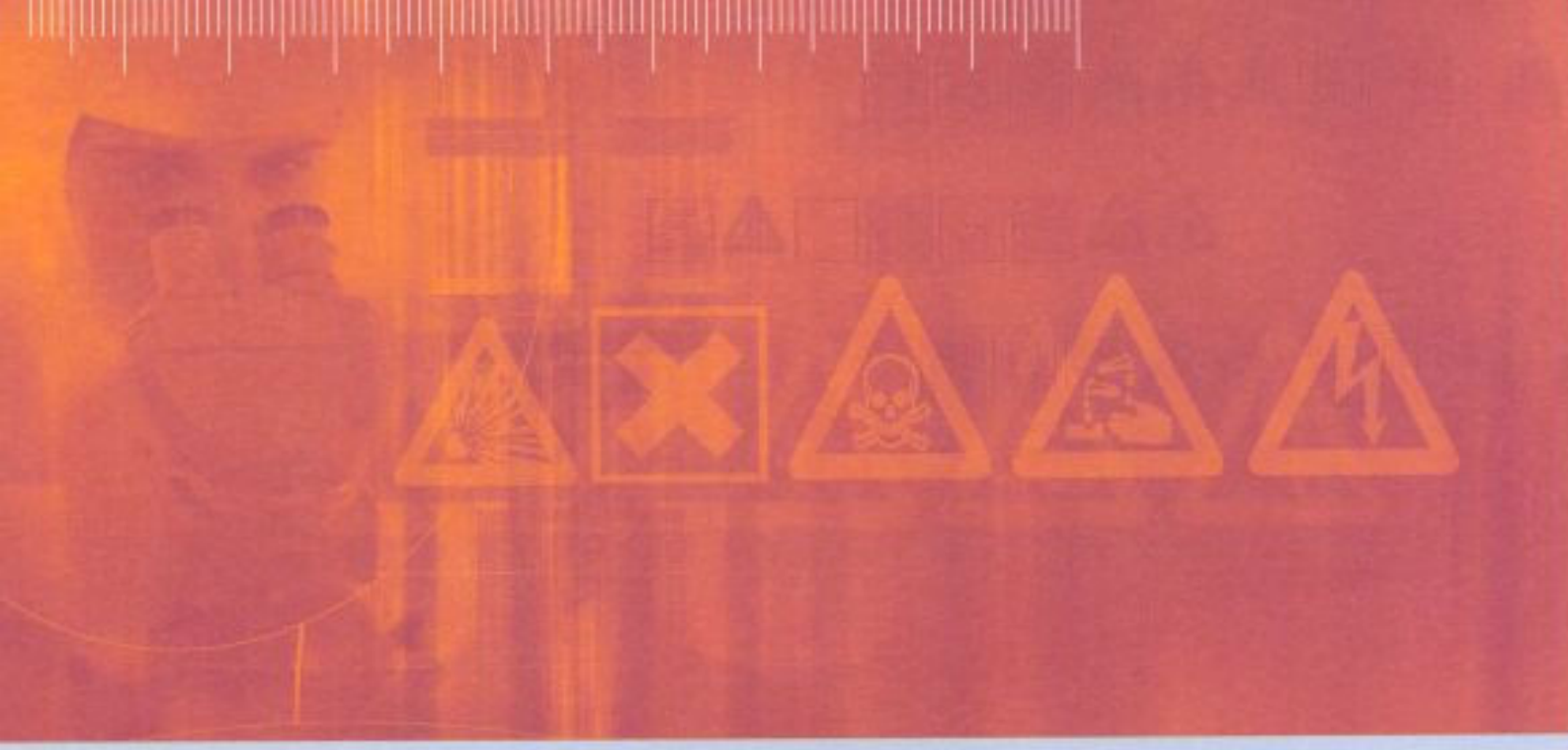


RAPPORT D'ÉTUDE 13/10/2006
N° INERIS-DRA-2006-P46055-CL47569

Formalisation du savoir et des outils dans le domaine des risques majeurs (DRA-35)

Ω-7

Méthodes d'analyse des risques générés par une installation industrielle

Ministère de l'Ecologie et du Développement Durable (MEDD)

INERIS

Formalisation du savoir et des outils dans le domaine des risques majeurs (DRA-35)

Ω-7

Méthodes d'analyse des risques générés par une installation industrielle

Direction des Risques Accidentels

Ministère de l'Ecologie et du Développement Durable (MEDD)

Liste des personnes ayant participé à l'étude :
B.DEBRAY, S.CHAUMETTE, S. DESCOURIERE, V. TROMMETER

PREAMBULE

Le présent document a été établi :

- au vu des données scientifiques et techniques disponibles ayant fait l'objet d'une publication reconnue ou d'un consensus entre experts,
- au vu du cadre légal, réglementaire ou normatif applicable.

Il s'agit de données et informations en vigueur à la date de l'édition du document, en septembre 2006.

Le présent document comprend des propositions ou recommandations. Il n'a en aucun cas pour objectif de se substituer au pouvoir de décision du ou des gestionnaire(s) du risque ou d'une partie prenante.

PAGE DE VALIDATION		
Méthodes d'analyse des risques générés par une installation industrielle		
Révision		
Auteur de la mise à jour 2006	**Vérificateur**	**Approbateur**
Bruno DEBRAY	Nelson RODRIGUES	Didier GASTON
Responsable du programme	Délégué appui technique à l'administration	Directeur Adjoint Direction des Risques Accidentels

REPERTOIRE DES MODIFICATIONS

Révision	Relecture	Application	Modifications
PROJET	Novembre 2001		Création du document
Version 1	Mai 2003		**Auteurs E. Bernuchon, O. Salvi**
Version 2	Juin 2006		Ajout des méthodes intégrées

TABLE DES MATIERES

1 OBJECTIF ET DOMAINE D'APPLICATION

1.1 OBJET DU PROGRAMME DRA-35

Depuis plusieurs années, le Ministère en charge de l'Environnement (actuellement, Ministère de l'Ecologie et du Développement Durable) finance un programme d'études et de recherches intitulé « Formalisation du savoir et des outils dans le domaine des risques majeurs ».

L'objet du premier volet de ce programme est de réaliser un recueil formalisant l'expertise de l'INERIS dans le domaine des risques accidentels majeurs. Ce recueil sera constitué de différents rapports consacrés aux thèmes suivants :

- les phénomènes physiques impliqués en situation accidentelle (incendie, explosion, BLEVE…)
- l'analyse et la maîtrise des risques,
- les aspects méthodologiques pour la réalisation de prestations réglementaires (étude de dangers, analyse critique..)

Chacun de ces documents reçoit un identifiant propre du type « Ω-X » afin de faciliter le suivi des différentes versions éventuelles du document.

In fine, ces documents décrivant les méthodes pour l'évaluation et la prévention des risques accidentels, constitueront un recueil des méthodes de travail de l'INERIS dans le domaine des risques accidentels.

1.2 DOMAINE D'APPLICATION ET CONTEXTE

Le présent rapport référencé **Ω-7** présente quelques-uns des outils permettant d'identifier a priori les risques générés par des installations industrielles. Il s'inscrit dans une démarche de valorisation du savoir-faire de l'INERIS auprès des pouvoirs publics, des industriels et du public. Une première version de ce rapport a été écrite en 2001 (E.Bernuchon, O.Salvi). La présente version intègre des compléments relatifs aux méthodes intégrées d'analyse des risques. Elle tient compte aussi des évolutions réglementaires récentes en vue de l'application de la loi du 30 juillet 2003[1] et de l'évolution de la pratique de l'INERIS en matière d'analyse de risques dans les études de dangers.

[1] loi du 30 juillet 2003 relative à la prévention des risques technologiques et naturels et à la réparation des dommages, JO du 31 juillet 2003

1.2.1 CONTEXTE

Tout système industriel est susceptible de générer des risques de nature variée. Le guide ISO/CEI 73 définit le risque comme la "combinaison de probabilité d'un événement et de ses conséquences". D'un point de vue général, les conséquences peuvent être positives ou négatives. Dans le domaine de la sécurité, on s'intéresse plus particulièrement aux conséquences négatives, qui se traduisent par un dommage causé à un élément vulnérable. Dans ce cas le risque est défini comme la "combinaison de la probabilité d'un dommage et de sa gravité" [guide ISO/CEI 51].

Gérer un risque est un processus itératif qui a pour objectif d'identifier, d'analyser et de réduire au maximum le risque ou de le maintenir dans des limites acceptables. La gestion des risques est une des composantes fondamentales de la gestion d'un système. Elle est essentielle à la réussite des entreprises, que ce soit en terme économique ou environnemental. L'analyse de risques est une étape clé du processus de gestion des risques. Sa réalisation nécessite de mettre en œuvre une démarche structurée systématique. C'est ce à quoi sont destinées les méthodes que nous présentons dans ce rapport. Celles-ci sont applicables à une variété de risques d'origine technique, en particulier aux risques industriels majeurs auxquels la collection dans laquelle s'inscrit ce document est particulièrement consacrée.

Le risque industriel majeur est le risque qui résulte de l'exploitation d'installations industrielles dangereuses et qui est plus particulièrement relatif à la possibilité d'occurrence d'un accident majeur : « Evénement tel qu'une émission, un incendie ou une explosion d'importance majeure résultant de développements incontrôlés survenus au cours de l'exploitation d'un établissement, entraînant pour les intérêts visés à l'article L.511-1 du code de l'environnement, des conséquences graves, immédiates ou différées, et faisant intervenir une ou plusieurs substances ou des préparations dangereuses.» (arrêté du 10 mai 2000 modifié[2])

La législation sur les installations classées (livre V du code de l'environnement) prévoit, entre autres, que l'exploitation d'une installation classée soumise à autorisation est subordonnée à la réalisation d'une étude de dangers qui présente une analyse de risques. C'est notamment pour permettre aux acteurs concernés de répondre à cette obligation que l'INERIS a entrepris la rédaction de ce rapport.

L'article 4 alinéa 2 de l'arrêté du 10 mai 2000[2] précise les attentes de l'administration en matière d'analyse de risques.

"L'analyse de risques, au sens de l'article L. 512-1 du code de l'environnement, constitue une démarche d'identification et de réduction des risques réalisée sous la responsabilité de l'exploitant. Elle décrit les scénarios qui conduisent aux phénomènes dangereux et accidents potentiels. Aucun scénario ne doit être ignoré ou exclu sans justification préalable explicite.

---

[2] arrêté du 10 mai 2000 modifié relatif à la prévention des accidents majeurs impliquant des substances ou des préparations dangereuses présentes dans certaines catégories d'installations classées pour la protection de l'environnement soumises à autorisation

Cette démarche d'analyse de risques vise principalement à qualifier ou à quantifier le niveau de maîtrise des risques, en évaluant les mesures de sécurité mises en place par l'exploitant, ainsi que l'importance des dispositifs et dispositions d'exploitation, techniques, humains ou organisationnels, qui concourent à cette maîtrise.

Elle porte sur l'ensemble des modes de fonctionnement envisageables pour les installations, y compris les phases transitoires, les interventions ou modifications prévisibles susceptibles d'affecter la sécurité, les marches dégradées prévisibles, de manière d'autant plus approfondie que les risques ou les dangers sont importants. Elle conduit l'exploitant des installations à identifier et hiérarchiser les points critiques en termes de sécurité, en référence aux bonnes pratiques ainsi qu'au retour d'expérience de toute nature."

Il existe, à l'heure actuelle, de nombreuses méthodes dédiées à l'analyse des risques et il serait illusoire de vouloir les décrire toutes dans le détail. Le parti a été pris dans ce document de présenter quelques-unes des méthodes dont l'usage est particulièrement répandu ainsi que quelques méthodes intégrées, qui régissent l'utilisation des méthodes simples dans une démarche globale d'évaluation des risques.

Soulignons également que les méthodes présentées dans ce document sont dédiées prioritairement à l'identification des risques générés par une installation industrielle sur son environnement. Dans le cadre d'une démarche exhaustive d'analyse des risques, il convient également de caractériser les risques d'agressions externes de l'environnement sur cette installation (par exemple, catastrophes naturelles, effets dominos…). Pour ce faire, il existe des méthodes spécifiques qui ne seront pas décrites dans ce document. Le lecteur peut cependant utilement se rapporter aux rapports rédigés dans le cadre du programme "Analyse des risques et prévention des accidents majeurs" (dra-34) dont l'opération f porte sur "l'Examen des conséquences pour les Installations Classées pour la Protection de l'Environnement des risques naturels et de la façon de les intégrer dans l'analyse des risques" [Vallée 2003], [Vallée 2004] et l'opération e porte sur les "Concepts et méthodes de détermination des effets domino" [Hubin 2005].

1.3 DEMARCHE OBSERVEE

Les méthodes d'analyse des risques ne sont que des outils d'aide à la réflexion et, en ce sens, leur qualité est fortement liée à leurs contexte et conditions de mise en œuvre. Il est donc indispensable de se pencher brièvement sur les raisons qui justifient l'utilisation de telles méthodes. Le chapitre 2 s'attache donc à présenter les liens existant entre l'analyse et la gestion des risques.

Le chapitre 3 décrit, quant à lui, la démarche générale de l'analyse de risques, dans laquelle viennent s'insérer les outils d'analyse des risques présentés dans ce document.

Le chapitre 4 est dédié à la description des méthodes de base suivantes :

- l'Analyse Préliminaire des Risques (APR),
- l'Analyse des Modes de Défaillances, de leurs Effets et de leur Criticité (AMDEC),
- la méthode HAZOP,
- la méthode « What-if ? », qui en est une évolution,
- l'analyse par arbre des défaillances,
- l'analyse par arbres d'évènements,
- le Nœud Papillon.

Le chapitre 5 présente quatre méthodes intégrées d'analyse de risques, qui traitent l'ensemble du processus d'analyse de risque en faisant appel à plusieurs méthodes simples :

- la méthode MOSAR,
- la méthode LOPA,
- la méthode ARAMIS,
- le QRA.

Le chapitre 6 décrit de façon synthétique la méthode appliquée le plus fréquemment par l'INERIS dans le cadre des études de dangers. Cette méthode est, par ailleurs, décrite en détail dans le rapport Oméga 9 relatif aux études de dangers [Joly 2006].

Le chapitre 7 présente les avantages et les limites des méthodes d'analyse des risques en général. Ceux-ci sont synthétisés dans un tableau qui permet de positionner les méthodes entre elles.

Enfin, pour la clarté du document, un glossaire est présenté au chapitre 1. Il reprend les définitions des termes relatifs à l'analyse des risques et fait, le cas échéant, référence à des normes et des textes réglementaires ainsi qu'au glossaire technique des risques technologiques publié par le SEI du MEDD et joint à la circulaire du 7 octobre 2005[3]. Ce glossaire est un document indicatif visant à éclairer la lecture des textes publiés postérieurement à sa publication et à harmoniser le vocabulaire utilisé par les services d'inspection des installations classées. Il est disponible avec le texte de la circulaire sur le site AIDA de l'INERIS (http://aida.ineris.fr).

---

[3] Circulaire n° DPPR/SEI2/MM-05-0316 du 7 octobre 2005 relative aux Installations classées - Diffusion de l'arrêté ministériel 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

2 PLACE DE L'ANALYSE DANS LA GESTION DES RISQUES

Ce chapitre s'appuie en partie sur les Guides ISO/CEI 51 :1999 : « Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes » et ISO/CEI 72 : 2002 : « Management du risque – Vocabulaire – Principes directeurs pour l'utilisation dans les normes » ainsi que sur le fascicule de documentation FD X 50-252 édité par l'AFNOR « Management du risque, lignes directrices pour l'estimation des risques » et le glossaire annexé à la circulaire du 7 octobre 2005 relative aux installations classées[1]. Il est essentiel de souligner dès maintenant que le vocabulaire de la gestion des risques souffre encore de nombreuses divergences, les mêmes termes prenant souvent des sens différents suivant le contexte dans lequel il sont utilisés. Ce qui est vrai dans une langue l'est encore plus lorsqu'il s'agit de traduire des termes utilisés dans des langues étrangères. Pourtant il apparaît qu'au-delà du vocabulaire, les concepts utilisés sont universels. Ce chapitre a pour objectif de clarifier ce que nous entendons par analyse de risques, expliquer comment celle-ci se distingue et s'articule avec les autres étapes de la gestion des risques.

2.1 PRINCIPES POUR LA GESTION DES RISQUES

La gestion des risques ou management des risques peut être définie comme l'ensemble des activités coordonnées menées en vue de réduire les risques à un niveau jugé tolérable ou acceptable à un moment donné et dans un contexte donné. Il existe actuellement plusieurs référentiels définissant le vocabulaire du management des risques qui présentent encore entre eux des différences relativement importantes sur les termes, comme l'illustre la Figure 1. Cependant, au-delà des mots, il est important de souligner que tous ces documents décrivent un processus de gestion identique dans son essence. Au sein de ce processus, l'analyse de risques occupe une place centrale, même si elle n'est pas toujours nommée explicitement.

Manager les risques implique d'abord de définir le système auquel le management s'applique, d'identifier les acteurs impliqués : les parties intéressées, les décideurs.

La phase qui suit est nommée différemment suivant les auteurs ou les sources de référence. Ainsi dans la version Française du guide ISO CEI 73 elle est appelée **appréciation du risque**, dans le fascicule de documentation AFNOR FD X50-252, **estimation des risques.** Cette phase se décompose en plusieurs étapes qui conduisent finalement à caractériser le risque présenté par le système étudié.

Celle-ci inclut l'identification des éléments qui sont à l'origine du danger et ceux qui peuvent en subir les conséquences, la détermination des scénarios potentiels qui conduisent à la réalisation d'un danger, l'estimation des grandeurs représentatives du risque : gravité des conséquences potentielles, probabilité associée. **L'analyse de risque telle que nous la décrivons dans la suite du document s'inscrit dans cette phase. Elle vise en particulier à identifier et décrire les scénarios qui peuvent conduire à une situation accidentelle et à en estimer la probabilité ainsi qu'un ordre de grandeur de gravité.** La quantification fine des

conséquences est considérée traditionnellement comme ne faisant pas partie de l'analyse de risques. Elle fait appel à des méthodes, modèles et outils qui ne sont pas décrits dans le présent document. De même, dans le contexte du risque accidentel, la détermination de la relation entre le danger et la gravité des dommages potentiels peut être considérée comme un préalable à l'analyse de risques (détermination des seuils d'effet des phénomènes dangereux).

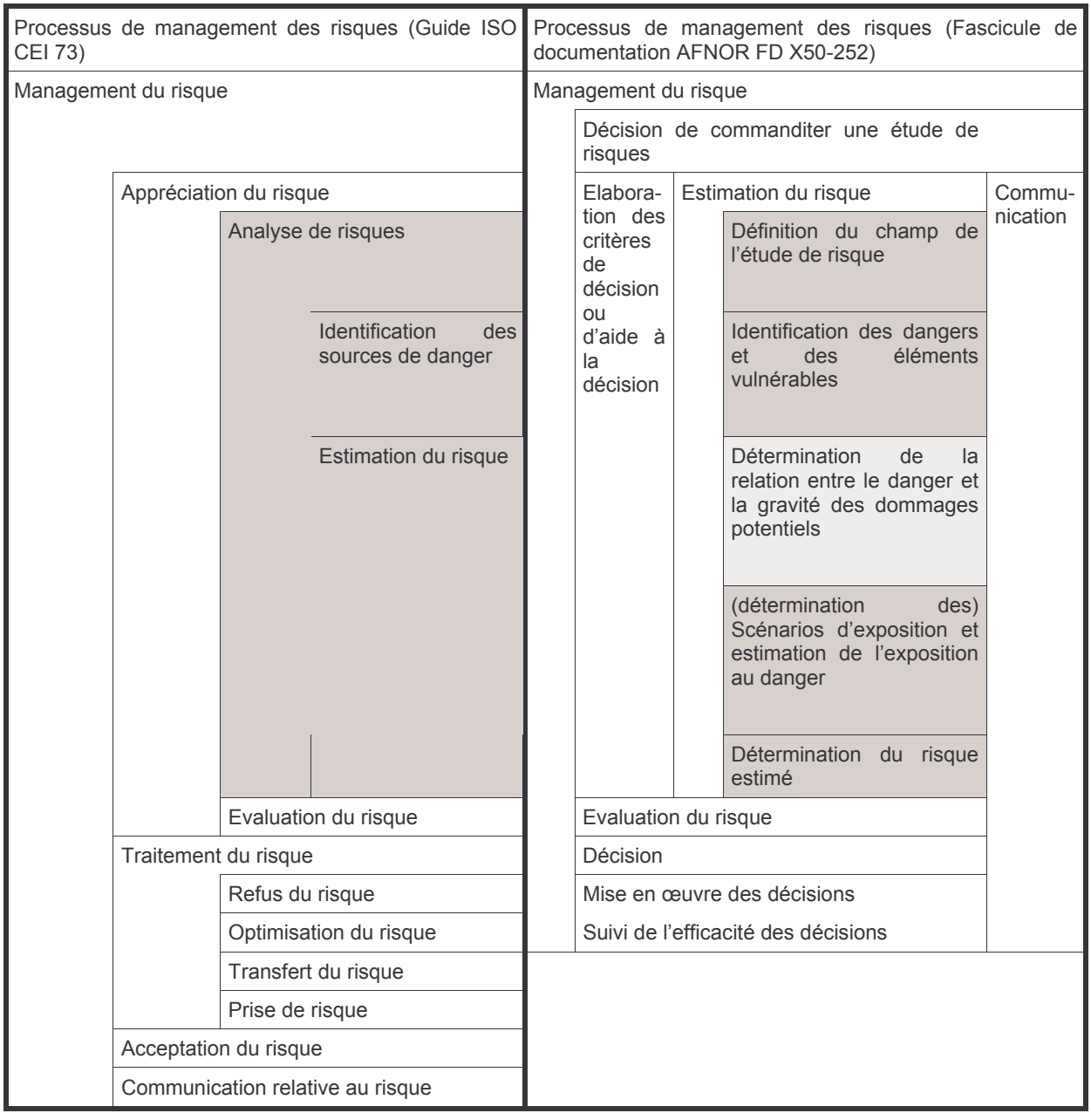


Figure 1: deux représentations du processus de management du risque décrits dans le guide ISO CEI 73 et dans le fascicule de documentation AFNOR FD X50-252. Dans cette figure, les cellules grisées correspondent aux activités typiques de l'analyse de risques.

L'approche de l'analyse de risques telle qu'elle se présente dans les méthodes intégrées comme ARAMIS ou LOPA correspond à l'ensemble de la démarche d'estimation du risque décrite dans le fascicule de documentation AFNOR. Celle que permettent les outils classiques comme l'APR, l'AMDEC ou l'HAZOP correspond de façon plus restrictive aux étapes d'identification des dangers et des éléments vulnérables, de description des scénarios d'accident et des mesures de maîtrise du risque et d'estimation de la probabilité. Dans le contexte du risque accidentel, la détermination de la relation entre le danger et la gravité des dommages potentiels peut être considérée comme un préalable à l'analyse de risques accidentels (détermination des seuils d'effet des phénomènes dangereux).

A l'issue de la phase d'appréciation (ou estimation) des risques, la phase d'évaluation consiste à comparer le risque estimé à des critères de décision. Cette phase peut revêtir diverses formes : comparaison des risques à un niveau d'acceptabilité du risque, hiérarchisation des scénarios pour identifier les scénarios devant faire l'objet d'un traitement en priorité…

Il est important de souligner que l'analyse des risques est une étape qui intervient en amont de l'étape nommée ici évaluation (même si ce terme est aussi souvent employé à la place d'appréciation ou estimation), qui consiste à comparer le risque estimé à des critères de décision dont l'élaboration fait l'objet d'un processus séparé mais qui conditionnent néanmoins le format des résultats de l'analyse des risques. Celle-ci s'inscrit dans un processus de décision et répond aux besoins d'acteurs (commanditaire, décideur) qu'il est essentiel de bien identifier.

2.2 DANGER, RISQUE, ALEA, VULNERABILITE, DIFFERENTES FAÇONS DE CONSIDERER LE RISQUE

Les textes réglementaires qui ont suivi la parution de la loi du 30 juillet 2003 ont mis en avant les notions d'aléa et de vulnérabilité des enjeux pour qualifier le risque technologique. Il s'agit d'une évolution qui amène à considérer le risque d'une façon un peu différente des approches traditionnelles qui considèrent uniquement la probabilité et la gravité d'un dommage. En pratique il s'agit d'une façon différente d'opérer le regroupement des composantes principales qui permettent de caractériser le risque. Ainsi, lorsque les paramètres sont agrégés, il demeure équivalent de dire que le risque est la combinaison de la probabilité et de la gravité ou de l'aléa et de la vulnérabilité, comme l'illustre la Figure 2. En revanche, suivant les décisions qui doivent être prises, il peut être plus utile d'adopter l'une ou l'autre des définitions.

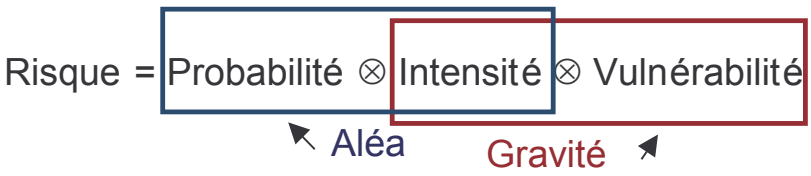


Figure 2 : Les composantes du risque

Dans les problématiques d'aménagement autour des sites à risques, il est essentiel de connaître l'aléa afin de réduire ou de supprimer la vulnérabilité par des mesures de renforcement du bâti, voire des mesures foncières, ou de l'empêcher d'augmenter par des mesures de maîtrise de l'urbanisation. Ces décisions sont cependant bien prises en considérant la probabilité et la gravité potentielle d'un phénomène dangereux qui exposerait des éléments vulnérables dont la présence résulterait des décisions de maîtrise de l'urbanisation.

