robustness, experience feedback, model-based risk analysis, risk assessment.

WIT Transactions on Information and Communication Technologies, Vol 43, ©2010 WIT Press
www.witpress.com, ISSN 1743-3517 (on-line)
doi:10.2495/RISK100091

1 Introduction

Industrial emergency plans are compulsory by law for industrial facility operators in many countries around the world. In the European Union area, the 96/82/CE Directive, also known as the "Seveso II" Directive, is the reference legislative text concerning the emergency management of industrial accidents involving hazardous materials. It has been transposed to the European Union Member States' law, either as is, such as the Common Ministerial Decision 12044/613/2007 in Greece, or as a part of a wider legislative framework, such as the Classified Installations for Environmental Protection in France or the Control of Major Accident Hazards regulation (COMAH) in the UK. In the United States, a number of legislative texts under the Code of Federal regulations, such as the Comprehensive Environmental Response, Compensation and Liability Act (CERCLA 1980), the Superfund Amendments and reauthorisation Act (SARA 1986) and the Emergency Planning and Community Right-to-Know Act (EPCRA, or SARA Title III), provide industrial emergency planning regulatory requirements for facility operators and public authorities.

Emergency plans are ongoing plans maintained by various jurisdictional levels for responding to a wide variety of potential hazards. They describe how people and property will be protected; detail who is responsible for carrying out specific actions; identify the personnel, equipment, facilities, supplies and other resources available; and outline how all actions will be coordinated [1]. They are fundamentally a risk management tool, in that they define the emergency response mechanism for all the hazards identified within a jurisdiction.

Industrial emergency plans are a type of emergency plan that define the emergency response mechanism for accidents occurring within an industrial facility. Major industrial accidents can occur in the process industries either during the storage of a hazardous material or as a result of the employment of hazardous substances in the process itself. An industrial emergency will usually involve an undesired chemical reaction giving rise to a thermal runaway or leading to an accidental release of toxic, reactive, or flammable substances. Hence, there will normally be three resulting hazards: fire, explosion and toxic release [2]. A major emergency in an industrial facility usually goes through three main stages: raising the alarm, declaration of the emergency and implementation of emergency procedures [3].

While there are a number of publications on emergency planning and industrial emergency plans are a regulatory requirement in many industrialised countries, standards for emergency plans are seldom defined. Several authors have highlighted the need for analysing and evaluating emergency plans [4–7]. Emergency plans are complex systems that can suffer a number of failures, such as unavailability of critical personnel or failure of technical assets. The purpose of this paper is to present a model-based approach for industrial emergency plan robustness analysis. It is organised as follows: first the main features of industrial emergency planning are reviewed, and then a method for building a structural-functional emergency plan model is presented. This method is assisted by the employment of knowledge acquired through lessons learned following real

industrial accidents or industrial emergency plan exercises. Section 2 is completed with the description of the industrial emergency plan robustness assessment method, based on the emergency plan model. An overview of the structural-functional model of an internal industrial emergency plan is given at the beginning of section 3 as an example, followed by a description of the experience feedback elements used. An example of the estimation of the robustness of one of the plan's functions is given in the next paragraph. Finally, conclusions are summarised in section 4.

2 Methodology

The definition of robustness is not globally agreed upon. The apprehension of this term is further complicated by its close relation to resilience and stability. Robustness is often defined as the capacity of a system to adapt its behaviour to deteriorated circumstances or unforeseen situations, such as a perturbation of the environment, or to internal dysfunctions in the organisation of the system [8]. In the context of industrial internal and external emergency plans, and for the purposes of this paper, robustness can be defined as the emergency response system's capacity to remain effective under deteriorated circumstances, that can result for example from failures of technical resources necessary to response operations, lack of competence of response personnel, or problems inherent in the emergency procedures themselves. In other terms, robustness is defined as the efficiency of the industrial emergency response system and its ability to perform according to plan under deteriorated circumstances. Therefore, in order to define the robustness of industrial emergency plans, one needs to identify the emergency response system's objectives in terms of its anticipated performance.

