Méthodologie pour l'analyse de robustesse des plans de secours industriels

Georgios-Marios Karagiannis, Eric Piatyszek, Jean-Marie Flaus

LM17_COMM_021_Georges_KARAGIANNIS_100506.docx

Méthodologie pour l'analyse de robustesse des plans de secours industriels

Georgios-Marios KARAGIANNIS et Eric PIATYSZEK
Ecole Nationale Supérieure des Mines de Saint-Etienne
158, cours Fauriel, 42023 Saint-Etienne cedex 02
Tél : +33 (0)4 77 42 66 67
Fax : +33 (0)4 77 42 66 33
E-mail : karagiannis@emse.fr

Jean-Marie FLAUS
Institut National Polytechnique de Grenoble
46, avenue Félix Viallet, 38031 Grenoble
Tél : +33 (0)4 76 82 62 29

Résumé

L'objectif de cette communication est de présenter une méthodologie pour l'analyse de la robustesse des plans de secours industriels. La robustesse est définie en termes de la capacité du dispositif de gestion de crise de répondre aux besoins opérationnels en mode dégradé. Le retour d'expérience effectué sur les accidents industriels est une source d'informations importante pour l'analyse des plans de secours, mais ne permet pas une analyse intégrée du dispositif de gestion de crise. La méthodologie utilisée repose sur une formalisation générique des plans de secours industriels à l'aide d'un modèle structurel et fonctionnel, décrivant à la fois les fonctions et les ressources permettant la réalisation de ces fonctions. Ce modèle permet par la suite de structurer l'analyse des dysfonctionnements pouvant se manifester lors de la mise en œuvre des plans. De plus, ce travail s'est accompagné de retours d'expérience à partir de 159 rapports d'accidents et de 31 exercices POI/PPI, qui ont permis d'identifier des défaillances pouvant survenir lors de la mise en œuvre des POI/PPI. Cette analyse est ainsi basée d'une part sur les retours d'expérience et d'autre part sur une analyse critique du modèle structurel et fonctionnel des plans. L'analyse de la robustesse est basée sur une évaluation du risque de défaillance des fonctions du plan. La probabilité de défaillance est estimée à partir des questions d'évaluation et des arbres de défaillances des ressources et des fonctions. La gravité de la défaillance de chaque fonction est déterminée en utilisant les études de danger, suivant la règle des dommages maximum qu'elle peut provoquer. Cette méthodologie constitue ainsi une boite à outils qui peut être utilisée à la fois pour l'évaluation des plans existants, mais aussi pour l'élaboration du dispositif défini dans un plan de secours industriel.

Summary

The objective of this paper is to present a methodology for the analysis of the robustness of industrial emergency plans. Robustness is defined in terms of the capacity of the emergency response mechanism to respond to operational needs under deteriorated conditions. Experience feedback on industrial accidents is a significant information source for the analysis of emergency plans, but does not allow for an integrated analysis of the emergency management mechanism. The methodology used in this paper is based on a generic formalization of industrial emergency plans through a structural and functional model, describing both the functions and the resources that allow the functions to be accomplished. This model is subsequently used to structure the analysis of failures that can occur during the application of these plans. Furthermore, this work has been enhanced by a lessons learned by 159 accident reports and 31 internal emergency plan exercises, that have allowed to identify failures that can occur during the application of industrial internal or external emergency plans. This analysis is hence based on one side lessons learned and on the other on a critical analysis of the structural-functional model of the plans. The analysis of robustness is based on the assessment of the risk of failure of the plan's functions. The failure probability is estimated through assessment questions and the use of function and resource fault trees. The severity of each function failure is determined by using the installation's hazard studies, and by applying the rule of maximum damage that this failure can cause. This methodology is hence a tool box that can be used both for the assessment of existing plans, but also for the development of the mechanism defined in an industrial emergency plan.

Introduction

La directive 96/82/CE de l'Union Européenne, dite « Seveso II », et la législation française des Installations Classées pour la Protection de l'Environnement (I.C.P.E.) et le Code Minier pour les stockages souterrains définissent le cadre de la gestion des risques industriels chimiques en Union Européenne et en France respectivement. Un certain nombre de mesures est préconisé aux services de l'Etat et aux exploitants, comprenant entre autres la mise en place des systèmes de gestion de la sécurité, des plans de secours, des mesures d'aménagement du territoire, la rédaction des rapports d'accidents et des inspections de sécurité. Les plans de secours industriels sont les Plans d'Opération Internes (POI) pour l'exploitant et les Plans Particuliers d'Intervention (PPI), annexés au dispositif ORSEC (Organisation de la Réponse de la Sécurité Civile), pour les autorités préfectorales. Les objectifs de ces deux plans sont la limitation des effets de l'incident, la protection des personnes, des biens et

de l'environnement, la communication vers le public et les autorités, et la prise des mesures pour le retour à la normale suivant un accident (par exemple la dépollution). Les exploitants et les autorités préfectorales sont obligés de mettre en œuvre ces plans sans retard si un accident industriel majeur survient ou est raisonnablement anticipé.

L'objectif de cette communication est de présenter une méthodologie pour l'analyse de la robustesse des plans de secours industriels. En effet, les plans d'urgence peuvent présenter des dysfonctionnements, comme par exemple l'absence du personnel indispensable ou la défaillance des équipements techniques. Cette approche est basée sur une analyse a priori de ces défaillances en utilisant un modèle fonctionnel et structurel du dispositif d'intervention d'urgence mis en place par le plan. Cette analyse est par la suite confirmée ou modifiée avec des informations obtenues par des retours d'expérience sur des accidents industriels déjà survenus.

Cet article est organisé de la manière suivante : la méthodologie utilisée afin de modéliser les plans de secours et analyser par la suite la robustesse des fonctions de ces plans est présentée dans la partie suivante. La suite présente les résultats de ce travail, notamment le modèle structuro-fonctionnel d'un Plan d'Opération Interne, le retour d'expérience utilisée pour l'analyse et le calcul de la robustesse d'une fonction comme exemple.

Méthodologie de modélisation itérative des plans de secours industriels et de leurs fonctions

1. Robustesse des plans de secours industriels

Il n'existe pas une définition généralisée de la robustesse, et ce terme est difficilement appréhendé à cause de sa relation avec la résilience et la stabilité. La robustesse est intuitivement définie comme la capacité d'un système d'adapter son comportement à des situations imprévues, comme par exemple une perturbation dans l'environnement, ou des dysfonctionnements dans l'organisation du système (Pavard et al. 2006). Cette définition ne met pas en évidence la différence entre les notions de robustesse et résilience. La résilience représente la capacité d'un environnement physique ou biologique, une société, une organisation ou une personne à traverser une expérience stressante, en minimisant son impact ou en utilisant l'adversité pour améliorer son organisation (Harding et al. 2001). Wybo (2008) définit la résilience comme la capacité d'une organisation (à tout niveau) de poursuivre l'accomplissement de ses taches en adaptant son fonctionnement à des situations dangereuses, l'incertitude, la pression du temps et les menaces. La robustesse est définie comme la capacité d'une organisation de survivre et rester en contrôle par l'émergence de nouveaux modes organisationnels.