2.3 ANALYSE DES RISQUES

L'analyse des risques vise donc tout d'abord à identifier les sources de dangers et les situations associées qui peuvent conduire à des dommages sur les personnes, l'environnement ou les biens.

Suivant les outils ou méthodes employés, la description des situations dangereuses est plus ou moins approfondie et peut conduire à l'élaboration de véritables scénarios d'accident.

L'analyse des risques permet aussi de mettre en lumière les barrières de sécurité existantes en vue de prévenir l'apparition d'une situation dangereuse (barrières de prévention) ou d'en limiter les conséquences (barrières de protection).

Consécutivement à cette identification, il s'agit d'estimer les risques en vue de hiérarchiser les risques identifiés au cours de l'analyse et de pouvoir comparer ultérieurement ce niveau de risque aux critères de décision.

L'estimation du risque implique la détermination :

- d'un niveau de probabilité que le dommage survienne,
- d'un niveau de gravité de ce dommage.

Il peut aussi être exprimé en termes de :

- niveau de probabilité qu'un phénomène dangereux se produise,
- niveau d'intensité du phénomène en question,
- présence d'enjeux ou éléments vulnérables exposés,
- vulnérabilité des enjeux.

L'estimation de ces grandeurs peut être qualitative, quantitative ou semi-quantitative, suivant le contexte, les exigences des décideurs et les outils et données disponibles.

Avec la loi n° 2003-699 du 30 juillet 2003[4] et la réglementation qui en découle, la probabilité acquiert un poids qu'elle n'avait pas jusqu'alors dans la décision publique. Il devient encore plus crucial qu'auparavant de pouvoir l'estimer à l'aide de méthodes fiables et reconnues. Les outils d'analyse de risque présentés dans la suite de ce document permettent un approche plus ou moins détaillée de la probabilité. Parmi ceux-là, les arbres de défaillance et d'événement sont les outils le plus adaptés aux calculs probabilistes. Cependant, leur mise en oeuvre purement quantitative se heurte encore bien souvent à une absence totale de données. Elle nécessite aussi de construire des arbres très détaillés, ce qui rend les études longues et coûteuses. Pour palier cette difficulté, l'INERIS préconise le recours à une approche semi-quantitative, qualifiée parfois "d'approche barrière", qui met l'accent sur la démonstration de la maîtrise des risques. Cette méthode est brièvement décrite à la fin du présent rapport. Elle est détaillée dans le rapport Oméga 9 sur l'étude de dangers [Joly 2006]. Par ailleurs, l'estimation de la probabilité a fait l'objet de deux rapports spécifiques rédigés dans le cadre du programme DRA 34 [Bouissou 2006],[De Dianous 2006], auxquels nous encourageons le lecteur à se reporter.

2.4 EVALUATION DU RISQUE

Dans les diverses normes présentées plus haut, l'évaluation du risque désigne l'étape de comparaison du risque estimé à des critères de décision face au risque. La plupart du temps, il s'agit de décider si le risque est acceptable ou s'il doit faire l'objet de mesures supplémentaires de maîtrise. La définition de critères d'acceptabilité du risque est réalisée en amont ou en parallèle au processus d'analyse de risque. Elle implique des acteurs différents : les décideurs, de préférence en concertation avec les parties intéressées.

La définition de critères d'acceptabilité du risque ou, plus généralement de critères de décision, est une étape clé dans le processus de gestion du risque dans la mesure où elle va motiver la nécessité de considérer de nouvelles mesures de réduction du risque et rétroactivement, influencer les façons de mener l'analyse et l'évaluation des risques.

Cette étape cruciale est bien souvent délicate. Il est entendu que ces critères sont fonction du contexte de l'établissement concerné et des objectifs poursuivis dans la gestion des risques.

A ce propos, la définition du risque tolérable donnée dans le guide ISO/CEI 51 :1999 laisse transparaître la difficulté de retenir des critères objectifs et forfaitaires pour l'acceptation du risque :

Risque tolérable (Guide ISO/CEI 51 :1999)
Risque accepté dans un certain contexte et fondé sur les valeurs admises par la société.

[4] Loi n° 2003-699 du 30 juillet 2003 relative à la prévention des risques technologiques et naturels et à la réparation des dommages, JO du 31 juillet 2003

Ainsi, l'acceptation du risque peut dépendre de facteurs éthiques, moraux, économiques ou politiques. Pour ce qui concerne le domaine des risques accidentels, la décision d'acceptation des risques repose également dans les mains des autorités compétentes.

Quels que soient les critères d'acceptation retenus, il est indispensable qu'ils soient connus et explicites préalablement à toute phase d'analyse des risques.

Les critères de décision ne font pas toujours référence explicitement à la notion de risque acceptable. Dans la réglementation applicable aux installations classées[5], par exemple, l'étude de dangers justifie que l'exploitant met en œuvre toutes les mesures de maîtrise du risque internes à l'établissement, dont le coût n'est pas disproportionné par rapport aux bénéfices attendus, soit en termes de sécurité globale de l'installation, soit en termes de sécurité pour les intérêts visés à l'article L. 511-1 du code de l'environnement ou de coût de mesures évitées pour la collectivité (arrêté du 10 mai 2000 modifié[6]). Le critère de décision s'exprime ici en termes de bénéfices attendus des actions de maîtrise de risque par rapport au coût qu'elles engendrent et ne fait pas référence, au moins explicitement, à un risque acceptable. Il s'apparente plus à la notion d'ALARP (As Low As Reasonably Practicable) c'est à dire aussi bas que raisonnablement atteignable.

L'administration est ensuite en charge d'apprécier le niveau de maîtrise des risques. Les évolutions réglementaires récentes faisant suite à l'adoption du la loi n° 2003-699 du 30 juillet 2003 ont permis, à ce niveau, de clarifier la notion de risque acceptable pour les installations classées. Ainsi, deux textes apportent des éléments d'information : la Circulaire du 29 septembre 2005 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[7] et le guide PPRT[8].

La circulaire du 29 septembre 2005 mentionnée au paragraphe précédent contient une grille qui définit les niveaux de probabilité et de gravité au-delà desquels des mesures de maîtrise du risque additionnelles doivent être appliquées pour une maîtrise du risque à la source.

---

[5] Article 3 du décret du 21 septembre 1977 pris pour l'application de la loi n° 76-663 du 19 juillet 1976 relative aux Installations Classées pour la Protection de l'Environnement modifié : " 5° L'étude de dangers prévue à l'article L. 512-1 du code de l'environnement. Elle justifie que le projet permet d'atteindre, dans des conditions économiquement acceptables, un niveau de risque aussi bas que possible, compte tenu de l'état des connaissances et des pratiques et de la vulnérabilité de l'environnement de l'installation. "

[6] Arrêté du 10 mai 2000 relatif à la prévention des accidents majeurs impliquant des substances ou des préparations dangereuses présentes dans certaines catégories d'installations classées pour la protection de l'environnement soumises à autorisation, JO du 20 juin 2000

[7] BOMEDD n° 05/21 du 15 novembre 2005

[8] PLAN DE PREVENTION DES RISQUES TECHNOLOGIQUES, Guide Méthodologique, MEDD-DPPR-SEI, MTETM-DGUHC, Décembre 2005, accessible sur

http://www.ecologie.gouv.fr/IMG/pdf/Guide_PPRT_16-12-2005-2.pdf

Le guide PPRT précise les niveaux d'aléa pour lesquels des mesures de maîtrise de l'urbanisation doivent être décidées, éventuellement à l'issue d'un processus de concertation, pour réduire encore plus le risque lié à l'exposition des enjeux présents à proximité du site à certains phénomènes dangereux. Le guide précise aussi les conditions suivant lesquelles certains phénomènes peuvent ne pas être pris en compte à ce stade du fait de leur faible probabilité intrinsèque et de la fiabilité des moyens de maîtrise des risques à la source additionnels mis en œuvre.

2.5 REDUCTION DU RISQUE

La réduction du risque (ou maîtrise du risque) désigne l'ensemble des actions ou dispositions entreprises en vue de diminuer la probabilité ou la gravité des dommages associés à un risque particulier.

De telles mesures doivent être envisagées dès lors que le risque considéré est jugé inacceptable.

De manière très générale, les mesures de maîtrise du risque se répartissent en[9] :

- mesures (ou barrières) de prévention : mesures visant à éviter ou limiter la probabilité d'un événement indésirable, en amont du phénomène dangereux.
- mesures (ou barrières) de limitation : mesures visant à limiter l'intensité des effets d'un phénomène dangereux.
- mesures (ou barrières) de protection : mesure visant à limiter les conséquences sur les cibles potentielles par diminution de la vulnérabilité.

Des mesures de réduction du risque doivent être envisagées et mises en œuvre tant que le risque est jugé inacceptable.

Les mesures de réduction du risque consistent souvent à mettre en place des barrières de sécurité, dispositifs techniques ou organisationnels qui assurent la maîtrise du risque. La réduction du risque effectivement apportée par les barrières de sécurité dépend de leur efficacité, de leur temps de réponse et de leur fiabilité caractérisée par un niveau de confiance. L'ensemble de ces critères est décrit dans le rapport Oméga 10 relatif à l'évaluation des performances des barrières techniques de sécurité accessible sur le site Internet de l'INERIS. Ce sont ces critères qui permettent d'estimer in fine la probabilité d'un scénario dans le cadre de l'approche barrière mentionnée plus haut. L'INERIS est en train de formaliser dans un nouveau rapport Oméga l'application de ces critères aux barrières humaines de sécurité (interventions humaines destinées à réduire le risque d'accident ou les conséquences d'un accident). Ce document sera prochainement disponible sur le site Internet de l'INERIS.

---

[9] Glossaire technique des risques technologiques annexé à la Circulaire n° DPPR/SEI2/MM-05-0316 du 7 octobre 2005 relative aux Installations classées

3 DEMARCHE POUR L'ANALYSE DES RISQUES ASSOCIES A DES INSTALLATIONS INDUSTRIELLES

Les paragraphes suivants présentent la démarche adoptée pour l'analyse des risques associés à l'exploitation d'installations industrielles. Cette démarche se décompose généralement en plusieurs étapes :

- Définition du système à étudier et des objectifs à atteindre.

Cette étape préliminaire permet de définir clairement le cadre de l'analyse des risques.

Recueil des informations indispensables à l'analyse des risques.

Cette seconde étape vise à collecter l'ensemble des informations pertinentes pour mener le travail d'analyse de façon efficace. Outre la description fonctionnelle de l'installation à étudier et de son environnement, il est indispensable d'avoir clairement identifié :

- les dangers associés aux installations et aux substances qu'elles contiennent, transforment ou produisent,
- les risques d'agressions externes sur l'installation étudiée,
- l'analyse des accidents survenus sur des installations similaires,
- la vulnérabilité de l'environnement.

- Définition de la démarche à adopter

Dans cette étape, il est notamment question de choisir un ou plusieurs outils ou méthodes pour mener l'analyse des risques et de retenir, si nécessaire, des échelles de cotation des risques et une grille de criticité.

- Mise en œuvre de l'analyse de risques, de préférence dans le cadre d'un groupe de travail (en respectant cependant le principe de proportionnalité[10]).
  - Dans le cas de l'analyse de risques d'accident majeurs, le fait de réaliser cette évaluation en groupe de travail permet de répondre aux objectifs suivants :
  - L'analyse des risques doit tenir compte des spécificités de chaque établissement en matière d'environnement, d'exploitation ou de stratégie de sécurité. Ces renseignements sont disponibles auprès des personnes travaillant au quotidien sur les installations étudiées ou ayant une connaissance approfondie des installations (cas des projets).

---

[10] Suivant ce principe, par exemple, "Le contenu de l'étude de dangers doit être en relation avec l'importance des risques engendrés par l'installation et compte tenu de la vulnérabilité des intérêts visés par les articles L.211.1 et L.511.11 du Code de l'Environnement » (Art.3 - 5° du décret n°77-1133 du 21 septembre 1977 modifié)

- Les accidents majeurs sont généralement des sinistres rares résultant d'enchaînements et de combinaisons d'événements parfois difficiles à prédire. Une réflexion menée en commun par plusieurs personnes de sensibilités et compétences différentes favorise un examen plus riche des circonstances pouvant conduire à un accident majeur.
- L'analyse des risques en groupe de travail est un outil participant à l'appropriation de l'étude de dangers par l'exploitant, dans le cas où il ne la réalise pas lui-même, et à la communication entre certains services.

3.1 DEFINITION DU SYSTEME ET DES OBJECTIFS A ATTEINDRE

3.1.1 DEFINITION DU SYSTEME

L'analyse des risques est un travail qui peut s'avérer complexe et mobiliser des ressources importantes. Dès lors, il est indispensable d'identifier clairement le système à étudier et de déterminer sans ambiguïtés les limites de l'étude.

Il peut, par exemple, s'agir d'étudier les risques associés à une nouvelle installation devant être implantée, d'identifier les risques associés à la modification d'un procédé existant ou de passer en revue les risques à l'échelle d'un site industriel complet.

Cette définition permet notamment de limiter la description du système aux informations nécessaires et suffisantes au champ de l'étude.

3.1.2 DEFINITION DES OBJECTIFS A ATTEINDRE

La définition des objectifs de l'analyse des risques est une étape essentielle qui permet notamment de définir les critères d'acceptabilité des risques.

Il peut par exemple être nécessaire de mener une analyse des risques dans l'un des buts particuliers suivants :

- analyser les risques d'accidents de manière générale et les évènements pouvant nuire à la bonne marche du procédé (pannes, incidents…),
- analyser plus spécifiquement les risques aux postes de travail, réaliser une étude ATEX (Code du travail),
- analyser les risques d'accidents majeurs (cas de l'étude des dangers).

Selon les objectifs poursuivis, la démarche et les outils utilisés pourront être significativement différents.

3.2 RECUEIL DES INFORMATIONS INDISPENSABLES A L'ANALYSE DES RISQUES

Le recueil des informations nécessaires à l'analyse des risques est probablement une des phases les plus longues du processus mais également une des plus importantes.

Avant de mettre en œuvre la démarche d'analyse des risques, il est généralement nécessaire de respecter les étapes suivantes :

- description fonctionnelle et technique du système,
- description de son environnement,
- identification des potentiels de dangers internes et externes,
- analyse des incidents/accidents passés.

3.2.1 DESCRIPTION FONCTIONNELLE ET TECHNIQUE DU SYSTEME

La description fonctionnelle vise notamment à collecter l'ensemble des informations indispensables pour mener l'analyse.

De manière très générale, il s'agit de traiter les points suivants :

- identifier les fonctions du système étudié,
- caractériser la structure du système,
- définir les conditions de fonctionnement du système,
- décrire les conditions d'exploitation du système.

3.2.1.1 FONCTIONS DU SYSTEME

Des questions classiques du type « A quoi sert… ? » permettent d'identifier simplement les fonctions du système étudié.

L'identification de ces fonctions permet de caractériser les défaillances possibles du système. La défaillance d'un système peut être définie comme la cessation de l'aptitude d'une entité à accomplir une fonction requise.

Notons ici que, selon le système étudié (unités de process, stockages…), une défaillance du système (perte de la fonction) n'induit pas automatiquement la possibilité d'un phénomène dangereux (a fortiori d'un accident majeur). L'identification des fonctions globales du système s'avère utile pour décrire par la suite la structure du système et les fonctions de chacun de ses composants.

3.2.1.2 STRUCTURE DU SYSTEME

La définition de la structure du système vise à décrire les différents éléments qui le composent et plus précisément :

- leurs fonctions, performances et gammes de fonctionnement,
- leurs connexions et interactions,

- leurs localisations respectives.

Dans le même temps, il faut lister les substances présentes ou susceptibles d'être présentes dans le système étudié ainsi que les réactions chimiques mises en œuvre. Cette partie sera complétée par l'identification des dangers (voir 3.2.3.1).

Cette étape permet également de réunir les plans et schémas des installations et de s'assurer de leur mise à jour le cas échéant.

3.2.1.3 CONDITIONS DE FONCTIONNEMENT DU SYSTEME

Cette description vise à caractériser les états de fonctionnement du système ainsi que de ses composants, en particulier les états suivants : arrêt, fonctionnement normal, démarrage après un arrêt court ou prolongé…

Il est ainsi primordial de décrire le mode de gestion de transition du système ou de ses composants depuis un état vers un autre. De façon générale, il faut identifier les procédures de conduite du système, les consignes spécifiques en cas d'incident, …

Cette étape doit également permettre de définir les conditions dans lesquelles se trouvent les substances mises en jeu pour ces différents états (phase, température, pression…).

3.2.1.4 CONDITIONS D'EXPLOITATION

Les conditions d'exploitation regroupent les éléments qui concernent les conditions de surveillance du système (alarmes, inspections, vérification, tests périodiques) ainsi que les conditions d'intervention (maintenance préventive, corrective…).

3.2.2 ENVIRONNEMENT DU SYSTEME

La description de l'environnement du système est importante à double titre :

- l'environnement peut être une source d'agressions pour le système,
- l'environnement constitue généralement un ensemble d'éléments vulnérables pouvant être affectés en cas d'accident.

3.2.2.1 ELEMENTS VULNERABLES[11] PRESENTS DANS L'ENVIRONNEMENT

Afin d'apprécier la gravité d'un accident ou incident potentiel, il est indispensable de bien identifier les éléments de l'environnement qui pourraient être affectés. En règle générale, il convient de repérer les éléments suivants :

---

[11] Le terme cible a longtemps été utilisé pour désigner les éléments potentiellement atteints par l'accident. Dans le glossaire annexé à la circulaire du 7 octobre 2005, le Ministère de l'Ecologie et du Développement Durable préconise maintenant l'emploi des termes **élément vulnérable** ou **enjeu**.

- les personnes (personnel du site concerné, populations habitant ou travaillant autour de sites industriels),
- les installations et équipements externes au champ de l'étude et pouvant être à l'origine d'accidents (équipements dangereux),
- certains équipements indispensables pour maintenir le niveau de sécurité des installations (équipements de sécurité critiques comme une salle de contrôle, un local pomperie incendie, un réseau torche…),
- les biens et les structures dans l'environnement des installations,
- l'environnement naturel (nappes phréatiques, cours d'eau, sols…),
- d'autres parties des installations, en fonction des objectifs particuliers de l'analyse des risques.

3.2.2.2 SOURCES D'AGRESSIONS EXTERNES

Les sources d'agressions externes peuvent, quant à elles, être multiples. Il est difficile d'en donner un inventaire exhaustif. Néanmoins, voici quelques-unes des sources d'agressions qu'il convient généralement de repérer :

- Les sources d'agressions sur le site étudié :
  - autres installations et équipements dangereux,
  - zones de circulation, de travaux…
  - malveillance,
  - pertes d'utilité.
- Les sources d'agressions naturelles :
  - conditions météorologiques extrêmes (gel, vent, neige, brouillard…),
  - mouvements de terrain et séismes,
  - foudre,
  - inondations.
- Les sources d'agressions liées à l'activité humaine autour du site étudié :
  - présence d'établissements industriels proches,
  - transport de matières dangereuses sur des voies de communication proches, et canalisations de transport,
  - présence d'aéroports, aérodromes,
  - malveillance.
- Eléments exceptionnels (barrages, éoliennes…).

3.2.3 IDENTIFICATION DES POTENTIELS DE DANGERS

3.2.3.1 POTENTIELS DE DANGERS INTERNES

La définition des potentiels de dangers internes doit être réalisée de la façon la plus exhaustive possible en étudiant entre autres :

- les dangers liés aux produits (ou, plus exactement, les substances et préparations). Il s'agit alors de qualifier les dangers (inflammabilité, toxicité….) présentés par les produits présents ou susceptibles d'être présents sur le site en quantité suffisante pour être à l'origine d'un accident majeur. Dans le cadre de cet examen, il est également indispensable d'étudier les incompatibilités entre produits.
- les conditions opératoires. Il s'agit d'identifier les conditions opératoires pouvant présenter un danger intrinsèque ou augmenter la gravité d'un accident potentiel. Par exemple, il convient de repérer les installations fonctionnant à des pressions élevées ou encore les équipements intégrant des pièces tournant avec une énergie cinétique importante (compresseur par exemple).
- les réactions chimiques. Pour les procédés mettant en jeu des réactions physico-chimiques, une classification des réactions permet de mettre en lumière les réactions présentant des risques d'emballement ou des réactions incontrôlées dangereuses. Il est alors important de spécifier les conditions (température, pression, mélange…) à partir desquelles les réactions chimiques peuvent devenir dangereuses.[12] L'analyse des risques liés aux réactions chimiques n'est pas spécifiquement traitée dans le présent document, même si elle peut être partiellement abordée avec une méthode comme l'Hazop. En revanche le lecteur peut se référer à plusieurs rapports INERIS disponibles sur le sujet dont [Demissy 2005].

3.2.3.2 POTENTIELS DE DANGERS EXTERNES

L'identification des potentiels de dangers externes doit permettre de caractériser les risques d'agressions externes sur le système.

Si parfois un examen rapide de ces potentiels de dangers externes apporte des éléments de réponse satisfaisants, dans d'autres cas, il est nécessaire de mettre en œuvre des outils spécifiques. Cela peut notamment être le cas pour :

- les risques d'agressions sismiques,
- les risques d'inondation,
- les risques liés à la foudre (cf. Arrêté du 28 janvier 1993 concernant la protection contre la foudre de certaines installations classées)[13],
- les synergies d'accidents ou effets dominos.

---

[12] On peut utiliser à cet effet la fiche réaction donnée en annexe du cahier technique de l'UIC n°13 [UIC 1998].

[13] JO du 26 février 1993

Les méthodes permettant d'examiner ces risques ne sont pas traitées dans ce document mais font ou feront l'objet de documents spécifiques. Pour ce qui concerne les risques liés à la foudre, le lecteur pourra se reporter au rapport de l'INERIS " Ω-3 : Le risque foudre et les Installations Classées pour la Protection de l'Environnement " [Gruet 2001]. Il existe de même un "Guide pour la prise en compte du risque inondation" accessible sur le site de l'INERIS [Vallée 2004].

3.2.4 ANALYSE DES INCIDENTS/ACCIDENTS PASSES

L'analyse des accidents passés joue un rôle fondamental dans l'analyse des risques à de nombreux titres :

- Elle permet d'identifier a priori les incidents ou accidents susceptibles de se produire à partir :
  - des accidents ou incidents s'étant déjà produits sur le site étudié,
  - des accidents survenus sur des installations comparables à celles étudiées.
- Elle met en lumière les causes les plus fréquentes d'accidents et donne des renseignements précieux concernant les performances de certaines barrières de sécurité.
- Elle constitue une base de travail pertinente pour l'analyse des risques en groupe de travail qui devra identifier a priori des scénarios d'accidents.

Cette analyse porte à la fois sur les incidents et accidents survenus sur les installations étudiées ou sur des installations similaires.

3.3 DEFINITION DE LA DEMARCHE A METTRE EN OEUVRE

La définition précise de la démarche d'analyse des risques à mettre en œuvre demande notamment de choisir le ou les outils les mieux adaptés, de définir le groupe de travail qui participera à la réflexion et, le cas échéant, de fixer des échelles de cotation des risques et une grille de criticité.

3.3.1 CHOIX DES METHODES D'ANALYSE DES RISQUES

Il existe un grand nombre d'outils ou méthodes[14] dédiés à l'identification des dangers et des risques associés à un procédé ou une installation.

En 1990, M.Monteau et M. Favaro en avaient identifié une quinzaine particulièrement adaptés à l'analyse des risques professionnels. Tixier et al. en ont recensé 67 en 2002 en étendant le champ de l'analyse de risques à différentes situations et types de dangers.

---

[14] Les termes méthode et outil sont utilisé dans ce document avec un sens similaire en considérant que les méthodes d'analyse de risques constituent une catégorie d'outils à disposition de l'expert ou de l'industriel pour analyser les risques, au même titre que des modèles ou des référentiels. Il existe par ailleurs des outils informatiques qui permettent ou facilitent la mise en œuvre des méthodes décrites dans ce document. Il ne sera pas ici question de ce genre d'outils.

Quelques-unes des méthodes les plus fréquemment utilisées sont :

- l'Analyse Préliminaire des Risques (APR),
- l'Analyse des Modes de Défaillances, de leurs Effets et de leur Criticité (AMDEC),
- l'Analyse des risques sur schémas type HAZOP,
- la méthode « What-if ? » qui est une adaptation de la méthode HAZOP,
- l'Analyse par arbre des défaillances,
- l'Analyse par arbre d'évènements,
- l'Analyse par Nœud Papillon.

Ces méthodes prises individuellement ou de façon combinée permettent le plus souvent de répondre aux objectifs d'une analyse des risques portant sur un procédé ou une installation.

D'une manière générale, le choix de retenir une méthode particulière d'analyse des risques s'effectue à partir de son domaine d'application et de ses caractéristiques. Le Tableau 1 présenté au 3.3.1.3 peut être utilisé à cette fin. Au chapitre 1, le Tableau 16 apporte aussi des éléments de comparaison des méthodes simples et des méthodes intégrées d'évaluation des risques.

3.3.1.1 APPROCHE DEDUCTIVE / INDUCTIVE

Il existe deux grands types de démarches en vue d'analyser les risques : la démarche inductive et la démarche déductive.

Dans une approche inductive, une défaillance ou une combinaison de défaillances est à l'origine de l'analyse. Il s'agit alors d'identifier les conséquences de cette ou ces défaillances sur le système ou son environnement. On dit généralement que l'on **part des causes pour identifier les effets**. Les principales méthodes inductives utilisées dans le domaine des risques accidentels sont : l'Analyse Préliminaire des Risques, l'Analyse des Modes de Défaillance, de leurs Effets et de leurs Criticité (AMDEC), l'HAZOP, l'analyse par arbre d'évènements et What-If.