2.1 Model based risk analysis – FIS modelling approach

Disaster and emergency planning in general is guided by several guides and references, published by national authorities [1, 9–11], international bodies [12] and the scientific community [13]. Since industrial emergencies are technological in nature and involve many complex technical features (such as knowledge about hazardous materials), specific operational needs and constraints must often be taken into consideration in planning for this kind of accidents. Therefore, specific emergency planning guides are published by national authorities of industrialised countries to aid local authorities' emergency managers in planning for industrial accidents. Since it is a general rule that emergency plans should be all-hazard in scope, these documents are often an annex to a general emergency planning guide [14–16]. Finally, civil protection authorities and/or industrial safety bodies often publish special guides to assist industrial operators in internal emergency planning [17–20].

Despite the variety of industrial processes and facilities, industrial emergency plans will frequently contain the following functions [3]:

- Plant control/shut-down and engineering activities (repairs, utilities etc.)
- Leak control and hazard reduction (removal of tankers etc.)

- Fire fighting and chemical analysis (toxic, radioactive materials etc.)
- Movement of equipment (fire fighting, first aid, equipment etc.)
- Traffic control (at incident, within the plant, at plant entrance etc.)
- Evacuation (assembly points, accounting for personnel, contractors, visitors)
- Rescue, first aid and casualty clearance
- Communications, both inside the facility (messengers) and outside.

Therefore, given that industrial emergency plans contain a generally defined set of functions, one can create a structural and functional model of the emergency response system established by the plan. This step helps to identify the main features of industrial emergency plans by using a process modelling method to create a structural-functional method of a plan. Furthermore, the use of a structural-functional model enhances a modular approach in the analysis of the plan, which can help in managing the complexity of complex real world systems, such as emergency plans [21].

In order to create a generic, structural and functional model of the industrial emergency response mechanism, the FIS (Functions-Interactions-Structure) modelling approach is used in this paper. FIS is a hierarchic process modelling method designed for systematic risk analysis. It is based on the representation of every system as a set of interacting processes, each process being modelled using the process model diagram in fig. 1. XRISK is a software tool developed for carrying out structural-functional modelling and risk analysis [22].

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"*. 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. [21].

The system's role in terms of its objective constitutes its functions. Outputs are elements or effects generated by the system, while inputs are elements or effects used by the process to produce the outputs. Outputs and inputs are associated with a physical flow (energy, information, material) or action. [21].

Resources include all the elements that can be individually defined and are used to carry out the activity defined in the process. Each input is transformed to one or more resources inside the function, and each resource can be transformed to one output, thus creating input-resource-output chains inside every function. In the FIS approach, four categories of resources are identified [23]:

- technical resources: technical assets, such as devices or consumables;
- human resources: people/manpower;
- organisational resources: methods or procedures, i.e. elements that designate the way of performing tasks;
- informational resources: data, that are relevant to the operation and are organised in such a way so as to highlight their significance and facilitate their transmission and use.

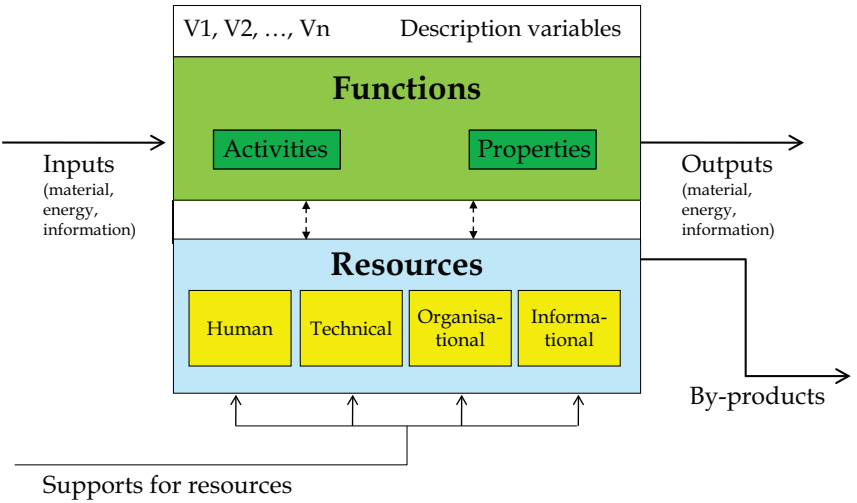

Figure 1: Process model diagram in the FIS method (adapted from Flaus [23]).