Dans le cadre du dispositif d'intervention d'urgence face à un accident industriel majeur, la robustesse peut être définie comme la capacité du dispositif de maintenir un niveau de réponse opérationnelle efficace (c'est-à-dire de survivre et rester en contrôle de la situation d'urgence) en situation dégradée des moyens d'intervention ou lors de la survenue d'un scénario s'écartant de ce qui a été prévu. Une telle situation peut se produire par exemple à cause d'une défaillance des ressources techniques nécessaires aux opérations d'urgence, du manque de compétence des personnels d'intervention ou des problèmes inhérents aux procédures d'intervention elles-mêmes. La robustesse peut donc être définie comme l'efficacité du dispositif industriel d'intervention d'urgence ou sa capacité de performance selon le plan en situation dégradée.

Dans cette étude nous nous sommes intéressés dans un premier temps à la première composante de la robustesse (situation dégradée des moyens d'intervention). Afin d'étudier la robustesse des plans de secours industriels, une méthode de modélisation de processus sera utilisée. Cette méthode permet d'identifier les fonctions du plan et les ressources associées. Ce modèle est ensuite utilisé pour structurer le retour d'expérience (REX). Cette approche permet d'analyser les points critiques dans la mise en œuvre des plans et fait l'objet de la section suivante.

2. Méthodologie FIS

Les plans de secours industriels sont souvent formalisés par des diagrammes de flux, ce qui rend leur appréhension plus facile (Ramsay 1999). Cette représentation est assez didactique, mais elle n'indique pas les aspects opérationnels et tactiques du dispositif mis en place par le plan, les ressources utilisées pour accomplir chaque fonction ou les interactions entre ces fonctions. En revanche, un modèle structurel et fonctionnel du plan de secours industriel peut mettre en évidence tous ces aspects.

Un autre avantage de ce type d'analyse est qu'un modèle fonctionnel permet de représenter chaque fonction comme une entité distincte. Des ressources, des interactions et d'autres attributs sont associés à la fonction, afin de compléter sa représentation. Des « paquets » ou « briques »comprenant la fonction, ses ressources et ses interactions sont ainsi créés pour chaque fonction. L'intégralité du plan peut ainsi être représentée comme un assemblage de ces « paquets ». Cette approche modulaire augmente la flexibilité de l'analyse et permet de se focaliser sur des parties spécifiques du plan sans pour autant perdre le degré de détail de la totalité du modèle.

Enfin, la modélisation fonctionnelle du plan de secours industriel permet de décomposer de manière structurelle le système complexe en sous-systèmes autonomes et indépendamment fonctionnels. La complexité inhérente dans les systèmes réels, comme les plans de secours industriels, peut être gérée par une approche de modélisation hiérarchique dans l'évaluation des risques (Flaus 2008). Dans une telle approche, des modèles de plus en plus détaillés peuvent être créés en décomposant de manière structurelle le système en des parties moins abstraites. Ces composants peuvent alors être analysés séparément, tout en tenant compte du modèle global du système étudié. Ceci permet d'augmenter le niveau de détail de l'analyse et faire des économies d'échelle dans le temps d'analyse (Baiardi et al. 2009).

La décomposition ne doit pas être l'objectif du travail, sinon ce dernier risque de devenir une perte d'énergie. Le temps et les ressources nécessaires pour décomposer tous les sous-systèmes d'un système jusqu'au niveau élémentaire peuvent rapidement dépasser les capacités de l'analyste. En revanche, l'abstraction favorise la flexibilité, la complétude et l'exactitude dans l'analyse. Les coûts et bénéfices de la décomposition structurelle peuvent être équilibrés à travers une abstraction partielle. L'analyste peut sélectionner un niveau d'abstraction, et ainsi mettre en évidence seulement les détails nécessaires. En ne décomposant que les sous-systèmes nécessaires d'un système plus grand, l'analyste peut focaliser son attention sur les aspects nécessaires à l'investigation (Simon 1981).

Dans le cadre de ce travail de recherche, la méthode FIS (Fonctions-Interactions-Structure) est utilisée pour créer un modèle structuro-fonctionnel des plans de secours industriels. La méthode FIS est une méthode de modélisation hiérarchique de processus destinée à l'analyse des risques. Elle est basée sur l'approche SIPOC (Supplier-Input-Process-Output-Customers), qu'elle étend, en ce qui concerne d'une part les relations interprocessus qui sont décrites d'un point de vue à la fois fonctionnel et matériel, et d'autre part la structure interne du processus pour lequel on analyse ses fonctions et les ressources utilisées pour réaliser ces fonctions (Flaus 2007). La méthode FIS permet de décrire les fonctions réalisées sous forme des séquences d'activités, ainsi que leur enchainement. Chaque système est représenté sous la forme de la fig. 1. XRISK est un outil informatique développé pour la modélisation structuro-fonctionnelle et l'analyse des risques en utilisant la méthode FIS (http://www.xrisk.fr).

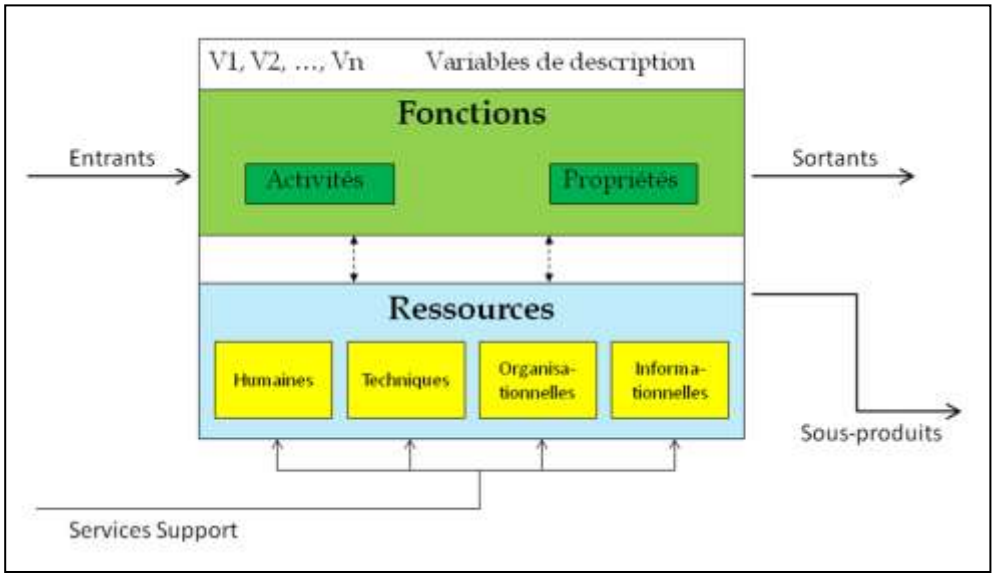

Figure 1 : Modélisation FIS d'un système (adapté depuis Flaus 2007)