A l'inverse, dans une approche déductive, le système est supposé défaillant et l'analyse porte sur l'identification des causes susceptibles de conduire à cet état. **On part alors des effets pour remonter aux causes**. L'analyse par arbre des défaillances constitue une des principales méthodes déductives.

3.3.1.2 DEFAILLANCES INDEPENDANTES OU COMBINEES

La plupart des méthodes inductives (APR, AMDEC, HAZOP…) présentées dans ce document considère généralement des défaillances simples et indépendantes d'un élément ou composant du système.

Il s'agit d'une hypothèse qui permet de simplifier une démarche souvent complexe d'identification des sources de dangers potentielles. Elle correspond à une image biaisée de la réalité dans la mesure où l'analyse d'accidents met en lumière que les sinistres surviennent généralement suite aux défaillances combinées de plusieurs composants ou équipements.

Notons toutefois que ces méthodes peuvent être adaptées en vue de prendre en compte des combinaisons de défaillances et d'identifier des modes communs de défaillanc[15].

L'utilisation de méthodes arborescentes (arbre de défaillances ou d'évènements) permet de prendre en compte la succession ou la simultanéité de défaillances de plusieurs équipements ou composants, conduisant in fine à un accident potentiel.

De telles approches peuvent s'avérer particulièrement lourdes à mettre en place pour des systèmes complexes et sont généralement réservées à l'étude de points critiques mis en lumière par une première analyse plus simple.

Notons au passage que les méthodes s'appuyant sur l'utilisation d'arbres (de défaillances et/ou d'événements) permettent une évaluation quantitative de la probabilité des risques identifiés à condition que les données de base sur la fréquence des événements initiateurs ou les taux de défaillance des équipements soient disponibles.

3.3.1.3 DOMAINES D'APPLICATION

Les outils d'analyse des risques doivent être choisis en fonction des caractéristiques des installations à étudier et du niveau de détail recherché.

Ainsi, il est possible de différencier les méthodes telles que l'APR réservée à une analyse « en surface » des risques ou à des installations peu complexes et les méthodes dédiées à une analyse plus détaillée et généralement centrée sur des sous-systèmes bien définis, comme l'AMDEC, par exemple.

Bien entendu, le domaine d'application et le niveau de détail sont également fonction des compétences et de l'expérience des personnes qui mèneront ce travail. En d'autres termes, certains outils peuvent être adaptés afin d'être utilisés dans un domaine d'application sensiblement différent de leur domaine d'origine.

Ces différentes informations sont synthétisées dans le Tableau 1, pour les principales méthodes d'analyse des risques dans le domaine des risques accidentels.

---

[15] Un mode commun de défaillance désigne un événement qui, en raison de dépendances, provoque simultanément les défaillances de plusieurs composants du système.

Méthodes	*Approche*	*Défaillances envisagées*	*Niveau de détail*	*Domaines d'application privilégiés*
APR	Inductive	Indépendantes	+	Installations les moins complexes Etape préliminaire d'analyse
HAZOP	Inductive	Indépendantes	++	Systèmes thermo-hydrauliques
What-if	Inductive	Indépendantes	++	Systèmes thermo-hydrauliques
AMDEC	Inductive	Indépendantes	++	Sous-ensembles techniques bien délimités
Arbre d'évènements	Inductive	Combinées	+++	Défaillances préalablement identifiées
Arbre des défaillances	Déductive	Combinées	+++	Evènements redoutés ou indésirables préalablement identifiés
Nœud papillon	Inductive Déductive	Combinées	+++	Scénarios d'accidents jugés les plus critiques

Tableau 1 : Critères de choix pour les principales méthodes d'analyse des risques

En définitive, il n'y a pas de « bonne » ou « mauvaise » méthode d'analyse des risques. Ces méthodes ne sont que des aides guidant la réflexion et il convient donc de retenir celles qui sont les mieux adaptées aux cas à traiter.
D'ailleurs, ces méthodes peuvent être tout à fait complémentaires. En effet, une phase préliminaire d'analyse des risques menée grâce à une APR, par exemple, permet d'identifier les parties d'une installation pour lesquelles l'utilisation de méthodes plus détaillées comme l'AMDEC ou l'HAZOP s'avère pertinente. De la même façon, la mise en œuvre d'une AMDEC par exemple est souvent particulièrement utile en vue de construire un arbre des défaillances.

Enfin, signalons que, pour des installations particulièrement simples, une démarche systématique d'identification des risques peut tout à fait convenir, même si elle n'est pas référencée de manière formelle dans la littérature. Pour ces systèmes simples, l'usage de listes de contrôle (check-lists) permet en général de répondre de façon satisfaisante aux objectifs de l'analyse des risques.

3.3.2 CONSTITUTION D'UN GROUPE DE TRAVAIL

De manière générale, les méthodes d'analyse des risques sont destinées à être mises en œuvre dans le cadre d'un groupe de travail. Si leur utilisation par une personne seule n'est pas impossible, les résultats obtenus risquent néanmoins de perdre de leur pertinence. Leur intérêt réside en majeure partie dans la confrontation d'avis et de remarques de personnes ayant des expériences et des connaissances complémentaires. Cette richesse de points de vue permet généralement de tendre vers un examen le plus exhaustif possible des situations de dangers.

Au sein de l'équipe, il convient de distinguer les personnes assurant un rôle d'encadrement et d'orientation (animateur, secrétaire…) des autres membres du groupe de travail apportant une contribution uniquement technique.

3.3.2.1 CONTRIBUTION TECHNIQUE

L'équipe doit être **pluridisciplinaire**. Pour cela, elle doit être composée des personnes travaillant au quotidien sur les installations étudiées ou ayant une connaissance approfondie des installations (cas des projets).

La composition habituelle des participants contribuant sur les aspects techniques peut être, à titre d'exemple, la suivante :

- responsable du projet,
- personne chargée de la sécurité,
- personne spécialiste du procédé, ingénieur procédé,
- personne chargée de la maintenance,
- spécialiste de l'automation et des systèmes, instrumentistes, automaticiens…
- personne travaillant en production, exploitant…

La composition du groupe de travail est souvent fonction de l'installation étudiée. A ce titre, il peut être fait appel à des personnes travaillant dans le domaine électrique ou le génie civil. Néanmoins, il faut garder à l'esprit qu'une équipe ne doit pas comporter plus de sept ou huit personnes au total pour être efficace.

3.3.2.2 ENCADREMENT

Un animateur intervient, lors des sessions de travail, à la fois dans le rôle d'animation et de garant de la méthode. Il est généralement accompagné d'une personne, chargée du rôle de secrétaire et assurant la prise de notes.

L'animateur a un rôle clé durant l'analyse. Il guide l'équipe au travers de questions systématiques durant les sessions. Il doit veiller à faire participer tout le monde et faire en sorte que l'ambiance soit toujours sereine et la productivité maximale. Il doit avoir le souci permanent d'obtenir un consensus et éviter d'être trop directif.

Enfin, certains membres du groupe de travail peuvent se sentir mal à l'aise en considérant que leurs compétences ou savoir-faire pourraient être remis en cause lors des discussions. De ce fait, il est important que l'animateur n'hésite pas à mettre en avant les aspects positifs déjà existants (choix d'équipements, mise en place de plans de maintenance, installations de dispositifs de sécurité,...).

En pratique, le rôle d'animateur ou de secrétaire ne se limite généralement pas qu'à animer le groupe de travail. Grâce à leur connaissance des situations accidentelles (causes, conséquences,…) et des moyens d'y faire face, ces personnes sont souvent à même de participer efficacement à la réflexion. Ainsi, ils peuvent apporter des compléments au groupe de travail composé de personnes connaissant bien le système étudié mais n'étant pas forcément familières des situations accidentelles (phénomènes physiques, analyse des accidents passés…).

La tâche finale de l'animateur et du secrétaire est de réaliser le compte-rendu des séances en synthétisant le travail réalisé par le groupe.

Les étapes de l'analyse des risques décrites précédemment ont conduit à l'identification des risques associés à un site complet, une installation, un équipement particulier, ainsi qu'à celle des barrières (équipements ou activités humaines) permettant de maîtriser ces risques.

Cette étape essentiellement qualitative est riche d'enseignements puisqu'elle permet d'aborder de manière systématique les évènements pouvant conduire à un accident majeur, et en conséquence, d'identifier les mesures et équipements prévus ou à envisager en vue de maîtriser les risques associés.

Dans le domaine des risques accidentels, il est souvent indispensable de compléter cette démarche par une approche quantitative visant à estimer le niveau de risque des situations mises en lumière.

3.3.3 ECHELLES DE COTATION DES RISQUES

Dans ces cas, il faut définir en amont de l'analyse des échelles de cotation des risques en termes de probabilité et de gravité ainsi qu'une grille de criticité explicitant les critères d'acceptabilité sur lesquels le groupe de travail se fondera pour proposer des mesures de maîtrise supplémentaires.

Notons que l'INERIS préconise cette estimation semi-quantitative dans le cadre de l'analyse des risques d'accidents majeurs réalisée dans l'étude des dangers [Joly 2006].

3.3.3.1 ECHELLES DE PROBABILITE, D'INTENSITE ET DE GRAVITE

Les échelles de probabilité, de gravité et/ou d'intensité(cf.2.2), utilisées pour une évaluation quantitative simplifiée des risques doivent être adaptées à l'installation étudiée. A cet égard, les exploitants possédant la meilleure connaissance de leurs installations, il est légitime de retenir les échelles de cotation qu'ils proposent. Il faut néanmoins s'assurer que ces dernières sont bien adaptées à la problématique à traiter (étude des dangers, risques au poste de travail…). En particulier, lorsque les résultats de l'analyse de risque sont destinés à être utilisés dans un cadre réglementaire, comme c'est le cas pour l'étude de dangers, il est essentiel de s'assurer de la compatibilité des échelles utilisées avec celles définies dans les textes. La définition des échelles de cotation doit être acceptée par le groupe de travail avant le début de l'analyse, en correspondance avec les objectifs à atteindre.

Les tableaux suivants présentent des exemples d'échelles de cotation en probabilité, intensité et gravité que l'INERIS peut utiliser pour l'analyse des risques d'accidents majeurs dans le cadre de l'étude des dangers.

qualitative :		"Evènement extrêment probable"	"Evénement très improbable"	"Evènemen improbable"	"Evénement probable"	"Evènemen courant"	
***semi-quantitative* CLASSE PROBABILITE (de 0 à 6)**	**6**	10^{-6} **5**	10^{-5} **4**	10^{-4} **3**	10^{-3} **2**	10^{-2} **1**	10^{-1} **0** 1

Tableau 2 : Exemple d'échelle de cotation en probabilité

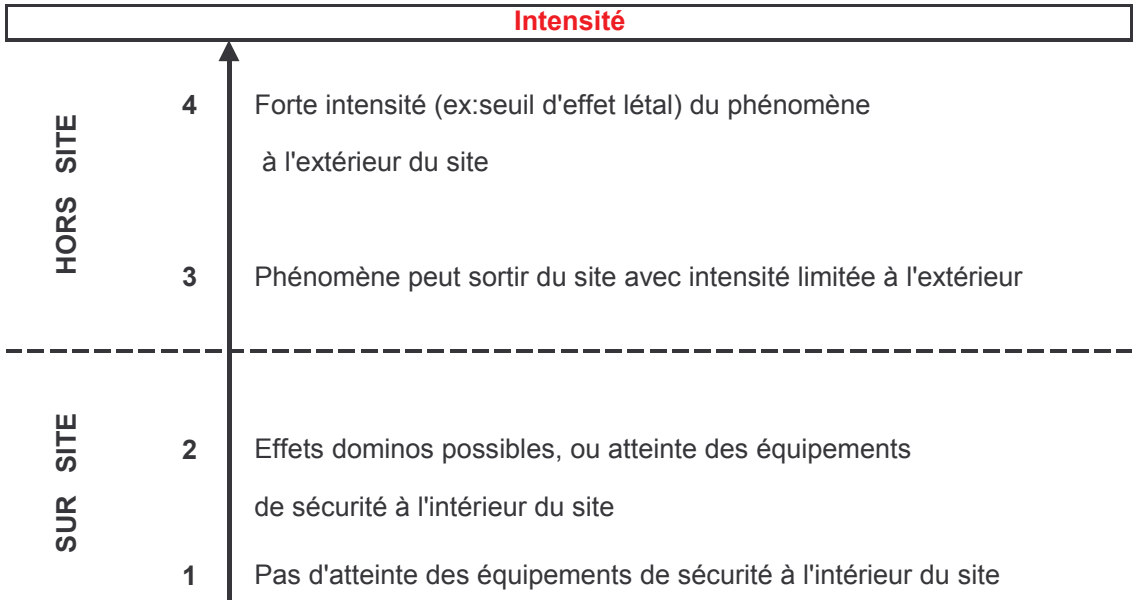


Figure 3 : Exemple d'échelle d'intensité utilisée pour les études de dangers

L'échelle de gravité présentée dans le Tableau 3 en page suivante est issue de 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. Elle se réfère aux seuils d'effet qui constituent des valeurs de référence pour l'estimation de l'intensité.

- Les seuils des effets irréversibles (SEI) délimitent la « zone des dangers significatifs pour la vie humaine ».
- Les seuils des effets létaux (SEL) correspondant à une CL 1 % délimitent la « zone des dangers graves pour la vie humaine ».
- Les seuils des effets létaux significatifs (SELS) correspondant à une CL 5 % délimitent la « zone des dangers très graves pour la vie humaine ».

Niveau de gravité des conséquences	Zone délimitée par le seuil des effets létaux significatifs	Zone délimitée par le seuil des effets létaux	Zone délimitée par le seuil des effets irréversibles sur la vie humaine
Désastreux	Plus de 10 personnes exposées (1)	Plus de 100 personnes exposées	Plus de 1000 personnes exposées
Catastrophique	Moins de 10 personnes exposées	Entre 10 et 100 personnes exposées.	Entre 100 et 1000 personnes exposées.
Important	Au plus 1 personne exposée	Entre 1 et 10 personnes exposées.	Entre 10 et 100 personnes exposées.
Sérieux	Aucune personne exposée	Au plus 1 personne exposée	Moins de 10 personnes exposées
Modéré	Pas de zone de létalité hors de l'établissement		Présence humaine exposée à des effets irréversibles inférieure à « une personne »
(1)Personnes exposées en tenant compte le cas échéant des mesures constructives visant à protéger les personnes contre certains effets et la possibilité de mise à l'abri des personnes en cas d'occurrence d'un phénomène dangereux si la cinétique de ce dernier et de la propagation de ses effets le permettent			

Tableau 3 : Echelle de gravité définie par l'arrêté du 29 septembre 2005[16]

L'échelle de gravité présentée en Tableau 3 ne considère que les dommages causés aux personnes à l'extérieur de l'établissement. Suivant le contexte, il est pertinent de considérer des échelles du même type pour les dommages causés à l'environnement ou aux travailleurs de l'établissement.

3.3.3.2 GRILLE DE CRITICITE

La grille de criticité permet au groupe de travail de définir les couples (Probabilité ; Gravité) ou (Probabilité; Intensité) correspondant à des risques jugés inacceptables ou devant faire l'objet d'action de maîtrise des risques de façon prioritaire. Il faut noter qu'il n'est pas nécessairement dans le mandat du groupe de travail de statuer sur l'acceptabilité d'un risque et de se prononcer sur la nécessité de mettre en place des mesures de sécurité supplémentaire. Il peut être amené à positionner les scénario dans une grille ne contenant aucune information sur le niveau d'acceptabilité ou proposer des mesures de réduction du risque qui ne seront pas retenues en application par exemple du critère ALARP du fait de leur coût excessif au regard du bénéfice attendu. Dans le contexte de l'étude de dangers, c'est in fine l'administration qui se prononce sur la nécessité de mettre en place des mesures supplémentaires.

Le Tableau 4 présente un exemple de grille de criticité générique classique. Les échelles d'intensité et de probabilité utilisées sont celles présentées en Tableau 2 et Figure 3.

---

16 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, JO n° 234 du 7 octobre 2005

Dans cette grille, le domaine gris foncé désigne les couples (intensité ; probabilité) des scénarios d'accidents qui sont considérés comme inacceptables.

L'objectif final de l'analyse des risques consiste ici à démontrer qu'aucun scénario d'accident ne se trouve dans cette zone grâce aux barrières de sécurité mises en place ou proposées au cours de l'étude.

Le domaine gris clair représente les risques jugés critiques pour lesquels les mesures de sécurité mises en place ont été jugées suffisantes en regard des risques. Néanmoins, compte tenu de l'intensité de ces accidents potentiels, un niveau de maîtrise optimal doit être maintenu pour assurer les performances des barrières de sécurité mises en place.

Dans le cadre de la maîtrise des accidents majeurs, cela passe notamment par des actions humaines et l'identification d'éléments Importants Pour la Sécurité (IPS).

Niveau d'intensité					
4					
3					
2					
1					
	6	5	4	3	***Niveau de probabilité***

	Risques jugés inacceptables
	Risques critiques

Tableau 4 : Exemple de grille de criticité

3.4 MISE EN ŒUVRE DE L'ANALYSE DES RISQUES EN GROUPE DE TRAVAIL

3.4.1 MISE EN CONDITION DU GROUPE DE TRAVAIL

Les personnes composant le groupe de travail ont été retenues pour leurs compétences (connaissances et expérience) dans des domaines techniques spécifiques. Elles ne sont pas obligatoirement familiarisées avec l'usage d'outils d'analyse des risques.

En conséquence, il est indispensable, avant d'entamer toute réflexion de :

- rappeler les objectifs de la réunion de travail,
- décrire précisément la démarche et les outils d'analyse qui ont été retenus,
- présenter, le cas échéant, les échelles de cotation des risques et la grille de criticité qui pourront être utilisées en vue d'estimer les risques.

Ces tâches incombent à l'animateur qui veillera à obtenir l'accord du groupe de travail avant d'entamer l'analyse.

De plus, il est souhaitable de rappeler les principales caractéristiques du système étudié (description fonctionnelle, substances et produits, environnement…), d'examiner rapidement les plans qui serviront de base à l'analyse et de réaliser une nouvelle visite des installations lorsqu'il ne s'agit pas d'un projet de construction nouvelle.

Par ailleurs, une synthèse des accidents survenus sur des installations similaires est présentée au groupe de travail. Ce dernier point permet une première estimation des risques et de montrer, le cas échéant, que des installations semblables ont effectivement pu être l'objet d'accidents plus ou moins graves.

3.4.2 MISE EN OEUVRE

L'analyse des risques en groupe de travail s'apparente à un travail de remue-méninges (« brainstorming »). Il s'agit d'envisager de la façon la plus exhaustive l'ensemble des risques générés en s'appuyant sur des méthodes systématiques d'analyse.

Lors de l'analyse des risques en groupe, quel que soit l'outil utilisé, il s'agit d'identifier une dérive ou défaillance de départ, d'en identifier l'ensemble des causes et enfin, d'en caractériser l'ensemble des conséquences (à savoir les effets sur les éléments vulnérables). Pour chaque cause et conséquence, le groupe de travail doit ensuite identifier l'ensemble des barrières de sécurité existantes.

Sur la base de cette identification, le groupe de travail estime le risque en termes de probabilité et gravité de façon quantitative ou semi-quantitative, voire qualitative. Il peut ensuite évaluer si les risques sont maîtrisés ou non. Pour cela, il peut s'appuyer sur une grille de criticité qu'il aura préalablement approuvée ou qui lui aura été fournie par le décideur.

Si les risques sont jugés insuffisamment maîtrisés, le groupe de travail peut proposer des mesures de réduction des risques supplémentaires jusqu'à un niveau de risques acceptable.

La démarche est ensuite de nouveau mise en œuvre en considérant une nouvelle dérive ou défaillance de départ.

3.4.3 SYNTHESE DE L'ANALYSE

Suite aux réflexions du groupe de travail, une synthèse des travaux doit être réalisée. Cette synthèse permet de mettre en lumière les principales conclusions du groupe et d'identifier clairement les points critiques qui devraient être étudiés de façon plus détaillée à l'aide d'outils plus spécifiques.

La mise au propre des notes prises au cours des réunions de travail est également primordiale pour assurer la traçabilité des travaux.

3.5 REMARQUE

La démarche d'analyse des risques proposée dans ce chapitre se veut volontairement générale. Dans le cadre particulier de la prévention des accidents majeurs et de l'étude des dangers, le lecteur est invité à se reporter au document de l'INERIS consacré à l'étude des dangers (voir le rapport Oméga 9 « Etude des dangers d'une Installation Classée pour la Protection de l'Environnement » [Joly 2009]).

Ce document décrit dans le détail la démarche particulière à mettre en œuvre pour identifier et démontrer la maîtrise des risques d'accidents majeurs.

4 LES METHODES CLASSIQUES D'ANALYSE DES RISQUES

Les principales méthodes d'analyse des risques d'accidents sont :

- l'Analyse Préliminaire des Risques (APR),
- l'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC),
- l'Analyse des risques sur schémas type HAZOP,
- la méthode « What-if ? »,
- l'Analyse par arbres des défaillances,
- l'Analyse par arbres d'évènements,
- l'Analyse par Nœud Papillon.

Il existe bien entendu de nombreuses autres méthodes qui ne seront pas présentées en détail dans ce document. Néanmoins, pour plus de précisions, le lecteur pourra consulter utilement l'article de Jerôme Tixier [Tixier 2002] et les deux articles écrits par Marc Favaro et Michel Monteau de l'INRS [Monteau 1990] déjà cités.

La description des outils présentés dans ce chapitre a été réalisée notamment à partir des ouvrages suivants :

- Sureté de Fonctionnement des systèmes industriels
  A. VILLEMEUR, Collection de la Direction des Etudes et Recherches d'Electricité de France, n°67, Ed. Eyrolles, 1988
- Cahiers de sécurité n°13 : Sécurité des Installations – méthodologie de l'analyse des risques
  Union des Industries Chimiques, Document Technique DT 54, Mars 1998
- Guidelines for Hazard Evaluation Procedures
  Center for Chemical Process Safety, American Institute of Chemical Engineers (AICHE), 1992
- Norme CEI 60812: 1985:
  « Techniques d'Analyse de la Fiabilité des Systèmes – Procédure d'Analyse des Modes de Défaillances et de leurs Effets (AMDE) »
- Norme CEI 61882 : 2001
  « Etudes de danger et d'exploitabilité (études HAZOP) – Guide d'application »

4.1 ANALYSE PRELIMINAIRE DES RISQUES (APR)

4.1.1 HISTORIQUE ET DOMAINE D'APPLICATION

L'Analyse Préliminaires des Risques (Dangers) a été développée au début des années 1960 dans les domaines aéronautiques et militaires. Elle est utilisée depuis dans de nombreuses autres industries. L'Union des Industries Chimiques (UIC) recommande son utilisation en France depuis le début des années 1980.

L'Analyse Préliminaire des Risques (APR) est une méthode d'usage très général couramment utilisée pour l'identification des risques au stade préliminaire de la conception d'une installation ou d'un projet. En conséquence, cette méthode ne nécessite généralement pas une connaissance approfondie et détaillée de l'installation étudiée.

En ce sens, elle est particulièrement utile dans les situations suivantes :

- au stade de la conception d'une installation, lorsque la définition précise du procédé n'a pas encore été effectuée. Elle fournit une première analyse de sécurité se traduisant par des éléments constituant une ébauche des futures consignes d'exploitation et de sécurité. Elle permet également de choisir les équipements les mieux adaptés (avant projet sommaire).
- dans le cas d'une installation complexe existante, au niveau d'une démarche d'analyse des risques. Comme l'indique son nom, l'APR constitue une étape préliminaire, permettant de mettre en lumière des éléments ou des situations nécessitant une attention plus particulière et en conséquence l'emploi de méthodes d'analyses de risques plus détaillées. Elle peut ainsi être complétée par une méthode de type AMDEC, HAZOP ou arbre des défaillances par exemple.
- dans le cas d'une installation dont le niveau de complexité ne nécessite pas d'analyses plus poussées au regard des objectifs fixés au départ de l'analyse des risques.

4.1.2 PRINCIPE

L'Analyse Préliminaire des Risques nécessite dans un premier temps d'identifier les éléments dangereux de l'installation. Ces éléments dangereux désignent le plus souvent :

- des substances ou préparations dangereuses, que ce soit sous forme de matières premières, de produits finis, d'utilités…,
- des équipements dangereux comme, par exemple, des stockages, zones de réception-expédition, réacteurs, fournitures d'utilités (chaudière…),
- des opérations dangereuses associées au procédé.

L'identification de ces éléments dangereux est fonction du type d'installation étudiée. L'APR peut-être mise en œuvre sans ou avec l'aide de liste de risques types ou en appliquant les mots guides Hazop (dérives de paramètres de fonctionnement). A titre indicatif, on pourra se référer à la liste fournie en Annexe 1.

Il est également à noter que l'identification de ces éléments se fonde sur la description fonctionnelle réalisée avant la mise en œuvre de la méthode.

A partir de ces éléments dangereux, l'APR vise à identifier, pour un élément dangereux, une ou plusieurs **situations de danger**. Dans le cadre de ce document, une situation de danger est définie comme une situation qui, si elle n'est pas maîtrisée, peut conduire à l'exposition d'enjeux à un ou plusieurs phénomènes dangereux.

Le groupe de travail doit alors déterminer les causes et les conséquences de chacune des situations de danger identifiées puis identifier les sécurités existantes sur le système étudié. Si ces dernières sont jugées insuffisantes vis-à-vis du niveau de risque identifié dans la grille de criticité, des propositions d'amélioration doivent alors être envisagées.