Any system that requires analysis in further detail can be decomposed into sub-systems. Each function of the parent system is then associated to one sub-system. Therefore, the system can be broken down into less abstract components. These components can 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 [24].

2.2 Industrial emergency plan model

By analysing the above mentioned references (paragraph 2.1) and a number of existing industrial emergency plans, an industrial emergency plan generic, structural and functional model of an industrial emergency plan can be built using the FIS modelling approach. As such, it will be a formal representation of the plan as a system and will form the base upon which this methodology is based.

The analysis of the robustness of the plan is based on the identification of potential failures of the emergency plan through a combination of an *a priori* and an *a posteriori* analysis. The *a priori* analysis of emergency plans rests upon the identification of potential failures through an examination of the plan model at resource and function levels. A failure of one or more resources of a function can result directly to the failure of that function. A fault tree, representing the logical combination of events that can lead to function failure, is built for each function. The failures of the resources of the function are the base events of the function's fault tree. Furthermore, the failure of a resource is often a direct result of the failure of one or more of this resource's support functions. Hence, a fault tree, representing the logical combination of events that can lead to resource failure, is

built for each resource. The base events of this fault tree are the failures of the resource's support functions. The *a posteriori* analysis is used to enhance the *a priori* analysis, by updating the model and identifying further failures or critical points.

The structural-functional industrial emergency plan model can be enhanced through lessons learned by past emergencies and emergency response exercises. Experience feedback related to emergency management in general is based on after action reports (AARs) that are compiled by the incident commander at the end of the mission. These reports usually contain a brief narrative of the operation, followed by a commentary on features of the action that worked well, elements that did not and suggestions for improvement. This information is then used at higher command echelons to improve the doctrine, operational methods and techniques.

The a priori and a posteriori analyses results are used to support a risk-based approach for the assessment of robustness of industrial emergency plans, as described in the next section.

2.3 Evaluation of the robustness of functions

The evaluation of the robustness of the emergency plan follows a risk analysis approach, in which the criticality of the failure of each function is estimated through the probability of failure and its severity.

Experience feedback can reveal elements of a plan that are effective and others that are not, thus highlighting the need for an improvement of the plan. Further analysis of lessons learned can offer valuable insight to what enhancements may be necessary. The process of experience feedback identifies failures that have already occurred but does not allow a systemic and exhaustive analysis of emergency plans [25, 26]. In this methodology, experience feedback is used to identify possible failures in the emergency plan.

The probability of failure of each function is estimated in terms of a failure probability class from the failure probability of the function's resources through the use of the function fault tree. In turn, the probability of failure of each resource is evaluated (also in terms of a failure probability calls) from the failure probability of the resource's supports through the use of the resource fault tree. A number of assessment questions are assigned to each base or intermediate event in the resource fault tree. The probability class of each event is estimated through the answers to these questions. Evaluation questions have already been used as a means of assessment of emergency plans [27].

The evaluation of the severity of the failure of each function is based on the worst-case scenario rule, i.e. the maximum damage that can be caused by the failure of this function. Thus, in order to define the severity of a function's failure, one must follow the interactions defined in the FIS industrial emergency plan model arborescence and identify the hazardous events that can result from this failure. Each hazardous event corresponds to the failure of one output of the global emergency plan system, and can thus be directly associated to one hazard study scenario of the facility. The maximum severity can hence be estimated through the associated safety report scenario and the severity scale defined in

relevant industrial safety regulations. If one function has more than one failure modes, each one is associated to one safety report scenario. In this case, the worst-case scenario is attributed to the function.