Un processus est défini dans la norme ISO9001 comme un système organisé d'activités qui utilise des ressources (personnels, équipement, matériels, et machines, matières premières et informations) pour transformer des éléments entrants en éléments de sortie dont le résultat final attendu est un produit. Les fonctions d'un système sont le rôle d'un système exprimé en termes de finalités. Les sortants sont des éléments physiques ou des effets générés par le processus, tandis que les entrants sont des éléments utilisés par le processus. Notamment, les entrants sont analysés en identifiant les services (fonctions) requis par le processus et fournis par les autres processus. Les sortants et les entrants sont matérialisés par des flux physiques ou des actions et peuvent être définis sous forme de matière, d'énergie ou d'information (Flaus 2007).

Les ressources comportent tous les éléments qui peuvent être définis de manière individuelle et sont utilisés pour accomplir l'activité définie dans le processus. Chaque entrant se transforme en une ou plusieurs ressources dans la fonction et chaque ressource peut être associée à un sortant, constituant ainsi des chaines entrant-ressource-sortant à l'intérieur de chaque fonction. Dans le cadre de la méthode FIS, les ressources sont classées en ressources humaines, techniques,

organisationnelles et informationnelles. Les ressources humaines correspondent aux acteurs humains. Les ressources techniques sont les équipements utilisés par les acteurs humains ou activées automatiquement. Les ressources organisationnelles représentent les démarches devant être suivies par le dispositif afin que la mission soit accomplie. Les ressources informationnelles sont les données pertinentes pour l'opération qui sont organisées de manière à mettre en évidence leur importance et rendre leur transmission et utilisation plus faciles. Les supports des ressources sont des entrants (services) requis pour faire en sorte que les ressources soient en état de fonctionnement (Flaus 2008).

Lorsqu'un système est trop complexe, chaque fonction peut être associée à un sous-système et décomposée en sous-fonctions et étapes. Chaque sous-fonction peut par la suite être de nouveau associée à un sous-système et décomposée. Ainsi peuvent être effectués autant de degrés de décomposition que l'analyse du système le nécessite. L'ambigüité dans l'activité ou la propriété de la fonction diminue de la fonction vers l'étape : la fonction est plus abstraite que la sous-fonction, et cette dernière plus abstraite que l'étape.

La modélisation est itérative : le modèle structuro-fonctionnel du plan peut être enrichi en ajoutant des éléments nouveaux. Une nouvelle fonction ou ressource, ou un nouveau mode de défaillance peut être ajouté une fois identifié par les activités de recherche ou le retour d'expérience.

3. Retour d'expérience des plans de secours industriels

Le retour d'expérience est une activité primordiale dans l'amélioration des plans de secours et du dispositif d'intervention d'urgence en général. Il est basé sur des rapports qui suivent chaque exercice ou incident nécessitant l'activation du dispositif d'intervention d'urgence. Ces rapports comportent un narratif succinct de l'opération, accompagné d'un exposé sur les éléments de l'action qui ont bien ou mal fonctionné et des propositions d'amélioration. Ces informations sont ensuite utilisées par la hiérarchie afin de faire évoluer la doctrine, les méthodes et les techniques opérationnelles.

Le retour d'expérience peut mettre en évidence des aspects du plan qui sont plus ou moins efficaces ou qui nécessiteraient des modifications. Une analyse approfondie peut même révéler quelles modifications sont nécessaires. Le processus du retour d'expérience identifie des défaillances déjà survenues mais ne permet pas une analyse systémique et exhaustive des plans d'urgence (Jackson 2008, Lagadec 2007). Plusieurs auteurs ont déjà souligné le besoin d'une analyse systémique des plans de secours industriels (Alexander 2002 & 2008, Mayer 2005, Kanno et al. 2006, Jackson 2008). Dans le cadre de cette méthodologie, le modèle structuro-fonctionnel du plan de secours industriel est utilisé pour structurer et valoriser le retour d'expérience. En retour, le retour d'expérience enrichit le modèle et permet d'identifier des défaillances potentielles du dispositif de gestion de crise.

Les défaillances identifiées par le retour d'expérience et le modèle structuro-fonctionnel sont analysées en utilisant des méthodes d'analyse des risques comme les arbres de défaillances ou l'Analyse des Modes de Défaillance, de Leurs Effets et de leur Criticité (AMDEC) (U.S. DOD 1980, Villemeur 1988). Dans le cadre de ce travail, le retour d'expérience est directement associé aux fonctions du plan (identifiées dans le modèle FIS), ce qui facilite son intégration dans les plans futurs mais aussi son utilisation pour l'analyse des plans existants. Cette approche permet de prendre en compte la propagation des défaillances à travers les fonctions du dispositif de gestion de crise, mais aussi d'intégrer les analyses a priori et a posteriori des plans, comme ceci est décrit sur le paragraphe suivant.

4. Analyse de robustesse des fonctions du plan

La méthode d'analyse de la robustesse repose sur une évolution itérative d'un modèle de base. Un modèle structurel, fonctionnel et générique de base est construit pour le plan de secours, en utilisant des guides de planification et des plans existants. Ce modèle de base peut être progressivement amélioré comme le retour d'expérience, la recherche ou la réflexion critique mettent en évidence de nouvelles défaillances, fonctions ou ressources. Ce processus est itératif et suit le principe de la roue de l'amélioration continue (Deming 1986). L'objectif est d'avoir un modèle qui représente au mieux possible la situation, en ajoutant de nouveaux éléments ou modifiant les existants, afin d'adapter le modèle à des nouveaux informations. Les changements sont toujours suivis d'une validation de la nouvelle version du modèle.