4.1.3 DEROULEMENT

L'utilisation d'un tableau de synthèse constitue un support pratique pour mener la réflexion et résumer les résultats de l'analyse. Pour autant, l'analyse des risques ne se limite pas à remplir coûte que coûte un tableau. Par ailleurs, ce tableau doit parfois être adapté en fonction des objectifs fixés par le groupe de travail préalablement à l'analyse.

Le tableau ci-dessous est donc donné à titre d'exemple.

Fonction ou système :						Date :	
1	2	3	4	5	6	7	8
N°	Produit ou équipement	Situation de danger	Causes	Conséquences	Sécurités existantes	Propositions d'amélioration	Observations

Tableau 5 : Exemple de tableau de type « APR »

Pour chaque fonction identifiée dans la phase de description des installations, les produits ou équipements sont passés en revue, en examinant les situations de danger potentielles de manière systématique. Pour cela, il est fait appel à l'expérience et à l'imagination de chacun. L'analyse d'accidents constitue de plus une source d'information à privilégier.

Le groupe de travail peut alors adopter une démarche systématique sous la forme suivante :

- Sélectionner le système ou la fonction à étudier sur la base de la description fonctionnelle réalisée.
- Choisir un équipement ou produit pour ce système ou cette fonction (colonne 2).
- Pour cet équipement, considérer une première situation de danger (colonne 3)
- Pour cette situation de danger, envisager toutes les causes et les conséquences possibles (colonnes 4 et 5).
- Pour un enchaînement cause - situation de danger - conséquences donné, identifier alors les barrières de sécurité existantes sur l'installation (colonne 6)
- Si le risque ainsi estimé est jugé inacceptable, formuler des propositions d'améliorations en colonne 7. La dernière colonne (colonne 8) est réservée à d'éventuels commentaires. Elle est particulièrement importante pour faire apparaître les hypothèses effectuées durant l'analyse ou les noms de personnes devant engager des actions complémentaires.
- Envisager alors un nouvel enchaînement cause - situation de danger - conséquences pour la même situation de danger et retourner au point 5).
- Si tous les enchaînements ont été étudiés, envisager une nouvelle situation de danger pour le même équipement et retourner au point 4).
- Lorsque toutes les situations de danger ont été passées en revue pour l'équipement considéré, retenir un nouvel équipement et retourner au point 3) précédent.
- Le cas échéant, lorsque tous les équipements ont été examinés, retenir un nouveau système ou fonction et retourner au point 2).

Une des premières difficultés rencontrées en pratique au cours d'une APR tient dans la définition du terme « situation de danger ». Il n'est en effet pas rare de constater au cours de l'analyse que des causes ou conséquences d'une situation de danger soient à leur tour identifiées comme situations de danger plus tard lors de l'analyse. Cette difficulté peut rendre délicate l'appropriation de la méthode par le groupe de travail. Toutefois, elle ne doit pas être considérée comme un frein pour l'analyse des risques mais au contraire, comme un moyen pour tendre vers plus d'exhaustivité.

Prenons l'exemple d'un réservoir de liquide inflammable type essence. Le groupe de travail identifie dans un premier temps comme situation de danger, un feu se développant dans la cuvette de rétention. La cause de cet incendie serait l'épandage de combustible dans la cuvette associé à la présence d'une source d'inflammation. Si ensuite le groupe de travail considère l'épandage seul d'essence comme situation de danger, il identifiera probablement en terme de conséquences le feu de nappe mais également la formation d'un nuage inflammable suite à l'évaporation de la nappe.

Précisons enfin que des colonnes peuvent être ajoutées au Tableau 5 afin de recueillir les résultats de l'estimation des risques réalisée en groupe de travail.

4.1.4 LIMITES ET AVANTAGES

Le principal avantage de l'Analyse Préliminaire des Risques est de permettre un examen relativement rapide des situations dangereuses sur des installations. Par rapport aux autres méthodes présentées ci-après, elle apparaît comme relativement économique en terme de temps passé et ne nécessite pas un niveau de description du système étudié très détaillé. Cet avantage est bien entendu à relier au fait qu'elle est généralement mise en œuvre au stade de la conception des installations.

En revanche, l'APR ne permet pas de caractériser finement l'enchaînement des évènements susceptibles de conduire à un accident majeur pour des systèmes complexes.

Comme son nom l'indique, il s'agit à la base d'une méthode préliminaire d'analyse qui permet d'identifier des points critiques devant faire l'objet d'études plus détaillées. Elle permet ainsi de mettre en lumière les équipements ou installations qui peuvent nécessiter une étude plus fine menée grâce à des outils tels que l'AMDEC, l'HAZOP ou l'analyse par arbre des défaillances. Toutefois, son utilisation seule peut être jugée suffisante dans le cas d'installations simples ou lorsque le groupe de travail possède une expérience significative de ce type d'approches.

4.2 AMDE ET AMDEC

4.2.1 HISTORIQUE ET DOMAINE D'APPLICATION

L'Analyse des Modes de Défaillance et de leurs Effets (AMDE) a été employée pour la première fois dans le domaine de l'industrie aéronautique durant les années 1960.

Son utilisation s'est depuis largement répandue à d'autres secteurs d'activités tels que l'industrie chimique, pétrolière ou le nucléaire.

De fait, elle est essentiellement adaptée à l'étude des défaillances de matériaux et d'équipements et peut s'appliquer aussi bien à des systèmes de technologies différentes (systèmes électriques, mécaniques, hydrauliques…) qu'à des systèmes alliant plusieurs techniques.

4.2.2 PRINCIPE

L'Analyse des Modes de Défaillance et de leurs Effets repose notamment sur les concepts de :

- défaillance, soit la cessation de l'aptitude d'un élément ou d'un système à accomplir une fonction requise,
- mode de défaillance, soit l'effet par lequel une défaillance est observée sur un élément du système,
- cause de défaillance, soit les évènements qui conduisent aux modes de défaillances,
- effet d'un mode de défaillance, soit les conséquences associées à la perte de l'aptitude d'un élément à remplir une fonction requise.

En pratique, il est souvent difficile de bien distinguer ces différentes notions. La maîtrise de ce vocabulaire est néanmoins primordiale pour une bonne utilisation de cet outil.

Pour illustrer ces différents concepts, prenons l'exemple d'une pompe. Dans des conditions normales d'exploitation, la fonction de cette pompe est définie comme son aptitude à fournir un débit donné à sa sortie. Si le débit en sortie de pompe est nul ou nettement inférieur ou supérieur à ce débit défini, la pompe sera dite « défaillante ».

Si, en cours d'exploitation, la pompe s'arrête de façon non désirée, on assistera bien à une défaillance de la pompe. Le fait que la pompe s'arrête constitue donc un effet par lequel une défaillance est observée ; il s'agit d'un mode de défaillance.

La coupure de courant qui a entraîné l'arrêt de la pompe sera alors définie comme une des causes de ce mode de défaillance. L'arrêt de l'approvisionnement du réacteur alimenté par cette pompe suivi d'une dégradation du produit de synthèse constitueront des conséquences de cette défaillance.

L'AMDE est une méthode inductive d'analyse qui permet :

- d'évaluer les effets et la séquence d'évènements provoqués par chaque mode de défaillance des composants d'un système sur les diverses fonctions de ce système,
- déterminer l'importance de chaque mode de défaillance sur le fonctionnement normal du système et en évaluer l'impact sur la fiabilité et la sécurité du système considéré,
- hiérarchiser les modes de défaillance connus suivant la facilité que l'on a à les détecter et les traiter.

Lorsqu'il est nécessaire d'évaluer la criticité d'une défaillance (probabilité et gravité), l'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC) apparaît comme une suite logique à l'AMDE. L'AMDEC reprend en effet les principales étapes de l'AMDE et y ajoute une évaluation semi-quantitative de la criticité. Cette dernière peut, par exemple, être réalisée sur la base des échelles proposées au paragraphe 3.3.3.1.

4.2.3 DEROULEMENT

De manière très schématique, une AMDEC se déroule sous la forme suivante :

- Dans un premier temps, **choisir un élément ou composant** du système.
- **Retenir un état de fonctionnement** (fonctionnement normal, arrêt…).
- Pour cet élément ou composant et pour cet état, retenir **un premier mode de défaillance**.
- Identifier les **causes** de ce mode de défaillance ainsi que ses **conséquences** tant au niveau du voisinage du composant que sur tout le système.
- Examiner les **moyens** permettant de **détecter** le mode de défaillance d'une part, et ceux prévus pour en **prévenir l'occurrence** ou en **limiter les effets**.
- Procéder à l'évaluation de la criticité de ce mode de défaillance en terme de probabilité et de gravité.
- Prévoir des **mesures ou moyens supplémentaires** si l'évaluation du risque en montre la nécessité.
- Vérifier que le couple (P,G) peut être jugé comme acceptable.
- Envisager un **nouveau mode de défaillance** et reprendre l'analyse au point 4).
- Lorsque tous les modes de défaillances ont été examinés, **envisager un nouvel état de fonctionnement** et reprendre l'analyse au point 3).
- Lorsque tous les états de fonctionnement ont été considérés, choisir **un nouvel élément ou composant** du système et reprendre l'analyse au point 2).

Dans les faits, il est intéressant de se doter de tableaux tant en qualité de support pour mener la réflexion que pour la présentation des résultats. Un exemple de tableau est fourni ci-dessous.

1	2	3	4	5	6	7	8	9	10	11
Equipement Repère	Fonctions, états	Mode de défaillance	Causes de défaillance	Effet local	Effet final	Moyens de détection	Dispositions compensatoires	P	G	Remarques

Tableau 6 : Exemple d'un tableau de type AMDEC

Les cases de ce tableau s'utilisent de la façon suivante :

4.2.3.1 EQUIPEMENT (COLONNE 1)

Dans cette première colonne, il s'agit de passer en revue chaque équipement ou composant identifié lors de la description fonctionnelle.

Il est généralement utile de repérer l'équipement considéré à partir des données fournies dans des diagrammes ou autres plans.

4.2.3.2 FONCTIONS ET ETATS (COLONNE 2)

Pour chacun des équipements, il s'agit de lister ses fonctions et états de fonctionnement.

Ces fonctions et états sont normalement identifiés au cours de la description fonctionnelle. Afin de mener l'analyse de la manière la plus complète possible, il est indispensable de considérer l'ensemble des états susceptibles de survenir au cours de l'exploitation (ex. fonctionnement normal, arrêt, démarrage, stand-by…)

4.2.3.3 MODES DE DEFAILLANCE (COLONNE 3)

Pour chaque équipement et en fonction de l'état de fonctionnement, le groupe de travail doit envisager de manière systématique les modes de défaillance possibles (Colonne 3).

La définition des modes possibles de défaillance pour un équipement peut être réalisée à partir du retour d'expérience associé à l'exploitation d'équipements similaires, de tests ou essais…

Par ailleurs, les modes de défaillance considérés devront tenir compte :

- des utilisations du système,
- des caractéristiques de l'équipement considéré,
- du mode de fonctionnement,
- des spécifications relatives au fonctionnement,
- des délais fixés,
- de l'environnement.

Quel que soit le type d'équipement considéré, la liste suivante tirée de la norme CEI 60812:1985 : « *Techniques d'analyse de la fiabilité des systèmes – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)* » facilite l'identification des modes de défaillance par le groupe de travail.

1	Fonctionnement prématuré
2	Ne fonctionne pas au moment prévu
3	Ne s'arrête pas au moment prévu
4	Défaillance en fonctionnement

Tableau 7 : Modes de défaillance généraux (extrait du tableau II de la norme CEI 60812:1985)

1	Défaillance structurelle (rupture)
2	Blocage physique ou coincement
3	Vibrations
4	Ne reste pas en position
5	Ne s'ouvre pas
6	Ne se ferme pas
7	Défaillance en position ouverte
8	Défaillance en position fermée
9	Fuite interne
10	Fuite externe
11	Dépasse la limite supérieure tolérée
12	Est en dessous de la limite inférieure tolérée
13	Fonctionnement intempestif
14	Fonctionnement intermittent
15	Fonctionnement irrégulier
16	Indication erronée
17	Ecoulement réduit
18	Mise en marche erronée
19	Ne s'arrête pas
20	Ne démarre pas
21	Ne commute pas
22	Fonctionnement prématuré
23	Fonctionnement après le délai prévu (retard)
24	Entrée erronée (augmentation)
25	Entrée erronée (diminution)
26	Sortie erronée (augmentation)
27	Sortie erronée (diminution)
28	Perte de l'entrée
29	Perte de la sortie
30	Court-circuit (électrique)
31	Circuit ouvert (électrique)
32	Fuite (électrique)
33	Autres conditions de défaillance exceptionnelles suivant les caractéristiques du système, les conditions de fonctionnements et les contraintes opérationnelles

Tableau 8 : Modes de défaillance génériques (extrait du tableau II de la norme CEI 60812:1985)

De plus, cette même norme propose une liste-guide de modes de défaillance génériques (Tableau 8), qui permet d'aider le groupe de travail dans l'analyse. Cette liste est reprise ci-après. Elle présente une série de modes de défaillance génériques pouvant s'appliquer en théorie à tous les cas de figure envisageables. Néanmoins, elle pourra être utilement complétée en vue de tenir compte des spécificités du système étudié.

4.2.3.4 CAUSES DE DEFAILLANCE (COLONNE 4)

Pour chaque mode de défaillance, le groupe de travail doit ensuite identifier les causes potentielles conduisant à ce mode de défaillance. Un mode de défaillance peut résulter de plusieurs causes, qu'il convient donc d'inventorier et de numéroter pour plus de facilité.

La liste présentée dans le Tableau 8 précédent permet également de préciser des causes de défaillance dans la mesure où ces causes peuvent parfois s'apparenter à des modes de défaillance.

Par exemple, un mode de défaillance d'une vanne devant se fermer peut être « Ne se ferme pas » (mode de défaillance n°6). Une des causes de ce mode de

défaillance peut être un blocage physique ou coincement (mode de défaillance n°2).

Enfin, il convient de tenir compte des défaillances possibles sur les équipements adjacents du système. L'évaluation des effets d'une défaillance d'un élément peut effectivement conduire à l'occurrence d'un mode de défaillance sur un autre élément du système. Il est ainsi nécessaire de veiller à l'adéquation entre les effets de défaillance considérés au cours de l'analyse et les causes d'autres modes de défaillance envisagés.

4.2.3.5 EFFETS DE LA DEFAILLANCE (COLONNES 5 ET 6)

De la même façon que le groupe de travail s'est attaché à identifier les causes potentielles de défaillance, il doit examiner les conséquences de cette défaillance, au niveau du composant lui-même tout d'abord (colonne 5) puis au niveau du système global (colonne 6).

4.2.3.6 MOYENS DE DETECTION (COLONNE 7)

Pour le mode de défaillance envisagé, le groupe de travail examine et consigne ensuite les moyens prévus pour détecter ce mode de défaillance.

4.2.3.7 DISPOSITIONS COMPENSATOIRES (COLONNE 8)

Toutes les dispositions prises, par exemple au niveau de la conception de l'installation, en vue de prévenir ou atténuer l'effet du mode de défaillance doivent alors être examinées. Cette étape, dont les résultats sont consignés en colonne 8, vise d'une certaine façon à caractériser le comportement du système lorsqu'un de ses composants est affecté par un mode de défaillance.

4.2.3.8 EVALUATION DE LA CRITICITE (COLONNES 9 ET 10)

Les colonnes 9 et 10 permettent de consigner les estimations réalisées par le groupe de travail de la probabilité du mode de défaillance (P) et de la gravité associée à ses conséquences (G). Cette approche permet de mesurer l'influence des barrières de sécurité mises en place et de juger de la pertinence d'envisager de nouvelles barrières au regard du risque présenté.

En pratique, il est parfois difficile de disposer de données précises et fiables pour procéder de manière fine à cette évaluation. On pourra alors se référer utilement à des échelles de cotations à plusieurs niveaux de probabilité et de gravité, semblables à celles présentées au paragraphe 3.3.3.1. Rappelons que les échelles de gravité et probabilité quels que soient les formats finalement retenus, doivent être présentées et acceptées en début d'analyse.

4.2.4 LIMITES ET AVANTAGES

L'AMDEC s'avère très efficace lorsqu'elle est mise en œuvre pour l'analyse de défaillances simples d'éléments conduisant à la défaillance globale du système. De par son caractère systématique et sa maille d'étude généralement fine, elle constitue un outil précieux pour l'identification de défaillances potentielles et les moyens d'en limiter les effets ou d'en prévenir l'occurrence.

Comme elle consiste à examiner chaque mode de défaillance, ses causes et ses effets pour les différents états de fonctionnement du système, l'AMDEC permet d'identifier les modes communs de défaillances pouvant affecter le système étudié. Les modes communs de défaillances correspondent à des événements qui de par leur nature ou la dépendance de certains composants, provoquent simultanément des états de panne sur plusieurs composants du système. Les pertes d'utilités ou des agressions externes majeurs constituent par exemple, en règle générale, des modes communs de défaillance.

Dans le cas de systèmes particulièrement complexes comptant un grand nombre de composants, l'AMDEC peut être très difficile à mener et particulièrement fastidieuse compte tenu du volume important d'informations à traiter. Cette difficulté est décuplée lorsque le système considéré comporte de nombreux états de fonctionnement.

Par ailleurs, l'AMDEC considère des défaillances simples et peut être utilement complétée, selon les besoins de l'analyse, par des méthodes dédiées à l'étude de défaillances multiples comme l'analyse par arbre des défaillances par exemple.

4.3 HAZOP

4.3.1 HISTORIQUE ET DOMAINE D'APPLICATION

La méthode HAZOP, pour HAZard OPerability, a été développée par la société Imperial Chemical Industries (ICI) au début des années 1970. Elle a depuis été adaptée dans différents secteurs d'activité utilisant des systèmes thermo-hydrauliques (chimie, pétrochimie…). L'Union des Industries Chimiques (UIC) a publié en 1980 une version française de cette méthode dans son cahier de sécurité n°2 intitulé « Etude de sécurité sur schéma de circulation des fluides ».

Considérant de manière systématique les dérives des paramètres d'une installation en vue d'en identifier les causes et les conséquences, cette méthode est particulièrement utile pour l'examen de **systèmes thermo-hydrauliques**, pour lesquels des paramètres comme le débit, la température, la pression, le niveau, la concentration… sont particulièrement importants pour la sécurité de l'installation.

De par sa nature, cette méthode requiert notamment l'examen de schémas et plans de circulation des fluides ou schémas P&ID (Piping and Instrumentation Diagram).

4.3.2 PRINCIPE

La méthode de type HAZOP est dédiée à l'analyse des risques des systèmes thermo-hydrauliques pour lesquels il est primordial de maîtriser des paramètres comme la pression, la température, le débit…

L'HAZOP suit une procédure assez semblable à celle proposée par l'AMDE. L'HAZOP ne considère plus des modes de défaillances mais les dérives potentielles (ou déviations) des principaux paramètres liés à l'exploitation de l'installation. De ce fait, elle est centrée sur le fonctionnement du procédé à la différence de l'AMDE qui est centrée sur le fonctionnement des composants de l'installation. Les deux méthodes se rejoignent dans la mesure où les causes et les conséquences de dérives de paramètres peuvent être des défaillances de composants et réciproquement.

Pour chaque partie constitutive du système examiné (ligne ou maille), la génération (conceptuelle) des dérives est effectuée de manière systématique par la conjonction :

- de mots-clé comme par exemple « Pas de », « Plus de », « Moins de », « Trop de »
- des paramètres associés au système étudié. Des paramètres couramment rencontrés sont la température, la pression, le débit, la concentration, mais également le temps ou des opérations à effectuer.

Mot-clé + Paramètre = Dérive

Le groupe de travail doit ainsi s'attacher à déterminer les causes et les conséquences potentielles de chacune de ces dérives et à identifier les moyens existants permettant de détecter cette dérive, d'en prévenir l'occurrence ou d'en limiter les effets. Le cas échéant, le groupe de travail pourra proposer des mesures correctives à engager en vue de tendre vers plus de sécurité.

A l'origine, l'HAZOP n'a pas été prévue pour procéder à une estimation de la probabilité d'occurrence des dérives ou de la gravité de leurs conséquences. Cette méthode est donc parfois qualifiée de qualitative. En pratique, elle peut être couplée, comme l'AMDE, à une estimation de la criticité.
Néanmoins, dans le domaine des risques accidentels majeurs, une estimation a priori de la probabilité et de la gravité des conséquences des dérives identifiées s'avère souvent nécessaire. Dans ce contexte, l'HAZOP doit donc être complétée par une analyse de la criticité des risques sur les bases d'une technique quantitative simplifiée. Dans une première approche, une démarche semi-quantitative similaire à celle présentée au paragraphe 3.3.3 pourra être retenue.
Cette adaptation semi-quantitative de l'HAZOP est d'ailleurs mentionnée dans la norme CEI :61882 « Etudes de danger et d'exploitabilité (études HAZOP) – Guide d'application ».

4.3.3 DEROULEMENT

Le déroulement d'une étude HAZOP est sensiblement similaire à celui d'une AMDE. Il convient, pour mener l'analyse, de suivre les étapes suivantes :

- Dans un premier temps, choisir une **ligne ou une maille**. Elle englobe généralement un équipement et ses connexions, l'ensemble réalisant une fonction dans le procédé identifiée au cours de la description fonctionnelle ;
- Choisir un paramètre de fonctionnement ;
- Retenir un **mot-clé** et étudier la **dérive** associée ;
- Vérifier que **la dérive est crédible**. Si oui, passer au point 5, sinon revenir au point 3 ;
- Identifier les causes et les conséquences potentielles de cette dérive ;
- Examiner les **moyens** visant à **détecter** cette dérive ainsi que ceux prévus pour en **prévenir l'occurrence ou en limiter les effets** ;
- Proposer, le cas échéant, des **recommandations** et améliorations ;
- Retenir un **nouveau mot-clé** pour le même paramètre et reprendre l'analyse au point 3) ;
- Lorsque tous les mots-clé ont été considérés, retenir un **nouveau paramètre** et reprendre l'analyse au point 2) ;
- Lorsque toutes les phases de fonctionnement ont été envisagées, **retenir une nouvelle ligne** et reprendre l'analyse au point 1).

La démarche présentée ici est globalement cohérente avec la démarche présentée dans la norme CEI :61882 « Etudes de danger et d'exploitabilité (études HAZOP) – Guide d'application ».

Notons de plus que, dans le domaine des risques accidentels, il est souvent nécessaire de procéder à une estimation de la criticité des dérives identifiées.

Enfin, comme le précise la norme CEI :61882, il est également possible de dérouler l'HAZOP, en envisageant en premier lieu un mot-clé puis de lui affecter systématiquement les paramètres identifiés.

Tout comme pour l'APR et l'AMDEC présentées dans les paragraphes précédents, un tableau de synthèse se révèle souvent utile pour guider la réflexion et collecter les résultats des discussions menées au sein du groupe de travail.

Un exemple de tableau pouvant être utilisé est présenté et commenté dans les paragraphes suivants.

Date : Ligne ou équipement :								
1	2	3	4	5	6	7	8	9
N°	Mot clé	Paramètre	Causes	Conséquences	Détection	Sécurités existantes	Propositions d'amélioration	Observations

Tableau 9 : Exemple de tableau pour l'HAZOP

4.3.3.1 DEFINITION DES MOTS-CLE (COLONNE 2)

Les mots-clé, accolés aux paramètres importants pour le procédé, permettent de générer de manière systématique les dérives à considérer. La norme CEI : 61882 propose des exemples de mots-clé dont l'usage est particulièrement courant. Ces mots-clé sont repris dans le tableau ci-dessous, inspiré du Tableau 3 de la norme pré-citée.

Type de déviation	***Mot-Guide***	***Exemples d'interprétation***
Négative	NE PAS FAIRE	Aucune partie de l'intention n'est remplie
Modification quantitative	PLUS	Augmentation quantitative
	MOINS	Diminution quantitative
Modification qualitative	EN PLUS DE	Présence d'impuretés – Exécution simultanée d'une autre opération/étape
	PARTIE DE	Une partie seulement de l'intention est réalisée
Substitution	INVERSE	S'applique à l'inversion de l'écoulement dans les canalisations ou à l'inversion des réactions chimiques
	AUTRE QUE	Un résultat différent de l'intention originale est obtenu
Temps	PLUS TOT	Un événement se produit avant l'heure prévue
	PLUS TARD	Un événement se produit après l'heure prévue
Ordre séquence	AVANT	Un événement se produit trop tôt dans une séquence
	APRES	Un événement se produit trop tard dans une séquence

Tableau 10 : Exemples de mots-clé pour l'HAZOP (norme CEI : 61882)

4.3.3.2 DEFINITION DES PARAMETRES (COLONNE 3)

Les paramètres auxquels sont accolés les mots-clés dépendent bien sûr du système considéré. Généralement, l'ensemble des paramètres pouvant avoir une incidence sur la sécurité de l'installation doit être sélectionné. De manière fréquente, les paramètres sur lesquels porte l'analyse sont :

- la température,
- la pression,
- le débit,
- le niveau,
- la concentration,
- l'agitation,
- la quantité,
- l'absorption,
- la composition,
- la séparation,
- l'homogénéité,
- la viscosité…

La combinaison de ces paramètres avec les mots clé précédemment définis permet donc de générer des dérives de ces paramètres.

Par exemple :

- « Plus de » et « Température » = « Température trop haute »,
- « Moins de » et « Pression » = « Pression trop basse »,
- « Inverse » et « Débit » = « Retour de produit »,
- « Pas de » et « Niveau » = « Capacité vide ».