Finally, the criticality of the failure of the plan's functions is obtained by aggregation of the probability and severity of their failure modes. The scenarios can be classified on a risk analysis matrix.

In this section a methodology for the analysis of the robustness of industrial emergency plans, based on an iterative model of their functions and potential failures, has been described. The next section will present a part of the application of this methodology in the case of the Internal Emergency Plan.

3 Results

3.1 Industrial internal emergency plan model

A number of emergency planning guides (as referenced in section 2.1) and 4 existing industrial emergency plans have been consulted in order to build the Industrial Major Accident Response structural-functional model using the FIS approach. Under this model, 3 main systems have been identified (fig. 2):

- ENVIRONMENT: This system represents the physical environment of the facility, including the people, property and natural environment around the facility. The environment in this sense plays a critical role in emergency management, as it defines the theatre of emergency operations.

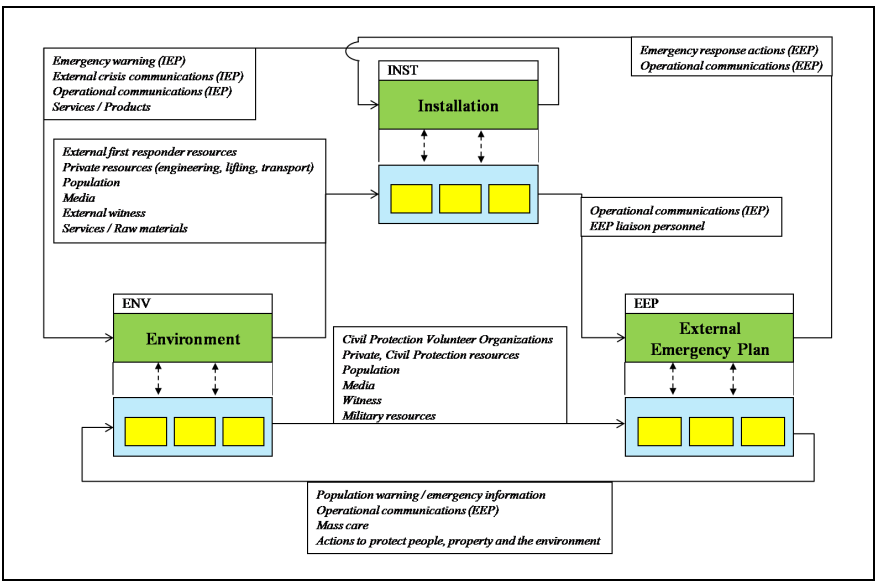

Figure 2: Industrial accidents response system structural-functional model.

- EXTERNAL EMERGENCY PLAN: This system represents the civil protection mechanism put in place in order to respond to emergencies originating from the facility.
- INSTALLATION: This system corresponds to the industrial facility itself. In this sense, its primary objective is the production of chemical substances. It is decomposed in two subsystems: PRODUCTION SYSTEMS, representing the production activities of the facility, and INTERNAL EMERGENCY PLAN, representing the internal industrial accidents response system of the facility.

In this paper, the discussion will focus (for simplicity of presentation) on the Internal Emergency Plan system. The INTERNAL EMERGENCY PLAN system is decomposed into 5 systems, each describing one main function (fig. 3):

INCIDENT SURVEILLANCE: This system corresponds to the detection of the occurrence of a hazardous event, by either a technical system (such as a monitoring device) or a person (such as facility workers or bystanders).

- EMERGENCY ACTIONS: This system corresponds to the emergency actions taken by on-site personnel to protect themselves from and/or remedy against the hazardous event. This may include simple actions aimed at avoiding the propagation of the accident or at self-protection.
- ACTIVATE EMERGENCY RESPONSE MECHANISM: This system represents the alert and mobilisation phase of the plan. It defines the available and on-site resources that are to be used for emergency response and includes the emergency warning issued within the entire facility area.