Une fois le modèle mis en place, le processus d'identification des défaillances est mis en route. Ce processus est basé sur une analyse a priori et a posteriori du plan de secours. L'objectif de l'analyse a priori est d'identifier des défaillances potentielles à partir d'un examen du modèle aux niveaux des fonctions et des ressources. Les défaillances des fonctions du plan peuvent être provoquées par les défaillances d'une ou plusieurs ressources. Afin d'analyser les dysfonctionnements potentiels des fonctions définies dans le modèle FIS, un arbre de défaillance local à la fonction est automatiquement généré à partir du modèle de chaque fonction, représentant la combinaison logique des défauts de ressources pouvant conduire à sa défaillance. Les événements de base de cet arbre sont les défaillances des ressources de cette fonction. Les défaillances des ressources résultent de la défaillance des fonctions les produisant ou la défaillance de leurs fonctions supports respectives. Un arbre de défaillance local à la ressource est ainsi bâti représentant la combinaison logique des événements qui, sous certaines conditions, peuvent rendre la ressource défaillante. Les événements au sommet de chaque arbre de défaillance de ressource

sont les événements de base de l'arbre de défaillance de la fonction, tandis que les événements de base sont les défaillances des supports de cette ressource. Cette analyse est affinée par le retour d'expérience qui constitue l'analyse a posteriori. Le REX est utilisé pour mettre à jour le modèle et identifier des défaillances ou points critiques potentiels qui auraient pu être manqués par l'analyse a priori, qui sont réintroduits dans le modèle initial FIS, de façon itérative.

De façon à générer et maintenir un outil d'audit de plan, à chaque événement des arbres de défaillances sont associées une ou plusieurs questions (Larken et al. 2001). Chaque question comporte une interrogation concernant les attributs du dispositif POI/PPI permettant d'éviter l'occurrence de la défaillance étudiée. Un nombre prédéfini de points est associé à chaque réponse des questions. Une fois toutes les questions correspondant au même événement répondues, les points sont ajoutés pour obtenir un score total, Un tableau de conversion permet enfin de transformer les scores en classes de probabilité de l'événement étudié. Les classes de probabilité sont celles utilisées dans *l'arrêté du 29 septembre 2005 relatif à l'évaluation et à la prise en compte de la probabilité d'occurrence, de la cinétique, de l'intensité des effets et de la gravité des conséquences des accidents potentiels dans les études de dangers des installations classées soumises à autorisation*. A partir des classes de probabilité des événements de base de l'arbre de défaillance de la ressource et en utilisant les règles d'exploitation semi-quantitative des arbres de défaillance (UIC 1981) le taux de défaillance de la ressource est calculé. Ce taux de défaillance permet ensuite de calculer le taux de défaillance de la fonction par la même méthode.

L'estimation de la gravité des modes de défaillances des fonctions est basée sur le principe de l'évaluation de la gravité maximale de l'impact des défaillances. Ainsi, afin de définir la gravité de la défaillance d'une fonction, l'utilisateur devra suivre les interactions définies dans l'arborescence du modèle FIS du plan de secours afin d'identifier le(s) événement(s) non souhaité(s) pouvant résulter de cette défaillance. Chacun de ces événements correspond à la défaillance d'un sortant du système qui représente le plan de secours dans sa globalité, et peut ainsi être directement associé à un scénario de l'étude de danger de l'installation. La gravité maximale d'un événement peut par conséquent être estimée à partir de la gravité du scénario de l'étude de dangers associée et l'échelle de gravité définie dans l'*arrêté du 29 septembre 2005 relatif à l'évaluation et à la prise en compte de la probabilité d'occurrence, de la cinétique, de l'intensité des effets et de la gravité des conséquences des accidents potentiels dans les études de dangers des installations classées soumises à autorisation*. Si une fonction présente plusieurs modes de défaillance, chacun est associé à un scénario du POI/PPI ou de l'étude de danger. Dans ce cas, le scénario ayant les conséquences les plus graves sera sélectionné et la gravité correspondante attribuée à la défaillance de la fonction étudiée.

La criticité des défaillances des différentes fonctions du plan est obtenue par agrégation de la gravité et de la probabilité de leurs modes de défaillance. Les différents scénarios peuvent être classés sur un tableau d'analyse de risque, comme le tableau dit « MMR », qui est défini dans la *circulaire du 29/09/05 relative aux critères d'appréciation de la démarche de maîtrise des risques d'accidents susceptibles de survenir dans les établissements dits « SEVESO », visés par l'arrêté du 10 mai 2000 modifié*.

Cette partie a été dédiée à la méthodologie d'analyse de la robustesse des plans de secours industriels basée sur une modélisation itérative de leurs fonctions et de leurs défaillances. La suite présentera les résultats de l'application de cette méthodologie dans le cas du Plan d'Opération Interne.

Résultats

1. Modèle structurel et fonctionnel d'un Plan d'Opération Interne

Le modèle structuro-fonctionnel du plan d'opération interne a été créé à partir de plusieurs guides de planification d'urgence (DSC 1985 & 2007, FEMA 1996, 2003 & 2009, GESIP 2001, U.S. NRT 2001) et 3 Plans d'Opération Internes des installations chimiques ou pétrochimiques existants. Trois grands systèmes sont pris en compte dans le modèle FIS de la gestion des accidents industriels majeurs (fig.2). Chacun de ces systèmes est par la suite décomposé à des sous-systèmes, selon le principe de la méthode FIS.

Le système ENVIRONNEMENT représente l'environnement du site industriel. Il comporte les personnes, les biens et l'environnement naturel situés autour du site, mais aussi les collectivités territoriales, les sites industriels avoisinants, les sociétés privées spécialisées. L'environnement va jouer un rôle important sur la gestion de la crise, en effet il définit le cadre de l'intervention, mais aussi les besoins de communications, les risques supplémentaires (par exemple une explosion provoquant un mouvement de terrain), le potentiel d'effets dominos etc.

Le système PLAN PARTICULIER D'INTERVENTION représente la disposition spécifique du dispositif opérationnel ORSEC dédiée aux accidents industriels majeurs, qui constitue ainsi la base de la réponse de la Sécurité Civile face aux accidents industriels majeurs qui dépassent ou risquent de dépasser les limites de l'installation industrielle dans laquelle ils surviennent. Cet article portant, pour des raisons de simplicité de présentation, sur le Plan d'Opération Interne, la décomposition de ce système ne sera pas présentée ici.

Le système INSTALLATION correspond au site industriel lui-même. La fonction principale de toute installation industrielle est la production des produits finis ou intermédiaires, à partir de matières premières ou d'autres produits intermédiaires. Ce système comporte deux fonctions principales, et peut ainsi être décomposé en deux sous-systèmes :

- Le sous-système SYSTEMES DE PRODUCTION, qui représente les activités de production de produits et/ou de services de l'installation. Ce système ne sera pas développé en plus de détail, vu que l'objectif de ce travail porte sur les plans de secours industriels.
- Le sous-système PLAN D'OPERATION INTERNE, qui représente le dispositif mis en place en interne d'un site industriel afin de gérer les accidents industriels majeurs.