4.3.3.3 CAUSES ET CONSEQUENCES DE LA DERIVE (COLONNES 4 ET 5)

De la même façon que pour une AMDE, le groupe de travail, une fois la dérive envisagée, doit identifier les causes de cette dérive, puis les conséquences potentielles de cette dérive.

En pratique, il peut être difficile d'affecter à chaque mot clé (et dérive) une portion bien délimitée du système et en conséquence, l'examen des causes potentielles peut s'avérer, dans certains cas, complexe.

Afin de faciliter cette identification, il est utile de se référer à des listes guides telles que celle présentée en Annexe 3 à titre illustratif.

4.3.3.4 MOYENS DE DETECTION, SECURITES EXISTANTES ET PROPOSITIONS (COLONNES 6, 7 ET 8)

La méthode HAZOP prévoit d'identifier pour chaque dérive les moyens accordés à sa détection et les barrières de sécurité prévues pour en réduire l'occurrence ou les effets.

Si les mesures mises en place paraissent insuffisantes au regard du risque encouru, le groupe de travail peut proposer des améliorations en vue de pallier ces problèmes ou du moins définir des actions à engager pour améliorer la sécurité quant à ces points précis.

4.3.4 LIMITES ET AVANTAGES

L'HAZOP est un outil particulièrement efficace pour les systèmes thermo-hydrauliques. Cette méthode présente tout comme l'AMDE un caractère systématique et méthodique. Considérant, de plus, simplement les dérives de paramètres de fonctionnement du système, elle évite entre autres de considérer, à l'instar de l'AMDE, tous les modes de défaillances possibles pour chacun des composants du système.

En revanche, l'HAZOP ne permet pas dans sa version classique d'analyser les évènements résultant de la combinaison simultanée de plusieurs défaillances.

Par ailleurs, il est parfois difficile d'affecter un mot clé à une portion bien délimitée du système à étudier. Cela complique singulièrement l'identification exhaustive des causes potentielles d'une dérive. En effet, les systèmes étudiés sont souvent composés de parties interconnectées si bien qu'une dérive survenant dans une ligne ou maille peut avoir des conséquences ou à l'inverse des causes dans une maille voisine et inversement. Bien entendu, il est possible a priori de reporter les implications d'une dérive d'une partie à une autre du système. Toutefois, cette tâche peut rapidement s'avérer complexe.

Enfin, L'HAZOP traitant de tous types de risques, elle peut être particulièrement longue à mettre en oeuvre et conduire à une production abondante d'information ne concernant pas des scénarios d'accidents majeurs.

4.4 WHAT-IF

La méthode dite « What if » est une méthode dérivée de l'HAZOP. Elle suit donc globalement la même procédure. Cependant la méthode « What-if » prévoit une analyse moins profonde des événements, se contentant d'en considérer les conséquences sans en examiner les causes. Elle prévoit en revanche les actions d'amélioration à entreprendre.

Une autre différence concerne la génération des dérives des paramètres de fonctionnement. Ces dérives ne sont plus dans ce cas envisagées en tant que combinaison d'un mot clé et d'un paramètre, mais fondées sur une succession de questions de la forme : « QUE (What) se passe-t-il SI (IF) tel paramètre ou le comportement de tel composant est différent de celui normalement attendu ? ».

L'identification des paramètres ou des composants objet des questions est libre et ne repose pas comme dans l'Hazop sur des listes guides à utiliser systématiquement. Il apparaît ainsi que l'efficacité de la méthode « What if » est encore plus dépendante de l'expérience des personnes réunies au sein du groupe de travail.

Cette méthode paraît donc moins fastidieuse à mener que l'HAZOP mais est réservée à une équipe expérimentée et demeure limitée en termes de profondeur d'analyse, en particulier des causes de dérives. Elle s'apparente plus à une méthode de brainstorming.

Que se passe-t-il si … ?	Réponse	Probabilité/ vraissemblance	Conséquences	Recommandations

Tableau 11 : Exemple de tableau d'application de la méthode What-if[17]

4.5 ARBRE DES DEFAILLANCES

4.5.1 HISTORIQUE ET DOMAINE D'APPLICATION

L'analyse par arbre des défaillances fut historiquement la première méthode mise au point en vue de procéder à un examen systématique des risques. Elle a été élaborée au début des années 1960 par la compagnie américaine Bell Telephone et fut expérimentée pour l'évaluation de la sécurité des systèmes de tir de missiles.

Visant à déterminer l'enchaînement et les combinaisons d'évènements pouvant conduire à un événement redouté pris comme référence, l'analyse par arbre des défaillances est maintenant appliquée dans de nombreux domaines tels que l'aéronautique, le nucléaire, l'industrie chimique,…

Elle est également utilisée pour analyser a posteriori les causes d'accidents qui se sont produits. Dans ces cas, l'événement redouté final est généralement connu car observé. On parle alors d'analyse par arbre des causes, l'objectif principal étant de déterminer les causes réelles qui ont conduit à l'accident.

4.5.2 PRINCIPE

L'analyse par arbre de défaillances est une méthode de type déductif. En effet, il s'agit, à partir d'un événement redouté défini a priori, de déterminer les enchaînements d'évènements ou combinaisons d'évènements pouvant finalement conduire à cet événement. Cette analyse permet de remonter de causes en causes jusqu'aux **évènements de base** susceptibles d'être à l'origine de l'événement redouté.

---

[17] d'après Chemical Engineering Processes Laboratory, Course Manual, MIT, 1999, Appendix VI.

http://web.mit.edu/course/10/10.27/www/1027CourseManual/1027CourseManual-AppVI.html

Les évènements de base correspondent généralement à des :

- évènements élémentaires qui sont généralement suffisamment connus et décrits par ailleurs pour qu'il ne soit pas utile d'en rechercher les causes. Certains de ces événements élémentaires peuvent être suffisamment fréquents pour qu'il soit possible d'en estimer une probabilité future sur la base d'une analyse statistique. Ce n'est cependant pas toujours le cas et la probabilité des événements élémentaire demeure une donnée difficile à établir.
- évènements ne pouvant être considérés comme élémentaires mais dont les causes ne seront pas développées faute d'intérêt ;
- évènements dont les causes seront développées ultérieurement au gré d'une nouvelle analyse par exemple ;
- évènements survenant normalement et de manière récurrente dans le fonctionnement du procédé ou de l'installation.

Quelle que soit la nature des éléments de base identifiés, l'analyse par arbre des défaillances est fondée sur les principes suivants :

- ces évènements sont indépendants ;
- ils ne seront pas décomposés en éléments plus simples faute de renseignements, d'intérêt ou bien parce que cela est impossible ;
- leur fréquence ou leur probabilité d'occurrence peut être estimée.

Ainsi, l'analyse par arbre des défaillances permet d'identifier les successions et les combinaisons d'évènements qui conduisent des évènements de base jusqu'à l'événement indésirable retenu.

Les liens entre les différents évènements identifiés sont réalisés grâce à des portes logiques (de type « ET » et « OU » par exemple). Cette méthode utilise une symbolique graphique particulière qui permet de présenter les résultats dans une structure arborescente.

Le lecteur peut, par exemple se reporter aux conventions de présentation proposées dans la norme CEI 61025 :1990 « Analyse par Arbre de Panne (APP) ».

A l'aide de règles mathématiques et statistiques, il est alors théoriquement possible d'évaluer la probabilité d'occurrence de l'événement final à partir des probabilités des évènements de base identifiés.

L'analyse par arbre des défaillances d'un événement redouté peut se décomposer en trois étapes successives :

- définition de l'événement redouté étudié,
- élaboration de l'arbre,
- exploitation de l'arbre.

Il convient d'ajouter à ces étapes, une étape préliminaire de connaissance du système. Nous verrons que cette dernière est primordiale pour mener l'analyse et qu'elle nécessite le plus souvent une connaissance préalable des risques.

4.5.3 DEFINITION DE L'EVENEMENT REDOUTE

La définition de l'événement final, qui fera l'objet de l'analyse, est une étape cruciale pour la construction de l'arbre. On conçoit que plus cet événement est défini de manière précise, plus simple sera l'élaboration de l'arbre des défaillances. Par ailleurs, s'agissant d'une méthode qui peut se révéler rapidement lourde à mener, elle doit être réservée à des évènements jugés particulièrement critiques.

En ce sens, l'utilisation préalable de méthodes inductives (APR, AMDEC, HAZOP) permet d'identifier les évènements qui méritent d'être retenus pour une analyse par arbre des défaillances et d'identifier certains événements initiateurs qui pourront être développés dans l'arbres de défaillance.

De manière classique, les évènements considérés peuvent concerner le rejet à l'atmosphère de produits toxiques ou inflammables, le risque d'incendie, d'explosion…

4.5.4 ELABORATION DE L'ARBRE

La construction de l'arbre des défaillances vise à déterminer les enchaînements d'évènements pouvant conduire à l'événement final retenu. Cette analyse se termine lorsque toutes les causes potentielles correspondent à des évènements élémentaires.

L'élaboration de l'arbre des défaillances suit le déroulement présenté en Figure 4.

La recherche systématique des causes immédiates, nécessaires et suffisantes (INS) est donc à la base de la construction de l'arbre. Il s'agit probablement de l'étape la plus délicate et il est souvent utile de procéder à cette construction au sein d'un groupe de travail pluridisciplinaire. De plus, la mise en œuvre préalable d'autres méthodes d'analyse des risques de type inductif facilite grandement la recherche des défaillances pour l'élaboration de l'arbre, en particulier en cas de système complexe.

Afin de sélectionner les évènements intermédiaires, il est indispensable de procéder pas à pas en prenant garde à bien identifier les **causes directes et immédiates** de l'événement considéré et se poser la question de savoir si ces causes sont bien nécessaires et **suffisantes**. Faute de quoi, l'arbre obtenu pourra être partiellement incomplet voire erroné.

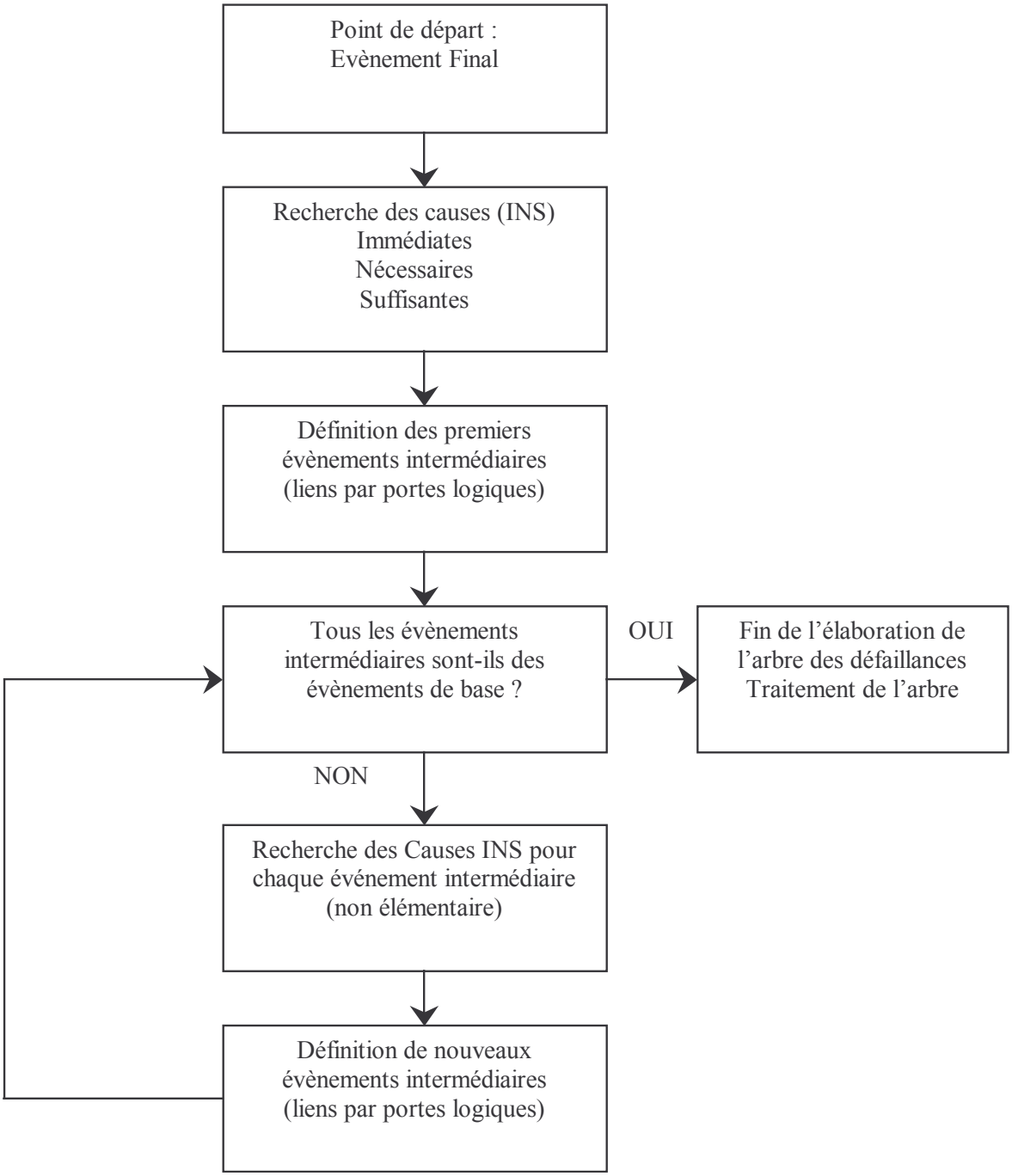


Figure 4 : Démarche pour l'élaboration d'un arbre des défaillances. Cette démarche est facilitée par l'application préalable d'une méthode de type APR, Hazop ou AMDEC

Enfin, il est nécessaire de respecter certaines règles supplémentaires à observer durant la construction de l'arbre à savoir (4) :

- vérifier que le système est cohérent, c'est-à-dire que :
  - la défaillance de tous ses composants entraîne la défaillance du système,
  - le bon fonctionnement de tous ses composants entraîne le bon fonctionnement du système,
  - lorsque le système est en panne, le fait de considérer une nouvelle défaillance ne rétablit pas le fonctionnement du système,
  - lorsque le système fonctionne correctement, la suppression d'une défaillance ne provoque pas la défaillance du système.
    Il peut en effet arriver qu'une défaillance survenant sur un composant annule les effets d'une défaillance antérieure et permette ainsi le fonctionnement du système. Dans un tel cas de figure (système non cohérent), le deuxième composant doit être supposé, dans l'analyse, en fonctionnement lorsque la première défaillance survient.
- s'assurer que tous les évènements d'entrée d'une porte logique ont bien été identifiés avant d'analyser leurs causes respectives,
- éviter de connecter directement deux portes logiques,
- ne sélectionner que les causes antérieures à l'existence de l'événement considéré.

En définitive, l'application de ces règles aux réflexions menées au sein d'un groupe de travail conduit à la construction d'un arbre de la forme suivante.

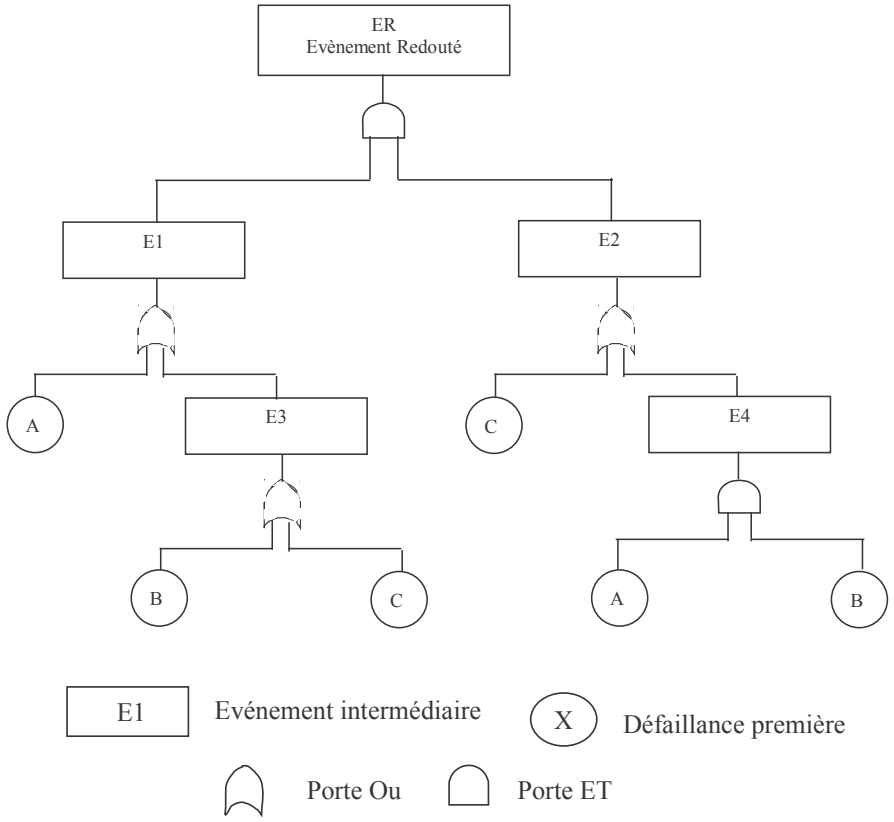


Figure 5 : Exemple d'arbre des défaillances (VILLEMEUR, 1988)

4.5.5 EXPLOITATION DE L'ARBRE DES DEFAILLANCES

L'analyse par arbre des défaillances permet d'estimer la probabilité d'occurrence d'un événement et de s'assurer que toutes les mesures possibles ont effectivement été envisagées en vue de prévenir le risque associé à cet événement. A la différence des méthodes inductives présentées précédemment, l'arbre des défaillances est directement conçu afin de pouvoir considérer des combinaisons de défaillances et de vérifier que toutes les causes potentielles ont bien été prises en compte.

Cette exploitation de l'arbre des défaillances peut être réalisée de manière qualitative et quantitative. Elle nécessite au préalable de traiter les résultats fournis au cours de la construction de l'arbre. Dans l'exemple précédent (Figure 5), les évènements A, B et C apparaissent plusieurs fois dans l'arbre : il n'y a donc pas indépendance des évènements de base. **Ainsi, il est indispensable d'éliminer ces fausses redondances préalablement à l'exploitation de cet arbre**.

L'élimination des fausses redondances fait appel aux notions de coupes minimales et de réduction d'arbres.

4.5.5.1 COUPES MINIMALES – REDUCTION D'ARBRE

Une coupe minimale représente la plus petite combinaison d'évènements pouvant conduire à l'événement indésirable ou redouté. On parle parfois également de « chemin critique ».

Dans l'exemple précédent, l'occurrence simultanée des évènements A, B et C conduit effectivement à l'événement final. Il ne s'agit cependant pas d'une coupe minimale puisque la combinaison A.B seule peut être à l'origine de l'événement final.

La recherche des coupes minimales est effectuée à partir des règles de l'algèbre de BOOLE en considérant que :

- à chaque événement de base correspond une variable booléenne,
- l'événement de sortie d'une porte « ET » est associé au produit des variables booléennes correspondant aux évènements d'entrée,
- l'événement de sortie d'une porte « OU » est associé à la somme des variables booléennes correspondant aux évènements d'entrée,

Quelques-unes des principales règles de l'algèbre de BOOLE sont résumées dans le tableau suivant :

Propriétés	***Produi (ET)t***	***Somme (OU)***
Commutativité	A.B = B.A	A + B = B + A
Idempotence	A . A =A	A + A = A
Absorption	A . (A+B) = A	A + A.B = A
Associativité	A . (B . C) = (A . B) . C	A + (B + C) = (A + B) + C
Distributivité	A . (B + C) = A.B + A.C	A + B.C = (A+B) . (A+C)

Tableau 12: principales règles de l'algèbre de BOOLE

Ainsi, dans l'exemple précédent, la recherche des coupes minimales peut s'effectuer comme suit :

ER = E1 . E2

E1 = A +E3 avec E3 = B + C

E2 = C + E4 avec E4 = A . B

Au total, nous avons donc :
ER = (A+B+C) . (C+A.B) = A.C + A.B + B.C + A.B + C +C.A.B

Or, A.C + C =C et A.B+ A.B.C = A.B (par absorption)

ER = C + A.B + B.C + A.B

De plus, A.B + A.B = AB (Idempotence) et C + B.C = C (Absorption)

D'où ER = C + A.B

Ainsi, l'événement C seul ou la combinaison des évènements A.B conduisent à l'événement redouté. Il n'existe pas de combinaison plus petite conduisant à cet événement. L'arbre présenté en exemple admet donc deux coupes minimales : C ainsi que A.B.

L'ordre d'une coupe est alors défini comme le nombre d'évènements combinés qui figurent dans cette coupe.

Finalement, cet arbre comporte :

- une coupe minimale d'ordre 1 : C,
- une coupe minimale d'ordre 2 : A.B.

L'arbre représentant ces coupes minimales est appelé « arbre réduit ». Pour l'exemple considéré dans la Figure 5, l'arbre réduit est le suivant.

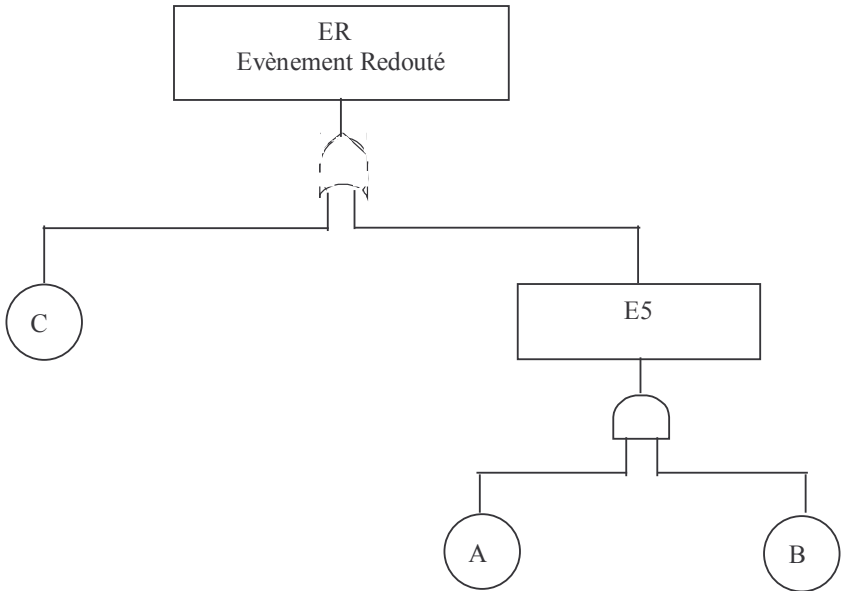


Figure 6 : Réduction de l'arbre des défaillances pris en exemple (VILLEMEUR, 1988)

La recherche des coupes minimales peut s'avérer fastidieuse pour des arbres de taille importante. Certains outils informatiques permettent heureusement d'automatiser cette démarche. Ces outils démontrent toute leur utilité pour la réduction d'arbres complexes. Leur utilisation ne doit cependant pas faire oublier que la définition précise de l'événement final constitue la première étape en vue de limiter la complexité de l'arbre des défaillances.

4.5.5.2 EXPLOITATION QUALITATIVE DE L'ARBRE DES DEFAILLANCES

L'exploitation qualitative de l'arbre vise à examiner dans quelle proportion une défaillance correspondant à un événement de base peut se propager dans l'enchaînement des causes jusqu'à l'évènement final. Pour cela, tous les évènements de base sont supposés équiprobables et on étudie le cheminement à travers les portes logiques d'événement ou de combinaisons d'évènements jusqu'à l'événement final.

De manière intuitive, une défaillance se propageant à travers le système en ne rencontrant que des portes « OU » est susceptible de conduire très rapidement à l'événement final. A l'inverse, un cheminement s'opérant exclusivement à travers des portes « ET » indique que l'occurrence de l'évènement final à partir de l'événement ou la combinaison d'évènements de base est moins probable et démontre ainsi une meilleure prévention de l'événement final.

La définition des coupes minimales permet d'accéder directement aux évènements et combinaisons d'évènements les plus critiques pour le système considéré. Ainsi, plus l'ordre d'une coupe minimale est petit, plus l'occurrence de l'événement final suivant ce chemin critique peut paraître probable. Un moyen de prévenir les évènements indésirables ou redoutés vise à modifier l'arbre des défaillances en vue d'obtenir des coupes minimales d'ordre le plus élevé possible, par l'introduction de portes « ET » par exemple.

Cette approche qualitative repose néanmoins sur l'hypothèse relativement forte que les évènements de base sont équiprobables. Il peut cependant arriver qu'une coupe minimale d'ordre 1 corresponde à un événement extrêmement peu probable alors qu'une coupe minimale d'ordre supérieur peut correspondre à des combinaisons d'évènements très probables.