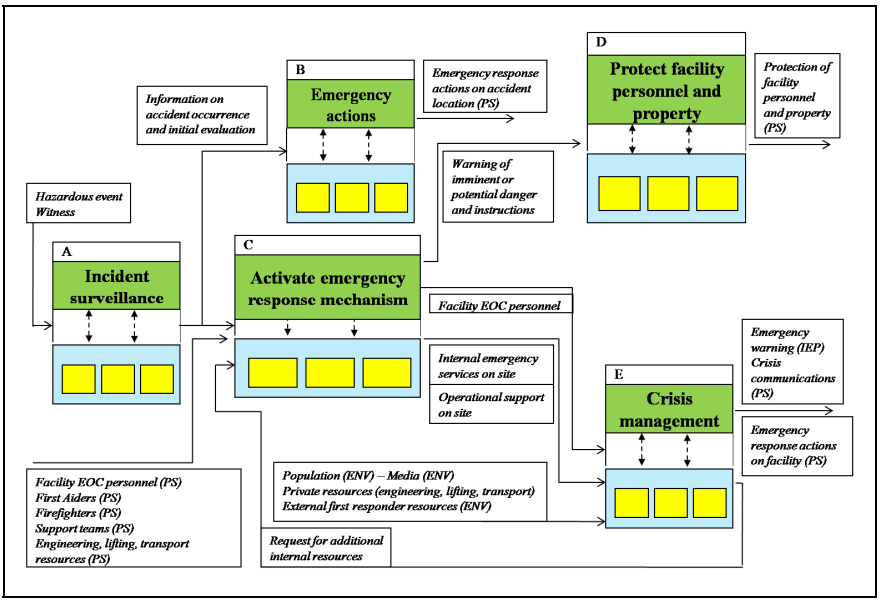

Figure 3: Industrial internal emergency plan structural-functional model.

- PROTECT FACILITY PERSONNEL AND PROPERTY: This system involves all actions taken by facility personnel (including subcontractors) and visitors to protect themselves from the adverse effects of the accident. Depending on the accident speed of onset, anticipated duration of exposure and estimated severity, evacuation or shelter-in-place may be chosen.
- CRISIS MANAGEMENT: This system corresponds to the function of the internal emergency response system. It includes activities such as internal emergency operations, communications and record keeping.

Overall, the model includes five generations of systems. At the lowest level of decomposition, the model is composed of 26 functions and more than 160 resources.

3.2 Experience feedback

In this paper, the identification of failures is based on the analysis of accident and exercise reports and on lessons learned as a result of the direct observation of a number of industrial emergency response exercises.

The ARIA database (Analysis, Research and Information on Accidents) of the French Ministry of Ecology, Energy, Sustainable Development and the Sea has been the main source of information for accident reports. A total of some 160 accident reports have been analysed. Furthermore, 29 internal and 3 external emergency plan exercises have been followed from January 2008 to May 2010. A total of 119 failures have been identified in internal emergency plans. They have been classified in order to highlight the function, resource(s) and support function(s) involved. Their cumulative frequencies are shown in figure 4.