A son tour, le système PLAN D'OPERATION INTERNE est décomposé en 5 sous-systèmes, chacun représentant une des fonctions principales d'in Plan d'Opération Interne. La structure et les interactions de ces sous-systèmes apparaissent dans la figure 3.

Le système ASSURER LA VEILLE représente la détection de la survenue d'un Evénement Non Souhaité qui a déjà ou qui peut potentiellement entrainer des dommages aux personnes, aux biens et à l'environnement (par exemple incendie ou fuite de matières dangereuses). La détection peut être effectuée par un ou plusieurs dispositifs technologiques de détection automatique (par exemple automate d'appel), par un ou plusieurs témoins humains, ou par une combinaison de ces deux.

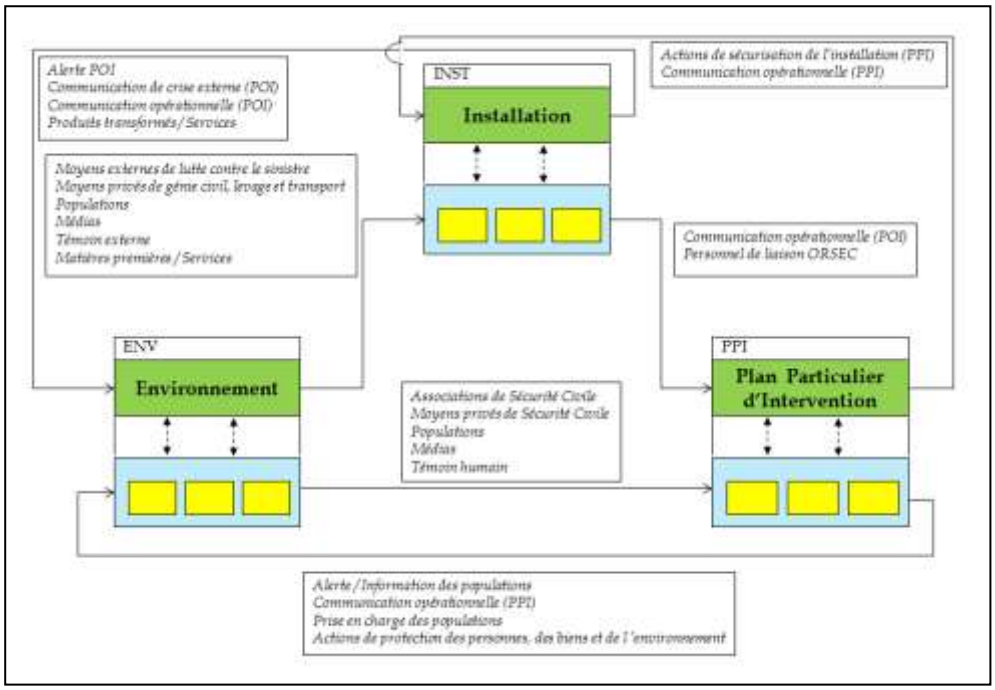

Figure 2 : Modèle structurel-fonctionnel du dispositif d'intervention d'urgence face aux accidents industriels majeurs

Une fois qu'un Evénement Non Souhaité potentiellement dangereux est identifié comme tel, les agents sur place doivent prendre les premières mesures qui visent à assurer leur propre sécurité. Cette fonction correspond au système PRENDRE LES 1ères MESURES. Ces mesures peuvent comprendre des actions simples qui visent à éviter la propagation de l'accident (par exemple, fermeture d'une vanne ou d'un circuit, extinction d'un petit foyer à l'aide des extincteurs) mais aussi une évacuation des lieux sinistrés et l'établissement d'un périmètre de sécurité autour de la zone de danger.

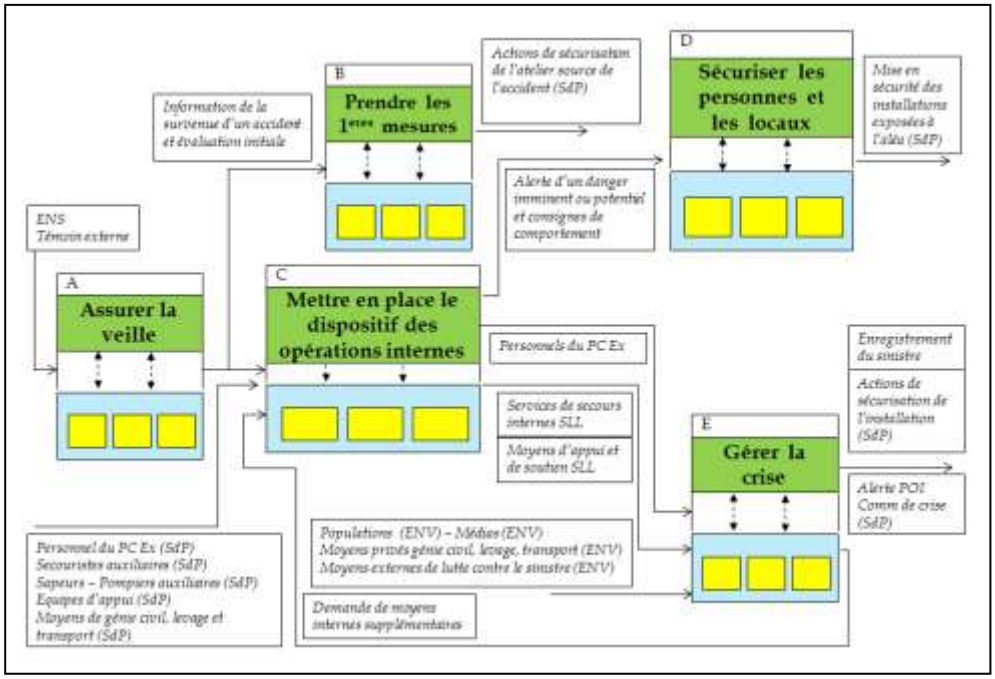

Figure 3 : Modèle structurel-fonctionnel d'un Plan d'Opération Interne

Le système METTRE EN PLACE LE DISPOSITIF DES OPERATIONS INTERNES représente la mobilisation du dispositif précisé dans le POI. Conformément aux dispositions du POI, l'appel d'urgence arrive à une structure adaptée de l'installation, et est ensuite répercuté vers les autres acteurs de gestion de crise à l'intérieur du site. C'est une fonction essentielle pour le déroulement des opérations internes. En effet elle définit les moyens qui seront mis en œuvre pour lutter contre le sinistre, pour gérer la crise, mais aussi pour l'autoprotection des personnels travaillant sur le site industriel.