4.5.5.3 EXPLOITATION QUANTITATIVE DE L'ARBRE DES DEFAILLANCES

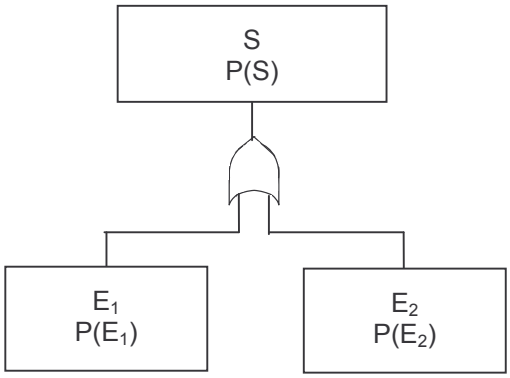
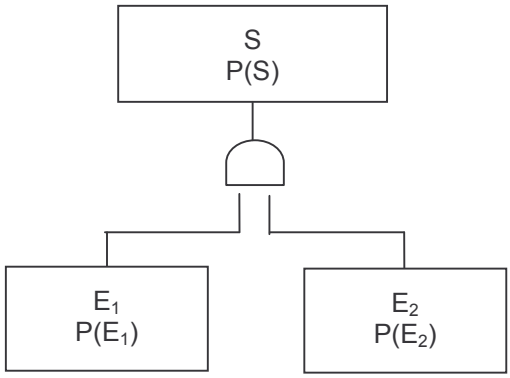
L'exploitation quantitative de l'arbre des défaillances vise à estimer, à partir des probabilités d'occurrence des évènements de base, la probabilité d'occurrence de l'événement final ainsi que des évènements intermédiaires. Il ne s'agit pas d'une démarche qui permet d'accéder avec exactitude à la probabilité de chaque évènement. Elle doit être mise en œuvre dans l'optique de hiérarchiser les différentes causes possibles et de concentrer les efforts en matière de prévention sur les causes les plus vraisemblables.

En pratique, il est souvent difficile d'obtenir des valeurs précises de probabilités des évènements de base. En vue de les estimer, il est possible de faire appel à :

- des bases de données,
- des jugements d'experts,
- des essais lorsque cela est possible,
- au retour d'expérience sur l'installation ou des installations analogues.

A partir des probabilités des évènements de base, il s'agit de remonter dans l'arbre des défaillances en appliquant les règles suivantes.[18]

[18] Cette hypothèse considère le système comme irréparable, c'est-à-dire que les défaillances subsistent une fois survenues.

Porte « OU »	Porte « ET »
	
P(S) = P(E1) + P(E2) – P(E1).P(E2) (Théorème de POINCARRE) Lorsque la probabilité des évènements de base est faible, il est possible de négliger le produit P(E1).P(E2) et de considérer : P(S) ≈ P(E1) + P(E2)	P(S) = P(E1).P(E2)

A titre d'exemple, appliquons cette démarche à l'arbre réduit présenté en Figure 6, en supposant les probabilités des évènements de base connues :

- $P(A) = 10^{-3}$,
- $P(B) = 10^{-2}$,
- $P(C) = 10^{-6}$.

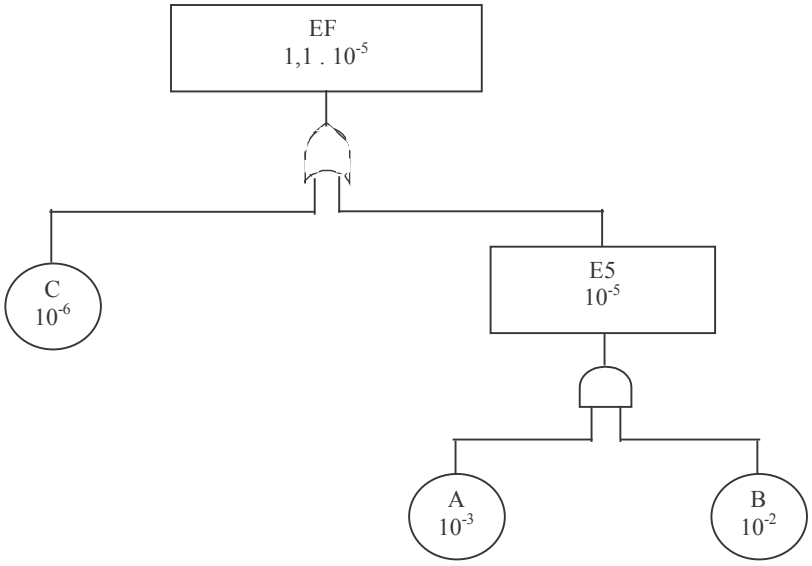


Figure 7 : Détermination de la probabilité de l'événement final

Cette exploitation quantitative de l'arbre, au même titre que son exploitation qualitative, ne peut être effectuée qu'à partir d'un arbre réduit.

Par ailleurs, notons, que pour des éléments de base de faible probabilité, la probabilité de l'événement final est sensiblement égale à la somme des probabilités affectées aux coupes minimales.

Dans l'exemple précédent, nous avons donc :

P(EF) = P(C + A.B) = P(C) + P(A).P(B) - P(A).P(B).P(C) (théorème de POINCARRE)
d'où **P(EF) ≈ P(C) + P(A).P(B)**

Les logiciels informatiques développés depuis une quinzaine d'années permettent de déterminer automatiquement les probabilités tout au long de l'arbre.

L'examen des probabilités des évènements intermédiaires conduisant à l'événement final permet de hiérarchiser les priorités de modifications du système en identifiant les causes les plus probables d'un événement indésirable ou final.

La réduction de la probabilité de cet événement final peut alors être envisagée de plusieurs manières :

- en supprimant ou réduisant la probabilité d'occurrence des évènements de base,
- en améliorant la fiabilité du système par l'ajout de portes « ET » entre l'événement final et les évènements de base. Les portes « ET » placées au plus proche de l'événement final permettent de traiter un maximum de coupes minimales et, le cas échéant, de traiter certaines causes qui n'auraient pas été envisagées.

Cette dernière stratégie correspond en pratique à l'ajout de barrières de sécurité. L'événement final ne peut alors se produire que si l'événement de base se produit et si la barrière de sécurité destinée à le compenser est elle-même défaillante.

4.5.6 LIMITES ET AVANTAGES

Le principal avantage de l'analyse par arbre des défaillances est qu'elle permet de considérer des combinaisons d'évènements pouvant conduire in fine à un événement redouté. Cette possibilité permet une bonne adéquation avec l'analyse d'accidents passés qui montre que les accidents majeurs observés résultent le plus souvent de la conjonction de plusieurs évènements qui seuls n'auraient pu entraîner de tels sinistres.

Par ailleurs, en visant à l'estimation des probabilités d'occurrence des évènements conduisant à l'événement final, elle permet de disposer de critères pour déterminer les priorités pour la prévention d'accidents potentiels.

L'analyse par arbre des défaillances porte sur un événement particulier et son application à tout un système peut s'avérer fastidieuse. En ce sens, il est conseillé de mettre en œuvre au préalable des méthodes inductives d'analyse des risques. Ces outils permettent d'une part d'identifier les évènements les plus graves qui pourront faire l'objet d'une analyse par arbre des défaillances et, d'autre part, de faciliter la détermination des causes immédiates, nécessaires et suffisantes au niveau de l'élaboration de l'arbre.

Depuis une quinzaine d'années, des logiciels informatiques sont commercialisés afin de rendre plus aisée l'application de l'arbre des défaillances. Ces outils se montrent très utiles pour la recherche des coupes minimales, la détermination des probabilités ainsi que pour la présentation graphique des résultats sous forme arborescente.

4.6 ARBRE DES EVENEMENTS

4.6.1 HISTORIQUE ET DOMAINE D'APPLICATION

L'analyse par arbre d'évènements a été développée au début des années 1970 pour l'estimation du risque lié aux centrales nucléaires à eau légère. Particulièrement utilisée dans le domaine du nucléaire, son utilisation s'est étendue à d'autres secteurs d'activité.

De par sa complexité proche de celle de l'analyse par arbre des défaillances, cette méthode s'applique sur des sous-systèmes bien déterminés. Elle apporte une aide précieuse pour traiter des systèmes comportant de nombreux dispositifs de sécurité et de leurs interactions. A l'instar de l'analyse par arbre des défaillances dont elle s'inspire, elle permet d'estimer les probabilités d'occurrence de séquences accidentelles à condition de disposer de la probabilité d'occurrence de l'événement initial et de la probabilité de défaillance des barrières de sécurité.

Cette méthode est aussi utilisée dans le domaine de l'analyse après accidents en vue d'expliquer les conséquences observées résultant d'une défaillance du système.

4.6.2 PRINCIPE

L'analyse par arbre des défaillances, comme nous l'avons vu précédemment, vise à déterminer, dans une démarche déductive, les causes d'un événement indésirable ou redouté retenu a priori. A l'inverse, l'analyse par arbre d'évènements suppose la défaillance d'un composant ou d'une partie du système et s'attache à déterminer les évènements qui en découlent.

A partir d'un événement initiateur ou d'une défaillance d'origine, l'analyse par arbre d'évènements permet donc d'estimer la dérive du système en envisageant **de manière systématique** le fonctionnement ou la défaillance des dispositifs de détection, d'alarme, de prévention, de protection ou d'intervention…

Ces dispositifs peuvent concerner aussi bien des moyens automatiques qu'humains.

4.6.3 DEROULEMENT

La démarche généralement retenue pour réaliser une analyse par arbre d'évènements est la suivante :

- définir l'événement initiateur à considérer,
- identifier les fonctions de sécurité prévues pour y faire face,
- construire l'arbre,
- décrire et exploiter les séquences d'évènements identifiées.

Les paragraphes suivants décrivent ces différentes étapes en suivant un exemple inspiré de l'ouvrage « Guidelines for Hazard Evaluation Procedures », cité en références.

4.6.3.1 DEFINITION DE L'EVENEMENT INITIATEUR

Il s'agit d'une étape importante pour l'analyse par arbre d'évènements. Etant donné qu'il s'agit d'une approche qui peut vite se révéler lourde à mener, il est généralement bon de sélectionner un événement initiateur qui peut effectivement conduire à une situation critique. Ceci suppose donc de connaître, au moins de manière partielle, les principaux risques associés à l'installation considérée. Pour une analyse après accidents, ces risques sont de fait connus. Ce cas mis à part, il est pertinent d'élaborer un arbre d'évènements suite à une première analyse qui a mis en lumière les accidents potentiels à envisager. En ce sens, cette méthode apparaît complémentaire de méthodes telles que l'APR par exemple.

L'exemple traité dans les paragraphes suivants considère un réacteur dans lequelle s'opère une réaction exothermique[19]. Le maintien en température du système est assuré par un système de réfrigération (AICHE).

Pour ce cas simple, il est aisé d'identifier le risque d'emballement de réaction. Cet emballement pourrait notamment résulter de la défaillance du système de refroidissement.

Cet événement sera considéré comme événement initiateur pour la construction d'un arbre d'évènements.

[19] Produisant de la chaleur

4.6.3.2 IDENTIFICATION DES FONCTIONS DE SECURITE

Les fonctions de sécurité doivent être assurées par des barrières en réponse à l'événement initiateur. Elles ont en général pour objectif d'empêcher que l'événement initiateur soit à l'origine d'un accident majeur.

Elles se déclinent le plus souvent en :

- fonctions de détection de l'événement initiateur,
- fonctions d'alarme signifiant l'occurrence de l'événement initiateur,
- fonctions de limitation visant à empêcher que l'événement initiateur ne perdure dans le temps,
- fonction d'atténuation s'attachant à réduire les effets de l'événement initiateur.

Cette liste n'est, bien sûr, pas exhaustive. De plus, ces fonctions peuvent être réalisées par des dispositifs automatiques ou bien des actions effectuées par des opérateurs conformément à des procédures.

Dans l'exemple du réacteur chimique, en réponse à la défaillance du système de refroidissement, les fonctions de sécurité suivantes ont été prévues :

- détecter la montée en température dans le réacteur,
- alarmer un opérateur de la montée en température,
- rétablir le fonctionnement du système de refroidissement,
- stopper la réaction.

Bien entendu, ces fonctions n'interviennent généralement pas simultanément. Il est particulièrement important de déterminer dans quel ordre elles vont intervenir suite à l'événement initiateur et donc d'identifier les seuils commandant leur mise en œuvre.

Ces informations permettent ainsi de donner des indications quant au temps nécessaire pour la mise en place de ces mesures de sécurité.

En conclusion de cette seconde étape, il est judicieux de dresser un tableau chronologique des fonctions de sécurité faisant figurer entre autres les systèmes ou équipements prévus pour assurer ces fonctions.

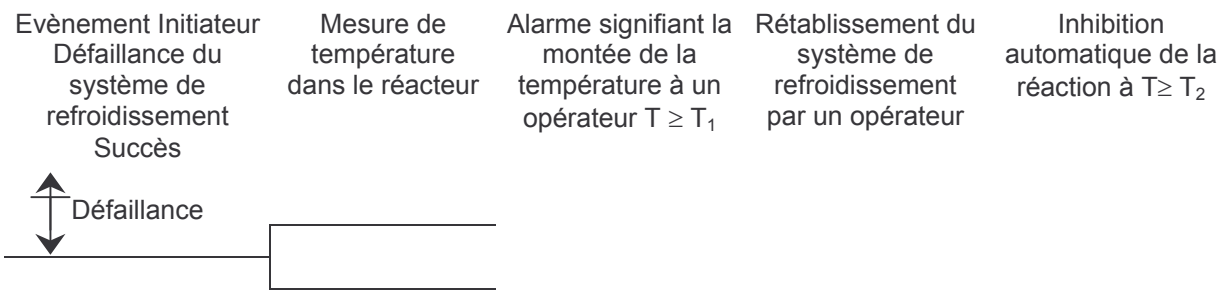
Fonctions	Mesure de la température dans le réacteur	Alarme	Rétablissement du système de réfrigération par un opérateur	Arrêt de la réaction
Dispositifs assurant la fonction	Sonde de température dans le réacteur	Signaux sonores et lumineux aux postes de travail	Opérateur selon une procédure	Introduction automatique d'un inhibiteur de la réaction
Paramètre ou Information déclenchant la fonction	Permanent	$T \geq T_1$	Alarme	$T \geq T_2$
Délai	Continu	1 mn	Si possible, estimé à 5 mn	Estimé à 10 mn (De T_1 à T_2)

Tableau 13 : Exemple de tableau définissant les fonctions de sécurité

Nota : Dans cet exemple, il sera supposé que la même sonde fournit les informations de température pour l'alarme et le déclenchement automatique de l'inhibition de la réaction.

4.6.3.3 CONSTRUCTION DE L'ARBRE

La construction de l'arbre consiste alors, à partir de l'événement indésirable, à envisager soit le bon fonctionnement soit la défaillance de la première fonction de sécurité. L'événement initiateur est représenté schématiquement par un trait horizontal. Le moment où doit survenir la première fonction de sécurité est représenté par un nœud. La branche supérieure correspond généralement au succès de la fonction de sécurité, la branche inférieure à la défaillance de cette fonction.



La suite de la méthode consiste alors à examiner le développement de chaque branche de manière itérative en considérant systématiquement le fonctionnement ou la défaillance de la fonction de sécurité suivante.

- Cette démarche temporelle permet d'identifier des séquences d'évènements susceptibles de conduire ou non à un accident potentiel. Elle n'est cependant généralement pas suffisante en vue de construire un arbre. Il est ainsi indispensable durant la construction de l'arbre d'observer les points suivants :
  - Si le succès d'une fonction dépend du succès d'autres fonctions, elle doit être considérée après les fonctions dont elle dépend.
  - Dans le même ordre d'idée, si l'échec d'une fonction implique automatiquement l'échec d'autres fonctions, le succès de ces dernières n'est pas à considérer. Ainsi, dans notre exemple, si la sonde de température est défaillante, il n'y a pas lieu d'étudier le fonctionnement de l'alarme ou le déclenchement automatique de l'inhibition de la réaction.
  - Si le succès d'une fonction agit sur le paramètre déclenchant d'autres fonctions ultérieures, le succès ou la défaillance de cette fonction ne doivent pas être envisagés dans le développement de cette branche. Ainsi, si l'opérateur parvient à rétablir le système de refroidissement avant que la température dans le réacteur ne dépasse T2, il n'y a pas lieu de considérer l'inhibition automatique de la réaction.
  - Si la défaillance d'un sous-système entraîne la défaillance commune de plusieurs systèmes assurant des fonctions de sécurité, ce sous-système doit être considéré avant ces systèmes. Ce cas de figure envisage ainsi les modes communs de défaillances. Elles se rapportent souvent à des pertes d'utilités (électricité, air comprimé…) ou des agressions externes majeures. Dans notre exemple, si l'alimentation électrique est commune à tous les systèmes considérés, il convient de considérer juste après l'événement initiateur une fonction du type « Maintien de l'alimentation électrique ». Nous considérerons ici que tous ces systèmes ont une alimentation distincte. De la même façon, la défaillance de la sonde de température dans le réacteur est supposée entraîner la défaillance commune du système d'alarme et d'inhibition de réaction. Elle a donc été considérée en premier lieu.

Le respect de ces règles et l'élimination des branches physiquement impossibles conduisent à l'élaboration d'un arbre d'évènements réduit, semblable à celui présenté ci-dessous relativement au cas de figure pris en exemple.

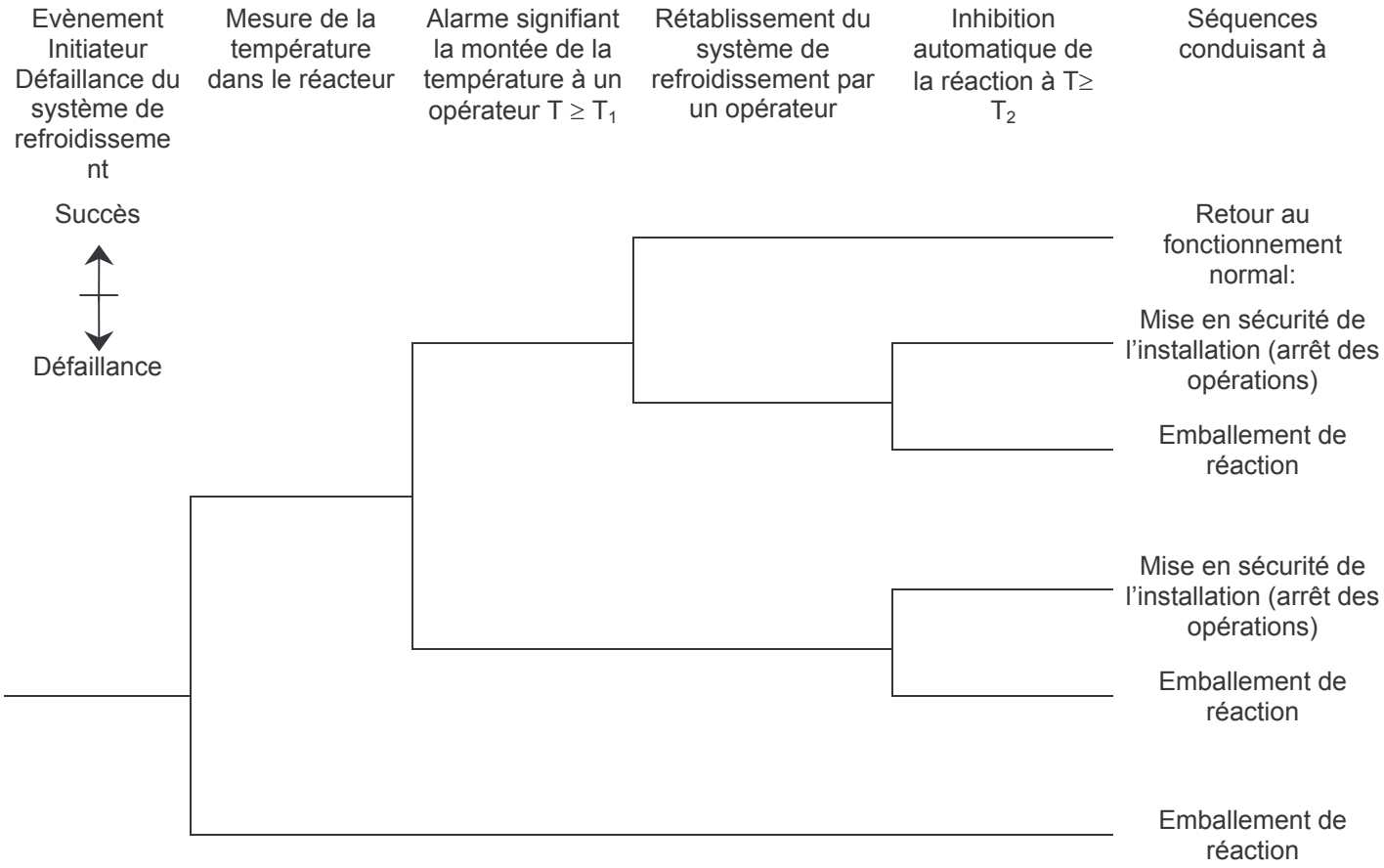


Figure 8 : Exemple d'arbre d'évènements réduit

4.6.3.4 EXPLOITATION DE L'ARBRE

La réalisation d'un arbre d'évènements permet en définitive de déterminer la probabilité d'occurrence des différentes conséquences à partir des séquences identifiées.

Cette dernière ne peut être effectuée qu'à partir d'un arbre d'évènements préalablement réduit. La réduction de l'arbre concourt entre autres à éliminer les chemins non physiquement possibles ainsi qu'à identifier les modes communs de défaillances. Cette opération est nécessaire pour assurer l'indépendance des évènements intermédiaires présentés.

La probabilité d'occurrence d'une conséquence suite à une séquence particulière peut alors être estimée, pour des évènements indépendants, comme le produit de la probabilité d'occurrence de l'événement initiateur et de la probabilité de défaillance ou de fonctionnement selon le cheminement des évènements intermédiaires.

La Figure 9 permet d'expliciter cette détermination des probabilités pour un arbre d'évènements réduit. Rappelons qu'un arbre des évènements ne doit pas être considéré comme un outil visant à déterminer la probabilité d'un événement avec exactitude mais comme un outil pour caractériser l'enchaînement des actions et des évènements pouvant conduire ou non à un accident.

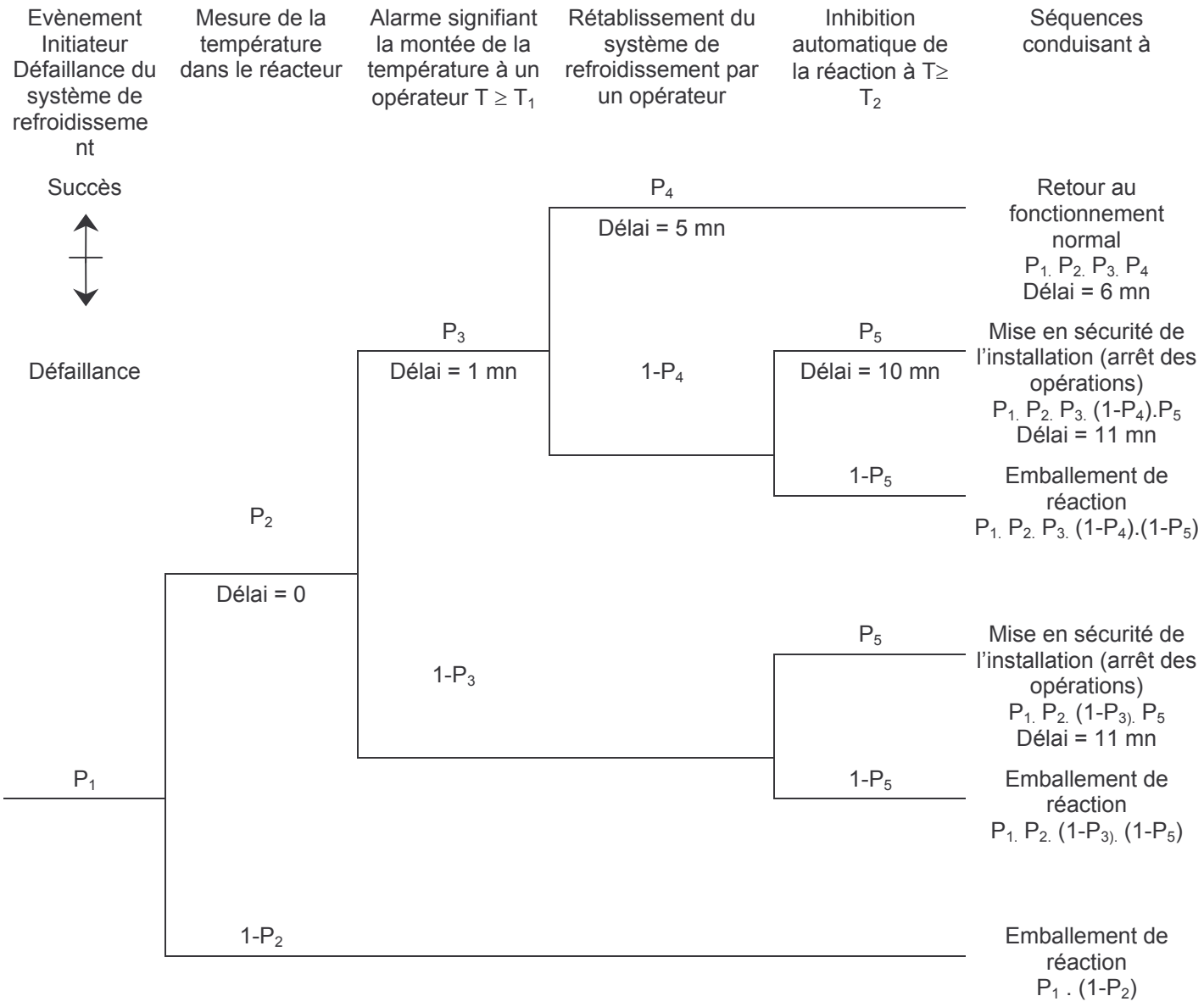


Figure 9 : Exemple d'exploitation d'un arbre d'évènements

4.6.4 LIMITES ET AVANTAGES

L'analyse par arbre d'évènements est une méthode qui permet d'examiner, à partir d'un événement initiateur, l'enchaînement des évènements pouvant conduire ou non à un accident potentiel. Elle trouve ainsi une utilité toute particulière pour l'étude de l'architecture des moyens de sécurité (prévention, protection, intervention) existants ou pouvant être envisagés sur un site. A ce titre, elle peut être utilisée pour l'analyse d'accidents a posteriori.