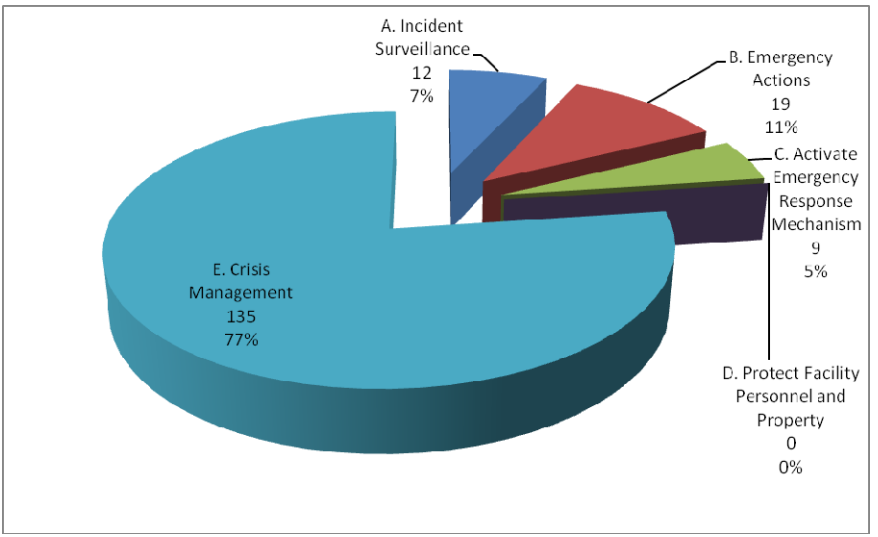

Figure 4: Industrial internal emergency response systems' failures.

3.3 Example: calculation of the criticality for a failure of a function

The critical points identified by the above analysis are used to validate the fault trees of each function and resource, each fault tree representing the logical combination of events that can lead to function or resource failure. The fault tree of the system E2: DIRECTION OF INTERNAL EMERGENCY OPERATIONS (which is a sub-system of E: CRISIS MANAGEMENT) is illustrated in fig. 5 as an example. The base events of this fault tree are the failures of the resources assigned to this function. Further fault trees are built for each one of these resources. The top event of each resource fault trees is the same as one of the base events of the function fault tree. Hence, function and resource fault trees can be assembled to form the complete fault tree of the function and its resources.

One or more assessment questions are generated after each base or intermediate event of the function's fault tree. The answer to each question is used to assign a probability class to each event. The fault tree is then used to calculate the probability class of the resource and function failures [28].

With regard to the severity of the E2 function, the latter interacts with all other sub-systems of the E: CRISIS MANAGEMENT system. Thus, its failure can cause this system to fail. The maximum severity is hence estimated by the highest damage that can be caused by the most hazardous event identified in the safety report of the facility. The criticality of failure of the function is hence obtained by the conjunction of the failure probability and severity.

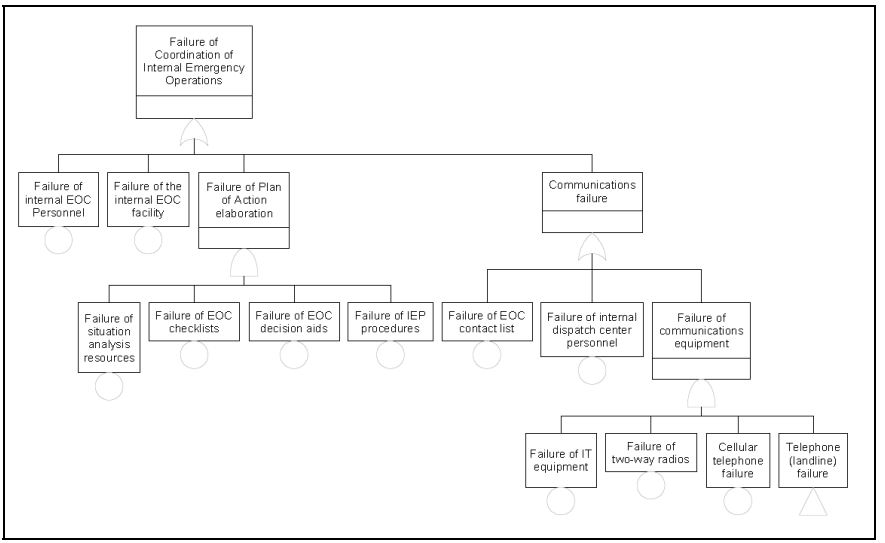

Figure 5: Fault tree for E2: coordination of internal emergency operations.

4 Conclusion

This paper has presented a model-driven and risk-based approach for the evaluation of the robustness of industrial emergency plans. The approach uses a structural-functional model to describe the emergency plan and identify potential failures through lessons learned from past accidents and exercises. These failures are then used to validate fault trees of the functions and resources of the plan and estimate the probability of failure of the functions. The severity of each function is based on the safety report scenarios and the worst-case principle. A semi-quantitative expression of the risk of failure can be estimated for each function. This method is a toolbox that can be used both during the planning phase but also for the evaluation of existing plans.