La fonction de la mise en sécurité de toutes les personnes et de tous les locaux se trouvant dans la zone de danger dans le site correspond au système SECURISER LES PERSONNES ET LES LOCAUX. Les accidents industriels majeurs ont souvent une cinétique rapide et/ou des effets qui peuvent atteindre toute l'installation industrielle en quelques minutes. Il est donc prudent d'assurer la protection des personnes se trouvant dans le site immédiatement après la confirmation de l'existence d'un risque. Dans ce but, le CTA interne alerte toutes les personnes se trouvant dans la zone à risques du site et tous les locaux (ateliers, bureaux etc.) en mode réflexe, afin de les informer de la survenue d'un accident et de leur donner des consignes de comportement. Pour la plupart des cas, deux solutions sont possibles : le confinement ou l'évacuation.

Enfin, le système GERER LA CRISE représente l'ensemble des actions de gestion de l'événement en interne. Il s'agit de la fonction la plus complexe du POI. Elle comporte toutes les actions qui sont effectuées afin de lutter contre le sinistre, diriger les opérations internes, communiquer, sécuriser le site, et assurer l'enregistrement de l'incident. Le POI sert à mettre en place cette fonction en identifiant des actions à réaliser en phase réflexe, et ensuite à aider le Directeur des Opérations Internes dans sa prise de décision lors de la gestion de l'incident en interne.

Le modèle comprend au total 5 niveaux de décomposition. Au 5ème niveau de décomposition, il comporte 26 fonctions, et plus de 150 ressources humaines, techniques, organisationnelles et informationnelles. Ce modèle a été validé par des professionnels de la sécurité des sites SEVESO.

2. Retour d'expérience

L'identification des défaillances a été basée sur trois piliers : l'analyse des rapports d'accidents déjà survenus, l'analyse des rapports d'exercices POI et PPI dans des installations classées SEVESO II « seuil haut » et enfin le retour d'expérience à partir de l'observation des exercices POI et PPI. L'objectif de ce travail de recherche est d'identifier les défaillances des fonctions du plan (identifiées dans le modèle FIS).

La base de données ARIA (Analyse, Recherche et Information sur les Accidents) recense les accidents technologiques survenus dans des installations classées au titre de la législation « Installations Classées pour la Protection de

l'Environnement » et celle du transport de matières dangereuses, et ayant porté atteinte à la santé ou la sécurité publiques, l'agriculture, la nature et l'environnement. Elle a été créée et est mise à jour régulièrement par le Bureau d'Analyse des Risques et Pollutions Industrielles (BARPI) de la Direction de la Prévention des Pollutions et des Risques (DPPR) du Ministère chargé de l'environnement.

En novembre 2008, la base de données ARIA recensait plus de 32.000 accidents ou incidents survenus en France ou à l'étranger. Elle est en évolution permanente, ce qui permet de collecter un grand nombre d'informations, classées sous forme de rapports d'accidents. Des rapports courts sont publiés et accessibles sur Internet. Un nombre d'accidents (159 en novembre 2008), sélectionnés pour leur richesse en enseignements tirés, fait l'objet des rapports longs, également accessibles sur Internet. L'intégralité des rapports longs a été étudiée afin de recenser des défaillances et des points critiques pouvant se produire lors de la mise en œuvre des plans des secours industriels (POI/PPI).

En plus de ce travail bibliographique, des exercices des Plans d'Opérations Internes ont été suivies sur deux installations SEVESO. Ces exercices, de nature mensuelle, annuelle ou biannuelle, ont permis de réaliser un retour d'expérience et d'identifier d'autres défaillances dans la mise en œuvre de ces plans. Jusqu'en mai 2010, 28 exercices POI et 3 exercices PPI ont été suivis. Ces exercices ont fait l'objet d'un rapport d'exercice, sous forme de main courante, accompagnée par des observations. Ces observations ont permis d'identifier plusieurs points critiques dans la mise en œuvre des Plans d'Opérations Internes.

Les défaillances identifiées ont été classées dans un tableau qui comporte le type de défaillance et les fonctions, ressources et supports associés. A partir de ce tableau, des fréquences ont été calculées pour chaque type de défaillance. Les fréquences cumulées de 119 défaillances recensées sur des POI (classées par fonction principale du système POI) sont présentées sur la fig. 4.

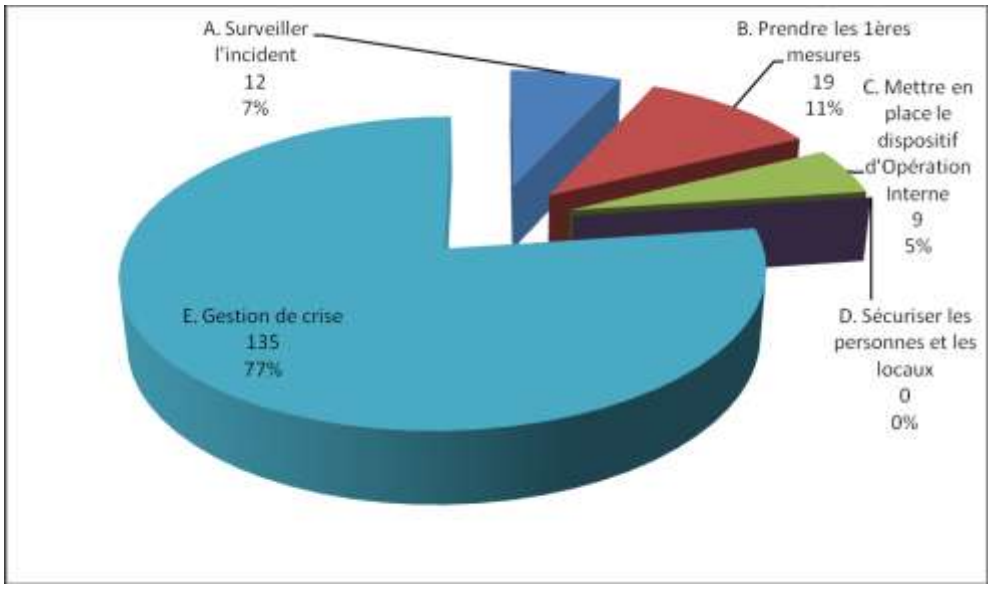

Figure 4 : Défaillances de dispositifs d'intervention d'urgence mis en place par des Plans d'Opération Internes, observées à partir d'exercices ou de l'analyse de rapports d'accidents

3. Exemple : méthode de calcul du taux de défaillance d'une fonction

Les points critiques identifiés par l'analyse présentée ci-dessus sont utilisés pour valider les arbres de défaillances pour chacune des fonctions et des ressources, représentant les combinaisons logiques des événements conduisant à la défaillance des fonctions et des ressources. La figure 5 illustre à titre d'exemple l'arbre de défaillances du système E2 : DIRIGER LES OPERATIONS INTERNES, qui est un sous-système de E : GERER LA CRISE.