Cette méthode peut s'avérer lourde à mettre en œuvre. En conséquence, il faut définir avec discernement l'événement initiateur qui fera l'objet de cette analyse.

4.7 NŒUD PAPILLON

4.7.1 HISTORIQUE ET DOMAINE D'APPLICATION

Le « Nœud Papillon » est une approche de type arborescente largement utilisée dans les pays européens comme les Pays-Bas qui possèdent une approche probabiliste de la gestion des risques. Le Nœud Papillon est utilisé dans différents secteurs industriels par des entreprises comme SHELL qui a été à l'origine du développement de ce type d'outils.

Dans ce document, l'INERIS présente une version particulière du Nœud Papillon qu'il a été amené à adapter.

4.7.2 PRINCIPE

Le nœud papillon est un outil qui combine un arbre de défaillances et un arbre d'événements représentés de façon un peu différente de celle décrite dans les paragraphes précédents. La Figure 10 en donne une représentation schématique sous la forme suivante où les barrières sont figurées par des barres verticales.

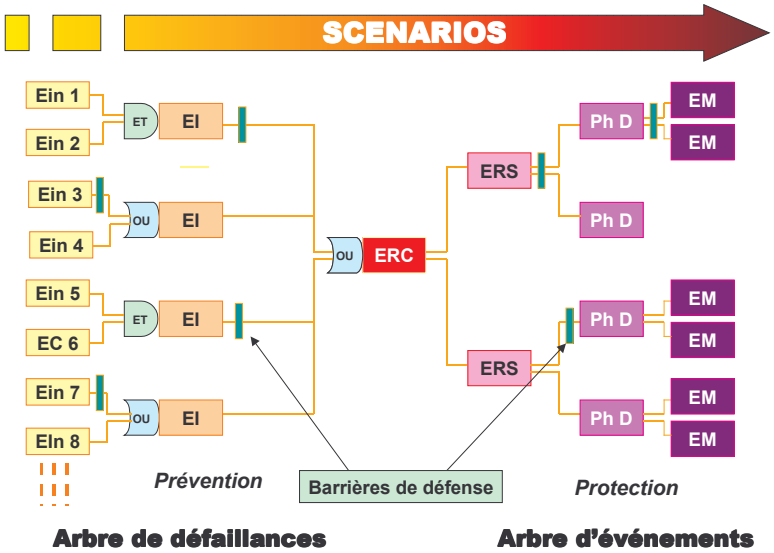


Figure 10 : Représentation de scénarios d'accident selon le modèle du nœud papillon

Désignation	Signification	Définition	Exemples
EIn	*Evènement Indésirable*	*Dérive ou défaillance sortant du cadre des conditions d'exploitation usuelles définies.*	*Le surremplissage ou un départ d'incendie à proximité d'un équipement dangereux peuvent être des évènements initiateurs*
EC	*Evènement Courant*	*Evènement admis survenant de façon récurrente dans la vie d'une installation.*	*Les actions de test, de maintenance ou la fatigue d'équipements sont généralement des évènements courants.*
EI	*Evènement Initiateur*	*Cause directe d'une perte de confinement ou d'intégrité physique.*	*La corrosion, l'érosion, les agressions mécaniques, une montée en pression sont généralement des évènements initiateurs*
ERC	*Evènement Redouté Central*	***Perte de confinement sur un équipement dangereux ou perte d'intégrité physique d'une substance dangereuse***	***Rupture, Brèche, Ruine ou Décomposition d'une substance dangereuse dans le cas d'une perte d'intégrité physique***
ERS	*Evènement Redouté Secondaire*	*Conséquence directe de l'événement redouté central, l'événement redouté secondaire caractérise le terme source de l'accident*	*Formation d'une flaque ou d'un nuage lors d'un rejet d'une substance diphasique*
Ph D	*Phénomène Dangereux*	*Phénomène physique pouvant engendrer des dommages majeurs*	*Incendie, Explosion, Dispersion d'un nuage toxique*
EM	*Effets Majeurs*	*Dommages occasionnés au niveau des éléments vulnérables (personnes, environnement ou biens) par les effets d'un phénomène dangereux*	*Effets létaux ou irréversibles sur la population* *Synergies d'accident*
Barrières ou Mesures de Prévention		*Barrières ou mesures visant à prévenir la perte de confinement ou d'intégrité physique*	*Peinture anti-corrosion, Coupure automatique des opérations de dépotage sur détection d'un niveau très haut…*
Barrières ou Mesures de Protection		*Barrières ou mesures visant à limite les conséquences de la perte de confinement ou d'intégrité physique*	*Vannes de sectionnement automatiques asservies à une détection (gaz, pression, débit), Moyens d'intervention…*

Tableau 14 : Légende des évènements figurant sur le modèle du nœud papillon

Le point central du Nœud Papillon, appelé ici Evènement Redouté Central, désigne généralement une perte de confinement ou une perte d'intégrité physique (décomposition). La partie gauche du Nœud Papillon s'apparente alors à un arbre des défaillances s'attachant à identifier les causes de cette perte de confinement. La partie droite du Nœud Papillon s'attache quant à elle à déterminer les conséquences de cet événement redouté central tout comme le ferait un arbre d'évènements.

Sur ce schéma, les barrières de sécurité sont représentées sous la forme de barres verticales pour symboliser le fait qu'elles s'opposent au développement d'un scénario d'accident. En pratique, ajouter une barrière dans l'arbre correspond à ajouter un événement « défaillance de la barrière » lié par une porte ET à l'événement qui la précède.

De fait, dans cette représentation, chaque chemin conduisant d'une défaillance d'origine (***évènements indésirable ou courant***) jusqu'à l'apparition de dommages au niveau des ***éléments vulnérables (effets majeurs***) désigne un scénario d'accident particulier pour un même événement redouté central.

Cet outil permet d'apporter une démonstration renforcée de la bonne maîtrise des risques en présentant clairement l'action de barrières de sécurité sur le déroulement d'un accident.

4.7.3 DEROULEMENT

Le Nœud Papillon, s'inspirant directement des arbres des défaillances et d'évènements, doit être élaboré avec les mêmes précautions.

S'agissant d'un outil relativement lourd à mettre en place, son utilisation est généralement réservée à des évènements jugés particulièrement critiques pour lesquels un niveau élevé de démonstration de la maîtrise des risques est indispensable.

En règle générale, un Nœud Papillon est construit à la suite d'une première analyse des risques menée à l'aide de méthodes plus simples comme l'APR ou l'HAZOP par exemple.

4.7.4 LIMITES ET AVANTAGES

Le Nœud Papillon offre une visualisation concrète des scénarios d'accidents qui pourraient survenir en partant des causes initiales de l'accident jusqu'aux conséquences au niveau des éléments vulnérables identifiés.

De ce fait, cet outil met clairement en valeur l'action des barrières de sécurité s'opposant à ces scénarios d'accidents et permet d'apporter une démonstration renforcée de la maîtrise des risques.

En revanche, il s'agit d'un outil dont la mise en œuvre peut être particulièrement coûteuse en temps. Son utilisation doit donc être décidée pour des cas justifiant effectivement un tel niveau de détail.

5 METHODES INTEGREES D'ANALYSE DES RISQUES

Le chapitre précédent était consacré à la présentation des méthodes de base de l'analyse de risque. Celles-ci doivent être mises en œuvre dans le cadre d'une démarche globale dont la version minimale est décrite au chapitre 3. De nouvelles méthodes ont vu le jour ou ont été plus largement utilisées au cours des dernières années. Il s'agit de méthodes intégrées, qui visent à répondre à travers une même démarche à plusieurs questions que se posent les acteurs de l'évaluation des risques et à apporter des outils pour faciliter l'analyse et l'estimation des risques. Ces méthodes intègrent donc différentes étapes d'identification des risques, d'évaluation des barrières ou d'évaluation de la vulnérabilité de l'environnement, par exemple.

5.1 ARAMIS

5.1.1 PRESENTATION, OBJECTIFS DU PROJET

ARAMIS est un projet européen de recherche réalisé dans le cadre du 5eme PCRD entre janvier 2002 et décembre 2004. ARAMIS signifie A Risk Assessment Methodology for IndustrieS. L'objectif du projet était de développer une nouvelle méthodologie d'évaluation des risques répondant aux exigences de la directive Seveso II et constituant une solution alternative aux approches purement déterministes ou purement probabilistes de l'évaluation des risques alors en vigueur en Europe.

A l'origine du projet il y avait le constat, renforcé par l'accident de Toulouse en décembre 2001, que les méthodes d'évaluation des risques disponibles n'étaient plus adaptées aux exigences de la directive et aux attentes qui émergeaient au niveau des décideurs publics et des populations.

Les pays ayant une approche purement déterministe se trouvaient confrontés à la difficulté de prendre des décisions publiques sur la base d'évaluations faisant ressortir systématiquement les scénarios majorants. Les résultats d'une estimation déterministe étaient facilement communicables au public mais donnaient une vision erronée du risque. Les méthodes d'évaluation associées n'étaient pas non plus un bon support pour la démonstration de la maîtrise du risque par l'industriel [Kirchsteiger 1999].

Pour les pays ayant une approche probabiliste le problème se posait autrement. Le résultat de l'estimation, libellé en terme de risque sociétal était peu communicable car peu compréhensible par la population. Par ailleurs, il s'appuyait généralement sur des données statistiques. Il ne reflétait donc pas la réalité locale ni les efforts de maîtrise du risque entrepris par l'exploitant.

Le projet ASSURANCE [Hourtolou 2002] avait par ailleurs montré que les méthodes d'évaluation des risques pratiquées par des experts de différents pays européens pouvaient donner des résultats très dispersés. Ce projet avait fait ressortir les sources d'incertitudes qui étaient notamment liées au choix des scénarios à prendre en compte à l'issue de l'évaluation et pour lesquels s'opposaient finalement les approches des pays ayant une vision probabiliste où les scénarios les plus probables étaient considérés comme les plus représentatifs et ceux ayant une approche déterministe qui considéraient les scénarios les plus graves.

Le projet ARAMIS avait donc pour objectif d'aboutir à une méthode qui permettrait d'estimer le risque en résolvant les difficultés exposées plus haut dans le contexte de la directive SEVESO II. Cette méthode devait fournir des résultats exploitables par les décideurs publics et les industriels, communicables à un public de non spécialistes. L'estimation du risque produite devait aussi tenir compte des mesures de réduction du risque mises en place par l'industriel et de l'influence du facteur humain et de l'organisation sur l'efficacité de ces mesures de réduction du risque.

5.1.2 PRINCIPAUX RESULTATS DU PROJET ARAMIS [ARAMIS 2005]

5.1.2.1 CONCEPTS DE BASE

Pour atteindre ces objectifs, la première étape a consisté à s'entendre sur les composantes du risque et sur les éléments à identifier et mesurer pour les estimer. Il faut rappeler qu'il n'existait pas à l'époque de définition du risque partagée par les pays de l'union européenne. La Figure 11 illustre la définition retenue. Le risque y est défini comme une combinaison de la probabilité de survenance d'un phénomène dangereux, de son intensité et de la vulnérabilité du territoire exposé. L'estimation de la probabilité implique d'identifier les événements initiateurs, causes des phénomènes dangereux, et d'en estimer la fréquence. Elle implique aussi d'identifier et de qualifier les barrières de sécurité qui s'opposent au déroulement du scénario accidentel depuis un événement initiateur jusqu'à un phénomène dangereux.

La performance de ces barrières dépend non seulement de leurs caractéristiques intrinsèques mais aussi de la qualité de l'organisation mise en place pour en assurer la conception, l'installation, l'utilisation, la maintenance et l'amélioration. La qualité de cette organisation est elle-même directement influencée par la culture de sécurité de l'entreprise.

L'évaluation de l'intensité des phénomènes dangereux dépend certes des modèles employés mais aussi beaucoup, voire principalement, des hypothèses retenues pour caractériser le terme source de ces phénomènes. Ainsi, est-il essentiel de préciser le mode de sélection des scénarios (c'est à dire l'ensemble des hypothèses de calcul) à modéliser pour estimer l'intensité de l'accident majeur redouté. Un nombre important de scénarios peuvent être sélectionnés par ce processus. Il faut donc aussi se doter d'un moyen de représenter le risque résultant de l'agrégation de ces scénarios d'accident. Un indice de sévérité, associant intensité et fréquence a été proposé à cet effet.

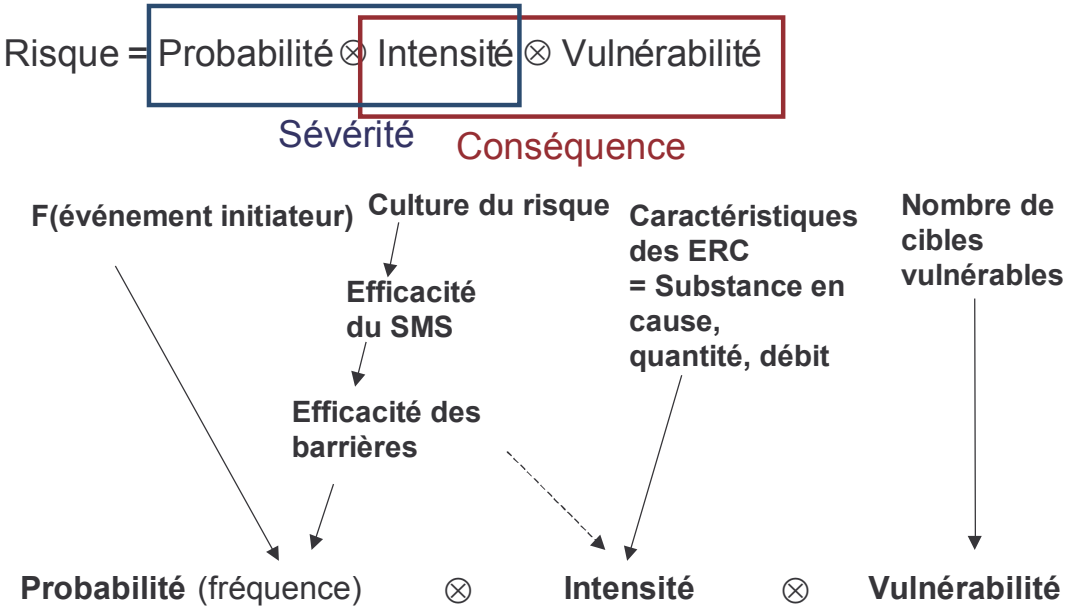


Figure 11 : les composantes du risque et les éléments à analyser (SMS= système de management de la sécurité, ERC= événement redouté central)

Enfin, la vulnérabilité du territoire est un sujet complexe qui peut être abordé suivant de nombreuses dimensions. En première approche, la vulnérabilité peut être considérée comme le facteur permettant d'estimer l'impact global d'un accident majeur.

5.1.2.2 DES OUTILS ET METHODES POUR L'EVALUATION DES RISQUES

A partir de ces définitions, le consortium d'ARAMIS a développé des méthodes et des outils pour :

- l'identification et la sélection des équipements dangereux en fonction des quantités de substances dangereuses qu'ils contiennent ;
- l'identification des événements redoutés centraux et la construction des scénarios accidentels. ARAMIS utilise pour cela les nœuds papillon (Figure 12), association d'un arbre de défaillance et d'un arbre d'événement. Pour faciliter cette analyse, des nœuds papillons génériques ont aussi été construits. Ils constituent un support de départ pour l'analyse d'une installation spécifique ;
- l'identification des fonctions et barrières de sécurité ;
- l'évaluation des performances des barrières de sécurité. Les outils proposés à cet effet par ARAMIS sont volontairement inspirés des normes CEI 61508 et CEI 61511 ;
- l'estimation de la probabilité du scénario à partir de la prise en compte des fréquences d'événements initiateurs et des niveaux de confiance des barrières, qualifiée d'approche barrière ;

- la qualification du système de management de la sécurité et son influence sur le niveau de confiance des barrières ;
- la qualification de la culture de sécurité ;
- la sélection des scénarios de référence : ceux qui doivent être modélisés pour établir l'indice de sévérité ;
- le calcul et la cartographie de l'indice de sévérité ;
- le calcul et la cartographie de la vulnérabilité.

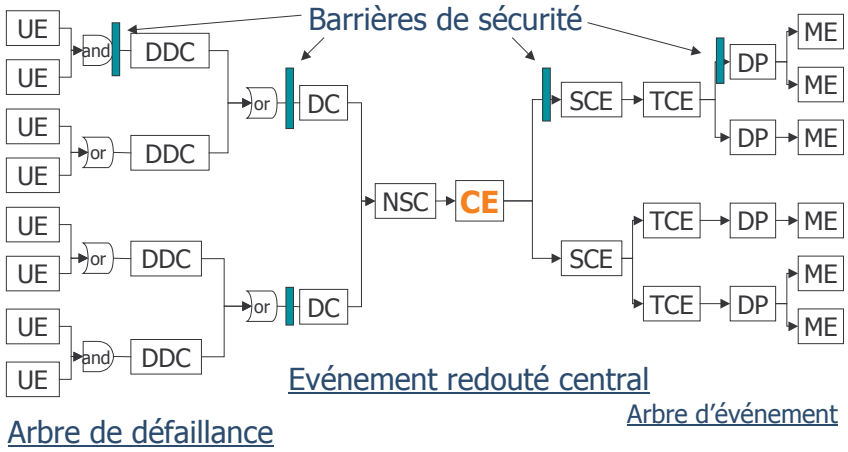


Figure 12 : La représentation des scénarios d'accident sous forme de nœud papillon est au cœur de la méthodologie ARAMIS

5.1.2.3 UNE APPROPRIATION PAR DIFFERENTS ACTEURS DE LA SECURITE INDUSTRIELLE

Les concepts, outils et méthodes d'ARAMIS ont été évalués dans le cadre d'études de cas qui ont permis de mettre en évidence leur pertinence et d'identifier les éléments d'amélioration possible. Depuis la fin du projet, chacun des partenaires a eu l'occasion de continuer à tester et améliorer ses résultats, contribuant ainsi à les diffuser dans son propre pays. ARAMIS a été identifié par de nombreuses autorités compétentes des pays de l'UE et a commencé à inspirer des évolutions réglementaires, prémices d'une convergence européenne en matière d'évaluation des risques. En France, les résultats d'ARAMIS ont en partie inspiré les autorités pour l'élaboration de la réglementation en vue de la mise en œuvre des PPRT et l'évolution des exigences en matière d'étude de dangers. L'évaluation séparée de l'aléa et de la vulnérabilité, la référence à l'approche barrière sont autant d'éléments qui font maintenant partie du cadre réglementaire français de l'évaluation des risques technologiques majeurs. La représentation des scénarios d'accident à l'aide du nœud papillon est maintenant largement adoptée pour répondre aux nouveaux objectifs de l'étude de dangers.

5.1.2.4 DEROULEMENT DE LA METHODE

La méthode ARAMIS est structurée en six étapes (Figure 13) :

1. Identification des scénarios potentiels d'accident majeur (MIMAH)

L'identification des scénarios d'accident repose sur l'utilisation d'une série d'arbres de défaillance et d'arbres d'événement génériques correspondant aux différents types d'équipements utilisés régulièrement dans l'industrie chimique.

L'identification des scénarios est précédée par une étape permettant de sélectionner les équipements, de l'installation étudiée, qui doivent faire l'objet d'une analyse. Cette sélection est réalisée en tenant compte de la nature et de la quantité des substances ainsi que des conditions dans lesquelles elles sont mises en œuvre.

Pour chaque couple formé d'un équipement et de la substance qu'il contient, la méthode permet de définir la liste des événements critiques (EC), perte de confinement ou perte d'intégrité physique, qu'il est susceptible de générer. A chaque EC ARAMIS associe un arbre de défaillance générique qui sera ensuite modifié pour correspondre aux spécificités de l'installation étudiée. De même, à partir d'un événement critique et de la substance dangereuse impliquée, la méthode permet de construire un arbre d'événement type, qui, combiné à l'arbre de défaillance forme un nœud papillon représentatif de plusieurs scénarios d'accident. Ces arbres génériques ne constituent naturellement qu'un guide pour l'analyste qui doit exercer son expertise pour conserver ou éliminer des événements, prolonger des branches lorsque c'est pertinent.

2. Identification des barrières de sécurité et évaluation de leurs performances

Une fois les scénarios d'accident potentiels identifiés, la méthode ARAMIS prévoit d'identifier les barrières de sécurité permettant de réduire la probabilité de l'accident ou d'en réduire la gravité potentielle. Des listes de barrières sont proposées pour aider l'utilisateur dans sa démarche.

En parallèle, un graphe de risque inspiré de la norme CEI 61508 permet de définir les exigences de sécurité associées à un scénario donné et de définir ainsi le niveau de confiance global que doivent avoir les barrières de sécurité pour que le scénario soit acceptable.

3. Evaluation de l'efficacité du management et de son influence sur les performances des barrières de sécurité

Deux questionnaires d'audit permettent de prendre en compte les performances du management de l'usine et la culture de sécurité sur le site. Les niveaux de confiance des barrières de sécurité sont affectés par le management et la culture de sécurité et sont donc recalculés à l'issue de cette évaluation.

4. Identification des Scénarios de Référence (MIRAS)

Une matrice de criticité est utilisée ensuite pour déterminer les scénarios de référence qui vont faire l'objet d'une modélisation des effets.

5. Estimation et cartographie de la sévérité des scénarios de référence

La sévérité des scénarios est alors évaluée. Plusieurs indices de sévérité ont été définis. Un premier indice permet de représenter les effets potentiels d'un scénario d'accident. Il repose sur une normalisation des effets dans une échelle unique. L'indice 100 correspondant au début des effets létaux et l'indice 0 à des effets nuls. L'évaluation des effets du scénario considéré conduit à calculer cinq distances d'effet correspondant à cinq seuils auxquels sont affectés les indices 100, 75, 50, 25 et 0. Entre ces distances seuils, l'indice de sévérité décroît de façon linéaire.

Un indice de sévérité global a aussi été défini. Il permet de représenter le cumul des sévérités de l'ensemble des scénarios d'accident sur le site pondéré par les probabilités associées à chaque scénario. A l'issue de ce calcul, il est donc possible de tracer une carte de sévérité autour du site.

6. Cartographie de la vulnérabilité

La carte de sévérité, une fois tracée, peut être mise en regard de la carte de vulnérabilité établie dans la dernière étape de la méthode. La vulnérabilité est estimée en faisant l'inventaire des éléments vulnérables potentiels (ou enjeux) autour du site industriel. Chaque type d'enjeu (humain, matériel, environnemental) est décomposé en différentes catégories dont la vulnérabilité relative à différents types d'effets a été évaluée sur la base d'un jugement d'expert. La vulnérabilité globale d'une zone est donc obtenue en effectuant une somme des différents types d'enjeux pondérée par leur vulnérabilité relative au type d'effet considéré.

La méthode ARAMIS a donc pour objectif de produire, in fine des résultats utiles à la décision en matière de maîtrise de l'urbanisation puisqu'elle permet de représenter de façon synthétique le risque sous forme d'une carte de sévérité couplée à une carte de vulnérabilité. Elle vise aussi à apporter des informations utiles relatives à la maîtrise du risque à la source, en identifiant les scénarios potentiels et les barrières qui permettent de les maîtriser. Enfin, elle constitue une approche innovante de la quantification de l'influence du management sur la sécurité du site.

Les études de cas réalisées au cours du projet ARAMIS ainsi que les applications qui ont été faites de la méthode depuis la fin du projet on montré son intérêt mais aussi certaines limites ou difficultés d'application. Une partie de ces limites est liée à l'absence de critères de décision permettant d'exploiter la représentation de la sévérité et de la vulnérabilité. Cette difficulté a été en partie levée en France par l'adoption des critères d'appréciation de la maîtrise des risques et des critères de définition des zones de maîtrise de l'urbanisation dans le cadre des PPRT, sur la base desquels l'indice de sévérité peut être réinterprété. De même, l'évaluation de la performance des barrières de sécurité faite dans ARAMIS correspondait à une première approche. Les connaissances en la matière ont bien évolué depuis la fin

du projet, notamment à l'INERIS où deux rapports Oméga ont été consacrés au sujet [Ayrault 2005], [Miché et Prats 2006].