References

[1] Federal Emergency Management Agency, *Developing and Maintaining State, Territorial, Tribal and Local Government Emergency Plans*: 2009.

[2] Fédération Nationale des Sapeurs-Pompiers Français, *Guide d'Intervention face au Risque Chimique* (French) : 2002

[3] Mannan, S., *Lees' Loss Prevention in the Process Management, 3rd ed., Volume 2*, Elsevier (Butterworth-Heinemann): Oxford, 2005.

[4] Jackson, B., *The problem of measuring emergency preparedness – The need for assessing "response reliability" as part of homeland security planning*, Rand Corporation: 2008.

[5] Alexander, D., Towards the development of a standard in emergency planning. *Disaster Prevention and Management*, **14(2005)**, pp. 158-175, 2005.

[6] Kanno, T., Furuta, K., resilience of Emergency Response Systems. 2nd Symposium on Resilience Engineering: Juan-les-Pins, France

[7] Mayer, H., *First Responder Readiness: A systems approach to readiness assessment using model based vulnerability analysis techniques*, Master thesis, U.S. Naval Postgraduate School: 2005.

[8] Pavard, B., Dugdale, J., Saoud, N.B., Darcy, S., Salembier, P., Design of robust socio-technical systems, *2nd Symposium on Resilience Engineering*: Juan-les-Pins, France, 2006.

[9] Federal Emergency Management Agency, *Guide for All-Hazard Emergency Operations Planning, State and Local Guide 101*: 1996

[10] U.S. National Fire Protection Association, *Standard on Disaster/Emergency Management and Business Continuity Programs, NFPA 1600*: 2007

[11] Direction de la Défense et de la Sécurité Civiles, *Guide ORSEC Départemental – Méthode Générale, Tome G.1* (French) : Paris, 2006

[12] International Federation of Red Cross and Red Crescent Societies, *Disaster Response and Contingency Planning Guide*: Geneva, 2007

[13] Alexander, D., *Principles of emergency planning and management*, Terra Publishing: Hertfordshire, 2002

[14] U.S. National Response Team, *Hazardous Materials Emergency Planning Guide*: Washington, D.C., 2001
[15] Federal Emergency Management Agency, *Guidelines for HazMat/WMD Response, Planning and Prevention Training*: 2003
[16] Direction de la Défense et de la Sécurité Civiles, *Guide ORSEC Départemental – Disposition Spécifique – Plan Particulier d'Intervention (PPI), Guide, Tome S.1.2* (French) : Paris, 2007
[17] Federal Emergency Management Agency, *Emergency Management Guide for Business and Industry*: 1993.
[18] Direction de la Défense et de la Sécurité Civiles, *Guide d'Elaboration d'un Plan d'Opération Interne* (French): Paris, 1985.
[19] 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* (French): Paris, 1996.
[20] 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* (French): Paris, 2001.
[21] Flaus, J.M., A model-based approach for systematic risk analysis, *Proc. IMechE*, **222(2008)**, pp.79-93
[22] XRISK, http://www.xrisk.fr
[23] Flaus, J.M., *Méthodologie FISE* (French), internal document Institut National Polytechnique de Grenoble: Grenoble, 2007
[24] Baiardi, F., Telmon, C., Sgandurra, D., Hierarchical, model-based risk assessment of critical infrastructures, *Reliability Engineering and Systems Safety*, **64(2009)**, pp.1403-1415.
[25] U.S. White House, *The Federal Response to Hurricane Katrina – Lessons Learned*: 2006
[26] U.S. House of Representatives, *A Failure of Initiative – Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*: 2006
[27] Larken, J., Shannon, H., Strutt, J.E., Jones, B., *Performance indicators for the assessment of emergency preparedness in major accident hazards*, U.K. Health and Safety Executive, 2001.
[28] Union des Industries Chimiques, *Les cahiers de sécurité, cahier n°3 : L'analyse par arbre des causes* (French): Paris, 1981