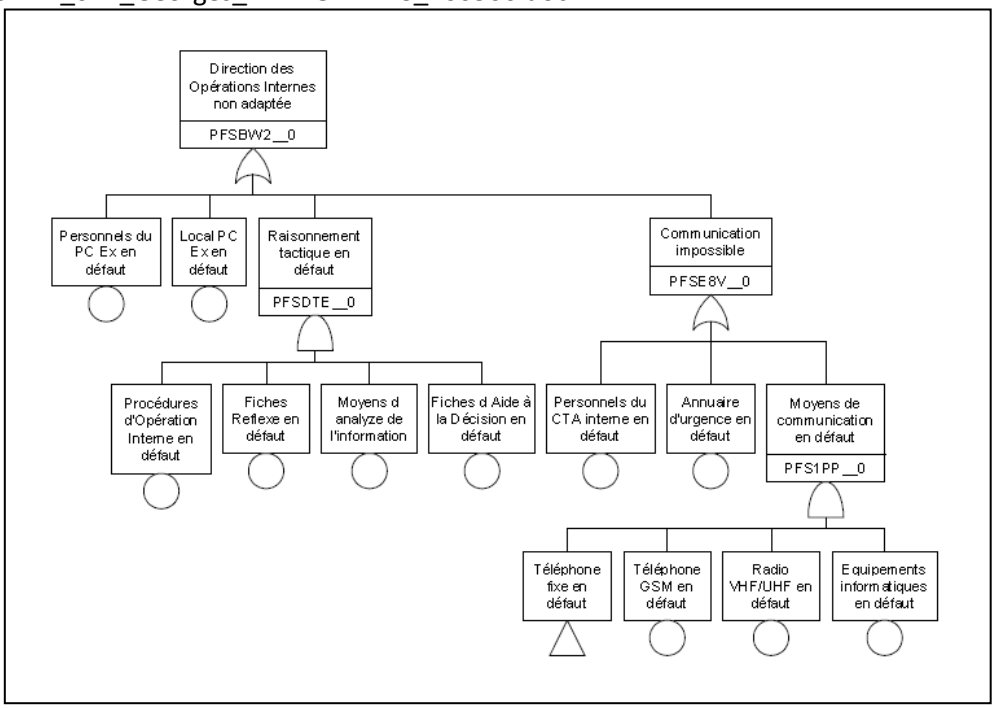

Figure 5 : Arbre de défaillance du système E2 : DIRIGER LES OPERATIONS INTERNES

Cet arbre de défaillance comporte la combinaison logique des événements qui peuvent entrainer la défaillance de la fonction. Les événements de base de cet arbre sont les défaillances des ressources de la fonction E2. L'arbre de défaillance de la ressource « Téléphone (fixe) » est donné comme exemple sur la fig. 6. L'événement au sommet de cet arbre (fig. 6) est l'événement de base correspondant de l'arbre de la fonction. Ainsi, l'arbre complet de la fonction peut être construit en assemblant les arbres de défaillance de la fonction et de toutes ses ressources.

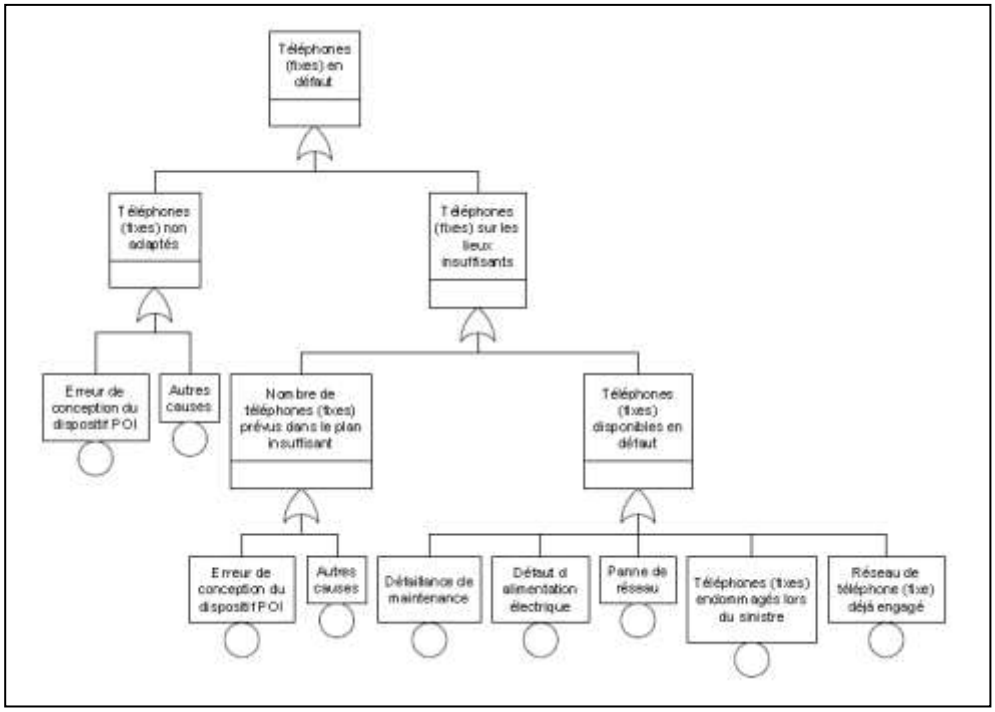

Figure 6 : Arbre de défaillances de fa ressource « Téléphone (fixe) »

Une ou plusieurs questions ont été associées à chaque événement de base ou intermédiaire de l'arbre de défaillance de chaque ressource. Par exemple, les questions associées à la ressource « Téléphone (fixe) » sont :

- Les téléphones fixes sont adaptés aux besoins opérationnels ?
- Les téléphones fixes prévus dans le plan sont suffisants en nombre ?
- Les téléphones fixes sont entretenus suivant les consignes du fabriquant ?
- Les téléphones fixes sont accessibles en cas d'accident ?
- L'alimentation électrique des téléphones fixes est assurée ?
- Est-ce que des moyens de communications redondants sont disponibles pour la communication entre le PC Ex et le dispositif sur le terrain ?

Les questions sont générées par les modes de défaillance et les arbres de défaillances des ressources à partir d'une procédure automatique et logique. La réponse oui/non à la question permet de choisir une classe de probabilité pour les événements de base. Les classes de probabilité de ces événements permettront d'évaluer la classe de probabilité de défaillance des ressources et des fonctions correspondantes à partir des relations logiques.

En ce qui concerne la gravité de défaillance de la fonction E2, cette dernière interagit avec tous les autres sous-systèmes du système E : GERER LA CRISE. Par conséquent, sa défaillance peut provoquer la défaillance de tout ce système. La gravité maximale sera ainsi définie par les dégâts les plus importants que peuvent être provoqués par l'événement le plus dangereux défini dans les études de danger.

Conclusion

Un modèle structuro-fonctionnel a été utilisé dans le cadre de ce travail de recherche pour faciliter une approche d'évaluation de la robustesse des plans de secours industriels, basée sur une analyse de risques itérative. Cette approche repose sur l'identification et l'analyse des dysfonctionnements pouvant se produire lors de la mise en œuvre du plan. Ces défaillances ont à leur tour été identifiées à travers une analyse a priori du modèle du plan et une analyse a posteriori issue de retours d'expérience d'accidents industriels et d'exercices d'intervention. Ces défaillances ont permis de valider des arbres de défaillances des ressources et des fonctions du plan, créés à partir du modèle FIS.

Cette double approche permet d'identifier des dysfonctionnements potentiels et de capitaliser cette connaissance en construisant des arbres de défaillance pour les fonctions du plan et leurs ressources. Des questions d'évaluation sont ensuite attribuées aux événements de ces arbres afin d'évaluer la probabilité de défaillance des ressources et des fonctions. La gravité de défaillance de chaque fonction est déterminée en utilisant les études de danger, suivant la règle des dommages maximum qu'elle peut provoquer. C'est ainsi qu'une expression quantitative du risque de défaillance de chaque fonction du plan est obtenue, ce qui permet d'évaluer la robustesse du plan en termes du risque de défaillance.

Cette méthode permet l'analyse des fonctions et de la structure d'un plan de secours industriel. Elle constitue une boite à outils qui peut être utilisée à la fois pour l'évaluation des plans existants, mais aussi pour l'élaboration du dispositif défini dans un plan de secours industriel.

Remerciements

Ce travail de recherche se déroule en collaboration directe avec le site de Sanofi-Aventis à Vertolaye (63) et la Plate-forme Chimique du Pont-de-Claix (38). Ils nous ont donné accès à leurs POI et nous font bénéficier de leur expertise et retour d'expérience sur le suivi d'incidents et accidents mais aussi lors d'exercices de simulation. Nous souhaitons remercier M. Jean-Luc LAUBE, Responsable Sécurité du site de Sanofi-Aventis à Vertolaye (63) et M. Damien REY, Responsable Sécurité de la Plate-forme Chimique du Pont-de-Claix (38), du soutien qu'ils nous ont apporté dans le cadre de ce travail.

Références

Alexander, D., 2002. Principles of emergency planning and management, Terra Publishing, ISBN: 1-903544-10-6.

Alexander, D., 2005. Towards the development of a standard in emergency planning. Disaster Prevention and Management, 14(2), 158-175.

Baiardi, F., Telmon, C., Sgandurra, D., 2009. Hierarchical, model-based risk management of critical infrastructures. Reliability Engineering and System Safety, 64 (2009), 1403-1415.

Deming, W.E., 1986. Out of the Crisis, MIT Press.

Direction de la Défense et de la Sécurité Civiles, 1985. Guide d'élaboration d'un Plan d'Opération Interne.

Direction de la Défense et de la Sécurité Civiles, 2007. ORSEC Départemental – Disposition Spécifique – Plan Particulier d'Intervention –PPI) – Etablissements SEVESO « seuil haut », Guide, Tome S.1.2.

Direction de la Défense et de la Sécurité Civiles, 2007. ORSEC Départemental – Disposition Spécifique – Plan Particulier d'Intervention (PPI) – Etablissements SEVESO « seuil haut », Mémento, Tome S.1.1.

Federal Emergency Management Agency, 1996. Guide for All – Hazard Emergency Operations Planning, State and Local Guide (SLG) 101.

Federal Emergency Management Agency, 2003. Guidelines for HazMat/WMD response, Planning and Prevention Training.

Federal Emergency Management Agency, 2009. Developing and maintaining state, territorial, tribal and local government emergency plans.

Flaus, J.M., 2007. Méthodologie FISE, document interne G-SCOP/INPG.

Flaus J. M. (2008), A model-based approach for systematic risk analysis, IMechE Vol.222 Part O: Risk and Reliability, pp.79-93

Groupe d'Etudes de Sécurité des Industries Pétrolières et Chimiques, 2001. Guide méthodologique du GESIP pour l'élaboration du P.O.I. d'un site industriel, usine chimique, complexe pétrochimique – Rapport GESIP 96/01.

Groupe d'Etudes de Sécurité des Industries Pétrolières et Chimiques, 2001. 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 – Réédition 2001.

Jackson B., 2008. The Problem of Measuring Emergency Preparedness – The Need for Assessing "Response Reliability" as Part of Homeland Security Planning, Rand Corporation.

Kanno, T., Furuta, K., 2006. Resilience of Emergency Response Systems. 2nd Symposium on Resilience Engineering: November 8-10, 2006, Juan-les-Pins, France.

Lagadec, P., 2007. Katrina : Examen des rapports d'enquête, Tomes 1 et 2, Ecole Polytechnique – Centre National de la Recherche Scientifique.

Larken, J., Shannon, H., Strutt, J.E., Jones, B., 2001. Performance indicators for the assessment of emergency preparedness in major accident hazards, U.K. Health and Safety Institute.

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

Ramsay, C., 1999. Protecting your business: from emergency planning to crisis management. Journal of Hazardous Materials, 65(1999), 131-149

Simon, H., 1981. The Sciences of the Artificial, MIT Press.

Union des Industries Chimiques, 1981. Les cahiers de sécurité, cahier n°3 : L'analyse par arbre des causes.

U.S. Department of Defense, 1980. Military Standard – Procedures for Performing a Failure Mode, Effects and Criticality Analysis, MIL-STD-1629A.

U.S. National Response Team, 2001. Hazardous Materials Emergency Planning Guide.

Villemeur, A., 1988. Sûreté de fonctionnement des systèmes industriels, Editions Eyrolles.