Des informations complémentaires sur la méthode ARAMIS peuvent être obtenues sur le site du projet : http://aramis.jrc.it. Voir aussi [ARAMIS 2005] et [Hourtolou 2004]

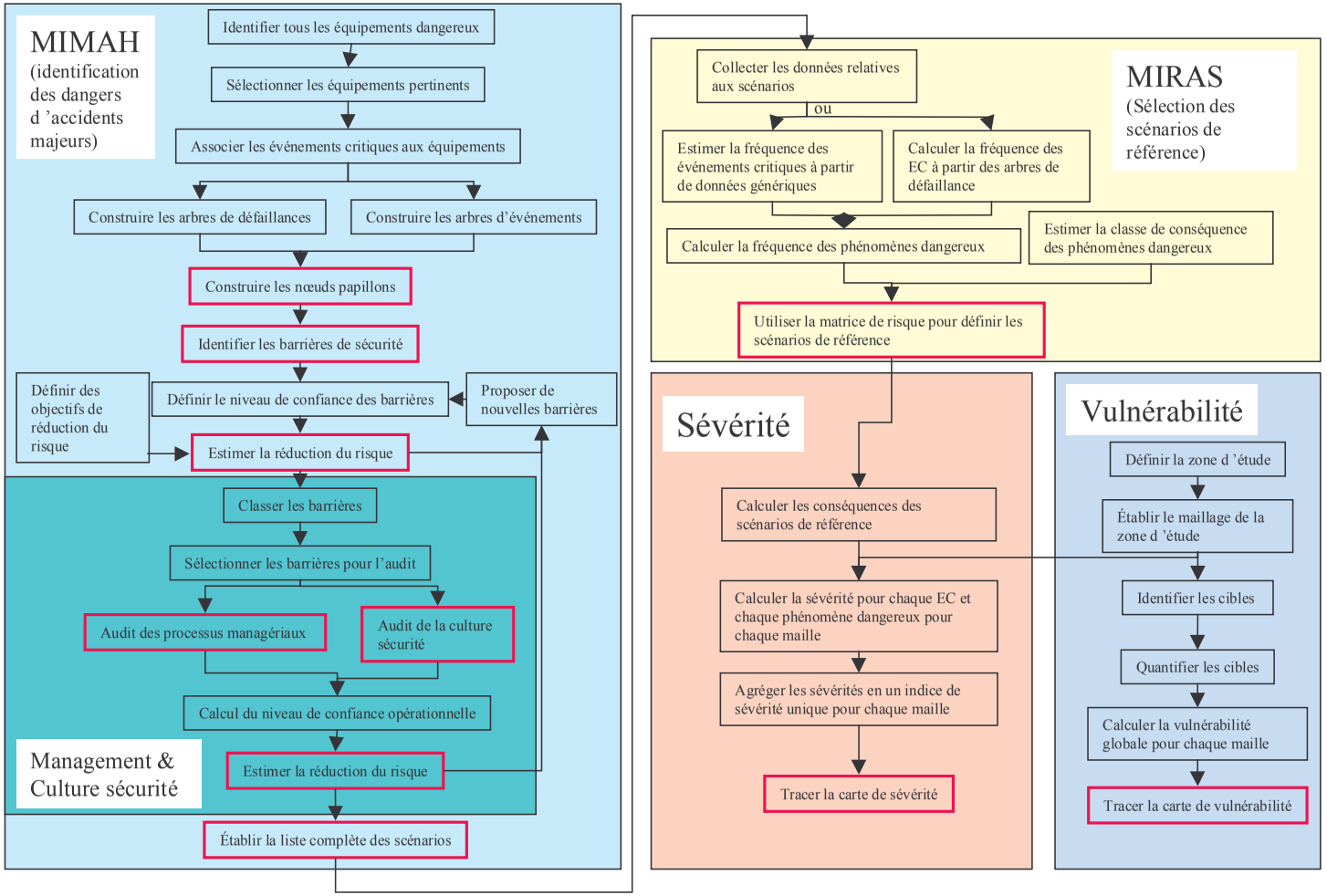


Figure 13 : Synoptique de la méthode ARAMIS.

5.2 LOPA

La méthode LOPA [CCPS 2001] a été développée à la fin des années 1990 par le CCPS (Center for Chemical Process Safety). LOPA signifie Layer Of Protection Analysis (Analyse des niveaux de protection). C'est une méthode orientée barrière au même titre qu'ARAMIS. Les premières étapes sont d'ailleurs assez comparables à celles de la méthode ARAMIS, en termes de principes généraux, même si de nombreuses différences subsistent au niveau des détails des deux méthodes. En revanche, LOPA ne prévoit pas de représentation cartographique de la sévérité et de la vulnérabilité.

La méthode LOPA peut être décomposée en six principales étapes :

1. Etablissement des critères de sélection des scénarios à évaluer.

Cette étape est un préalable à l'analyse de risques. Elle fournit le moyen de limiter la durée de l'étude en ne considérant que les scénarios significatifs en termes de conséquences. Le critère peut être un critère d'intensité (quantité de produit rejeté, flux mesuré à la source) ou un critère de conséquence qui intègre implicitement l'existence d'enjeux aux alentours.

2. Développement des scénarios d'accident

Les scénarios d'accident sont développés sur la base d'une analyse de risques utilisant des outil traditionnels tels que l'AMDEC ou l'HAZOP. Les scénarios sont représentés sous forme d'un nœud papillon.

3. Identification des fréquences d'événements initiateurs

Une analyse détaillée des scénarios est entreprise en considérant chaque combinaison d'événements initiateurs associés à une conséquence. La fréquence d'occurrence de chaque événement initiateur est estimée sur la base de données internes de retour d'expérience ou de données issues de la littérature.

4. Identification des dispositifs de sécurité et de leurs probabilités de défaillance à la demande

Pour chaque scénario on identifie alors les dispositifs de sécurité, en considérant les critères de qualification de ces dispositifs que sont leur indépendance par rapport au phénomène ou à l'événement auquel ils s'appliquent, la capacité de réalisation du dispositif, la possibilité d'inspecter le dispositif. Les dispositifs qui répondent à ces critères sont qualifiés d'IPL (Independent Protection Layer), concept à rapprocher de celui d'EIPS (Eléments Importants Pour la Sécurité).

A chaque dispositif de sécurité est associée une probabilité de défaillance à la sollicitation qui correspond à un facteur de réduction du risque. LOPA fait référence de façon explicite au niveau d'intégrité de sécurité (SIL, Safety Integrity Level), inspiré de la norme CEI 61508. Les systèmes de sécurité considérés sont essentiellement techniques, mais il est en théorie possible de prendre aussi en compte les barrières humaines ou organisationnelles [Gowland 2006].

5. Estimation du risque

La probabilité du scénario d'accident est alors estimée en réduisant la probabilité de l'événement initiateur de plusieurs ordres de grandeur correspondant aux niveaux de SIL des dispositifs de sécurité retenus. Comme dans la méthode ARAMIS, des matrices de décision permettent de définir le niveau de réduction du risque minimum que doivent présenter les systèmes en fonction du niveau de conséquence possible du scénario et de la fréquence de l'événement initiateur. La méthode LOPA n'impose cependant pas d'utiliser ces matrices et l'utilisateur est libre de mettre en œuvre des calculs de sûreté de fonctionnement plus traditionnels s'il le souhaite et en a la possibilité.

6. Evaluation du risque par rapport aux critères d'acceptabilité

La dernière étape de la méthode consiste à s'assurer que le risque est maîtrisé, c'est à dire qu'il est bien inférieur aux critères d'acceptabilité qui ont été fixés au préalable. LOPA n'impose pas de type de critère prédéfini et propose ainsi quatre catégories de critères :

- une grille de criticité comportant une limite d'acceptabilité en termes de gravité et de fréquence ;
- un critère purement quantitatif portant sur le niveau de conséquence du scénario ;
- un critère spécifiant le nombre de dispositifs de sécurité indépendants nécessaires pour considérer qu'un scénario est suffisamment maîtrisé ;
- un critère de risque cumulé maximum pour un site ou un procédé.

Il n'est pas prévu dans LOPA de produire des informations utiles pour la maîtrise de l'urbanisation. Ainsi l'évaluation de la vulnérabilité et la cartographie de la sévérité ne sont pas abordées dans la méthode.

5.3 MOSAR

La méthode MOSAR [PERILHON 2003], Méthode Organisée Systémique d'Analyse de Risques, développée au CEA, est une méthode intégrée qui permet d'analyser les risques sur un site de manière progressive. Cette méthode repose sur le modèle MADS (Méthodologie d'Analyse du Dysfonctionnement des Systèmes) présenté en Figure 14. Celui-ci représente le processus de danger, c'est à dire la libération d'un flux de danger par un système source sous l'effet d'un événement initiateur interne ou externe et l'impact de ce flux sur une cible, qui peut elle-même devenir système source de danger pour un processus équivalent. La méthode MOSAR met particulièrement l'accent sur l'enchaînement des processus de danger entre systèmes composant une installation et est donc particulièrement adaptée à l'étude des synergies d'accident ou des effets domino.

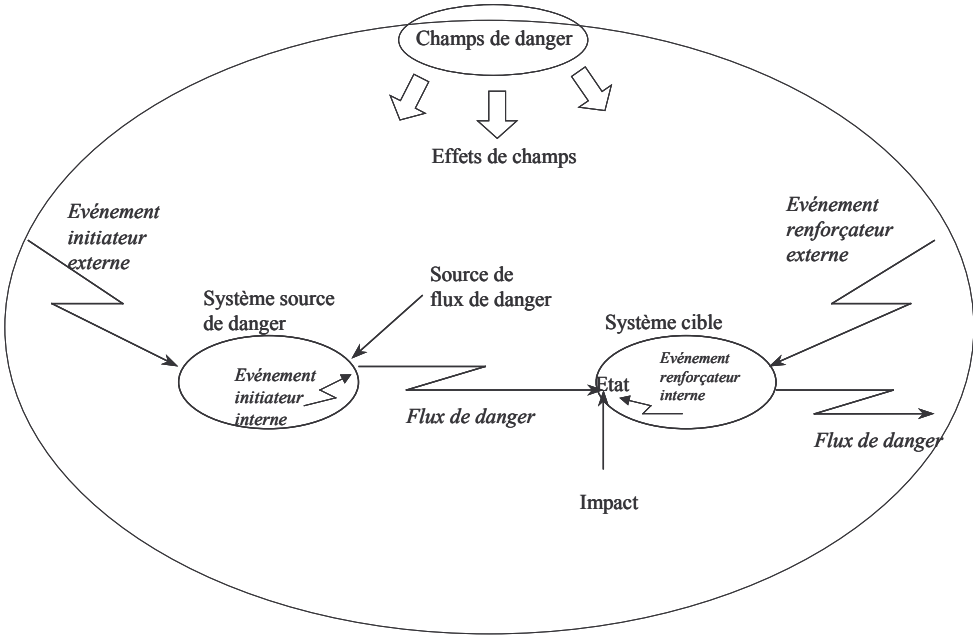


Figure 14 : le Modèle MADS du processus de danger

MOSAR est constituée de deux modules qui peuvent être utilisés de façon plus ou moins indépendante. Le module A correspond à une analyse macroscopique des risques sur un site industriel et s'apparente à une analyse préliminaire des risques. Le module B correspond à une analyse plus détaillée des scénarios identifiés dans le cadre du module A à l'aide des outils de la sûreté de fonctionnement.

La méthode MOSAR fait appel à des outils directement inspirés des méthodes d'analyse de risques traditionnelles : APR, AMDEC, arbres de défaillances. L'originalité de la méthode est d'en organiser l'utilisation et de proposer des grilles et des listes guides dans un souci d'exhaustivité. Par ailleurs, des outils sont proposés pour étudier les interactions entre sous-systèmes, notamment sous forme d'effets domino.

Les deux modules suivent à peu près la même structure :

Module A - analyse macroscopique :

- Représenter l'installation, identifier les sources de danger ;
- Identifier les dangers et construire les scénarios d'accident ;
- Evaluer les risques ;
- Négocier les objectifs de prévention ;
- Définir les barrières de sécurité.

Module B - analyse microscopique :

- Identifier les risques de dysfonctionnement ;
- Evaluer les risques en construisant des arbres de défaillance et en les qualifiant ;
- Négocier un objectif précis de prévention ;
- Affiner les moyen de prévention ;
- Gérer les risques.

Le module A de la méthode MOSAR s'appuie sur une liste des sources de danger et sur un tableau d'analyse de risques. La "grille 1", qui fait office de check-list, désigne des systèmes sources dont elle précise le danger (par exemple, systèmes sources de toxicité et d'agressivité), regroupés sous huit rubriques :

A- Systèmes sources de danger d'origine mécanique ;

B- Systèmes sources de danger d'origine chimique ;

C- Systèmes sources de danger d'origine électrique ;

D- Systèmes sources de danger de développement d'incendie ;

E- Systèmes sources de danger liés aux rayonnements ;

F- Systèmes sources de danger de nature biologique ;

G- Systèmes sources de danger liés à l'environnement actif ;

H- Systèmes sources de danger d'origine économique et sociale.

L'évaluation de la probabilité est faite, au choix de l'utilisateur de façon qualitative, semi-quantitative ou quantitative à l'aide des outils classiques présentés plus haut (arbres des défaillances, arbres d'événements). MOSAR prescrit par ailleurs explicitement l'identification et la qualification des barrières de sécurité et établit la distinction entre barrières techniques et barrières d'utilisation (qualifiées dans d'autres méthodes de barrières humaines).

5.4 QRA

L'analyse quantitative des risques [Bedford 2001], en anglais Quantitative Risk Assessment (QRA), est une méthode dont l'objectif est d'évaluer la probabilité de dommages causés par un accident potentiel. Cette méthode, initialement développée dans le domaine des transports et dans le nucléaire a été progressivement adaptée à l'industrie des procédés, notamment dans les pays du nord de l'Europe. La particularité des méthodes de QRA tient dans la façon d'exprimer et de représenter les résultats de l'analyse de risques. On calcule généralement d'une part la probabilité qu'un individu, à un emplacement donné, meure des effets de l'accident, qualifié de risque individuel et, d'autre part, la fraction de la population susceptible de mourir des effets de l'accident et la fréquence associée, qualifiées de risque sociétal. Il est à noter que le QRA ne prend donc souvent en compte que les effets létaux sur les personnes[20]. Ces résultats sont généralement représentés sous forme de c*ourbe fréquence/gravité* (ou courbe F/N) pour le risque sociétal ou de courbes *iso risque* pour le risque individuel.

Dans le domaine des risques liés aux installations fixes, la référence en matière de QRA reste l'ouvrage du Committee for the Prevention of Disasters, "guidelines for quantitative risk assessment" plus connu sous le titre de "Purple book" [CPR 18^{E}, 1999] qui constitue la référence pour l'établissement du QRA dans le cadre des procédures réglementaires hollandaises. Les principales étapes du QRA définies par le "Purple book" sont les suivantes :

- Sélection des installations pour le QRA

La sélection des installations repose sur le calcul pour chaque installation d'un indicateur A qui prend en compte la quantité de substance dangereuse stockée ou mise en œuvre, le type d'équipement (stockage ou process), l'exposition de l'installation à des conditions particulières, l'état physique de la substance et la nature de la substance. En fonction de la valeur que prend cet indicateur, l'installation est retenue ou non pour le QRA.

- Définition des événements redoutés centraux (pertes de confinement) et des fréquences associées

Pour chaque installation retenue pour le QRA, la méthode prévoit d'établir la liste des événements de perte de confinement potentiels. Ces événements sont considérés indépendamment de leurs causes sur la base d'une association préétablie entre une typologie d'équipements et une typologie d'événements. A chaque type d'événement, le "Purple book" associe une valeur de fréquence qui est utilisée pour les calculs probabilistes qui suivent. Ces valeurs sont issues d'études statistiques réalisées dans les années quatre-vingts essentiellement aux Pays-Bas. Elles reflètent donc un niveau de maîtrise moyen correspondant à la technologie de l'époque et du lieu ainsi qu'aux types d'industries concernées par l'étude (malheureusement non précisés). La méthode prévoit qu'il est possible d'altérer les données statistiques en fonction de

[20] Certaines version de QRA, dont celle développée par l'INERIS pour l'évaluation quantitative des risques liés au transport de marchandises dangereuses, prennent aussi en compte les risques de blessure.

l'environnement de l'exploitation en augmentant de façon forfaitaire (d'un facteur 3 à 10) la fréquence de référence si l'installation est soumise à des vibrations, des cycles thermiques importants ou des sources de corrosion/érosion. Si des barrières de sécurité supplémentaires sont présentes pour limiter ou mitiger les conséquences d'une perte de confinement il est en théorie possible de les prendre en compte en appliquant des méthodes de type arbre d'événements. En revanche, il n'est pas prévu de prendre en compte des barrières de prévention spécifiques qui viendraient réduire la probabilité d'une perte de confinement.

- Modélisation de l'intensité du phénomène

L'étape suivante est une étape de modélisation des conséquences. Elle conduit à calculer l'intensité du phénomène dangereux pour chaque événement de perte de confinement issu de l'étape précédente. L'intensité s'exprime par la répartition des concentrations en substance toxique, par des niveaux de flux thermique ou par des niveaux de surpression en fonction du phénomène considéré. Les modèles à utiliser sont ceux qui sont décrits dans le "Yellow Book"[CPR 14^{E} 1997]. Il s'agit de modèles de dispersion, d'effets thermiques et d'explosion classiques. Les modélisations sont réalisées pour différentes conditions météorologiques auxquelles sont associées des probabilités d'occurrence. Chaque ensemble de conditions initiales est aussi qualifié en terme de probabilité. Les résultats ainsi obtenus seront utilisés dans la dernière étape pour calculer le risque individuel et le risque sociétal. A ce stade, ces résultats sont exprimés en termes d'intensité du phénomène et de probabilité associée à cette intensité.

- Modélisation de l'exposition et des dommages

Cette étape consiste à convertir des intensités de phénomènes dangereux (concentration de gaz toxique, flux thermique, onde de pression) en probabilité de mort d'un individu exposé et en fraction de population tuée. Les fonctions de probit sont utilisées à cette fin. Les modèles utilisés sont décrits dans le "Green Book"[CPR 16^{E}, 1992] et dans le "Purple Book" [CPR 18^{E}, 1999].

- Calcul et présentation des résultats.

La dernière étape du calcul permet en premier lieu d'estimer le risque individuel, qui est calculé en effectuant la somme des probabilités de mort associées à chaque résultat de l'étape 3. Le risque sociétal est ensuite obtenu en divisant l'espace autour de l'installation en cellules d'égale superficie et en évaluant la population potentiellement exposée dans chaque cellule et le nombre de morts parmi cette population pour chaque résultat de l'étape 3. En effectuant la somme du nombre de morts de chaque cellule environnant l'installation pour un scénario donné et un ensemble de conditions données, on obtient la contribution en nombre de morts de ce scénario et de cet ensemble de conditions. Pour établir le risque sociétal, on établit alors des classes de mortalité (1, 10, 100, 1000 morts) et, pour chacune de ces classes, on calcule la somme des fréquences (F_N) des scénarios qui peuvent produire un nombre supérieur ou égal au nombre de morts (N) de la classe. La représentation graphique des fréquences associées à chaque classe produit une courbe F/N.

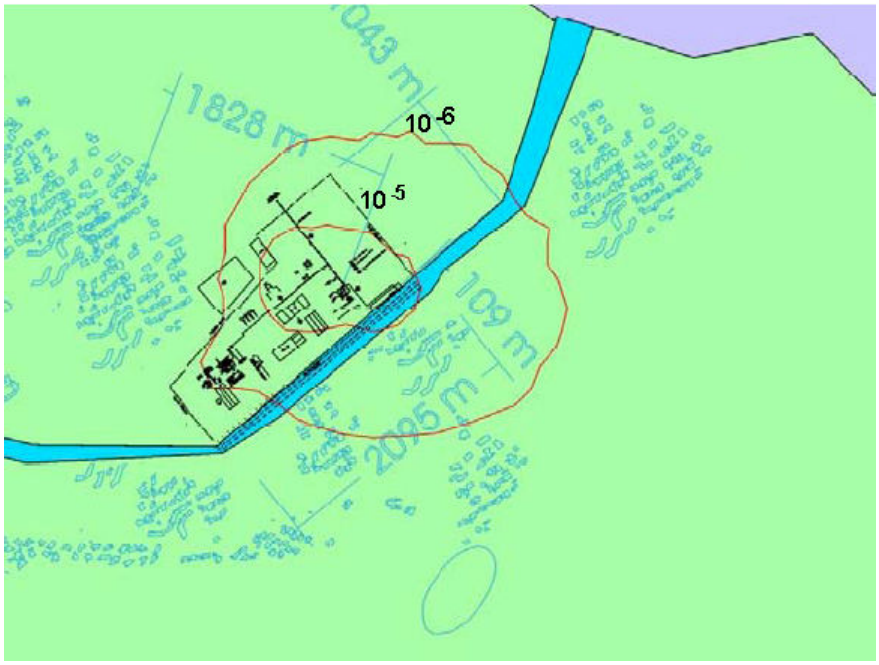


Figure 15 : Exemple de courbe iso risque ou carte du risque individuel (fictive)

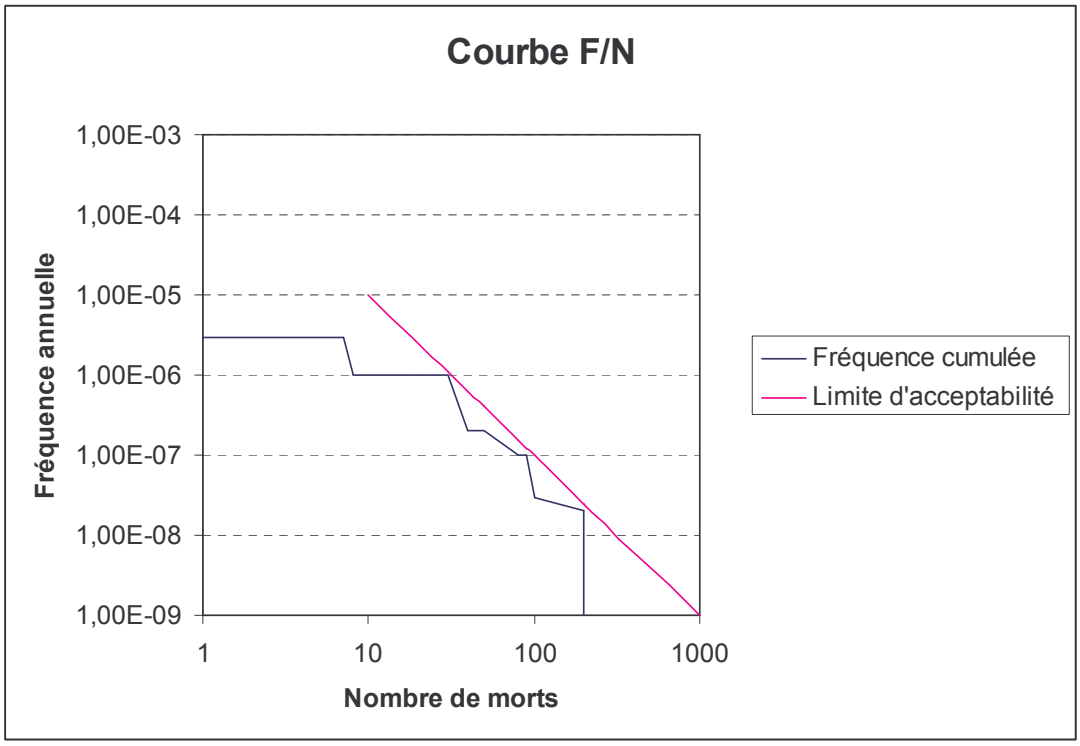


Figure 16 : représentation du risque sociétal courbe F/N typique (d'après [CPR 18^{E}, 1999])

Les résultats du QRA peuvent donc être représentés de deux manière : soit sous la forme d'une carte du risque individuel (Figure 15), soit sous la forme d'une courbe F/N (Figure 16). Dans les deux cas, l'exploitation de ces résultats pour la prise de décision implique la définition d'un niveau de risque acceptable en terme de probabilité de mortalité.

Même si par plusieurs aspects, ARAMIS et LOPA peuvent être rapprochées de la méthode du QRA, celle-ci se distingue des deux autres par le fait qu'elle est moins adaptée à la prise en compte des barrières de prévention spécifiques au site étudié. Seules les barrières permettant de limiter ou mitiger une perte de confinement peuvent être explicitement considérées pour le calcul de la probabilité finale de dommages. Le QRA est donc moins adapté à la démonstration de la maîtrise du risque sur un site industriel comme le demande la directive SEVESO II.

6 DEMARCHE D'ANALYSE DE RISQUES PRATIQUEE PAR L'INERIS DANS LES ETUDES DE DANGERS

La démarche d'analyse des risques pratiquée par l'INERIS dans les études de dangers est décrite en détails dans le rapport Oméga 9 sur les études de dangers [Joly 2006]. Nous n'en rappelons donc ici que les principales caractéristiques. Elle se déroule en deux étapes. Une première Analyse Préliminaire des Risques (APR) permet d'identifier l'ensemble des scénarios d'accident potentiel. Elle est suivie d'une étude détaillée des risques qui permet de qualifier les scénarios jugés critiques en termes de probabilité et gravité.

6.1 L'ANALYSE PRELIMINAIRE DES RISQUES

6.1.1 LE DEROULEMENT DE L'APR EN SEANCE

Le support utilisé par la Direction des Risques Accidentels de l'INERIS pour la mise en œuvre de la méthode est un tableau qui est rempli, en partie, en séances d'Analyse Préliminaire des Risques. Un exemple figure ci-après :

Section étudiée : **Installation :** **PID :**	**Mode de fonctionnement :** **Entrée de la maille :** **Sortie de la maille :**

N°	Cause (de la dérive)	Dérive	Evènement Redouté Central	Phénomène dangereux	Fréquence de la cause	Intensité (de 1 à 4)	Gravité sur les populations	Gravité sur l'environ-nement	Barrières de sécurité					NC
									Intitulé	Cause	Dérive	ERC	Phéno	

Tableau 15 : Exemple de tableau utilisé dans les Analyses Préliminaires des Risques

A partir du tableau, le groupe de travail adopte une démarche systématique sous la forme suivante :

1) **Sélection du système ou de la fonction** à étudier sur la base de la description fonctionnelle réalisée au préalable.

2) **Choix d'un équipement ou produit** pour ce système ou cette fonction.

3) Pour cet équipement, prise en compte d'**une première situation de dangers** (colonne « Evènement Redouté Central »).

4) Pour cet ERC, identification de **toutes les causes** (colonnes « Dérive » et « Causes ») **et des phénomènes dangereux susceptibles de se produire directement ou par effets dominos** (colonne « Phénomène Dangereux »).

5) Cotation de la **fréquence** d'occurrence de la cause envisagée sans prise en compte des barrières de sécurité existantes selon l'échelle de cotation choisie par le groupe, (un exemple est donné en Tableau 2 au chapitre 3).

6) Pour les phénomènes dangereux identifiés, estimation de l'**intensité** des effets et cotation associée en fonction de l'échelle de cotation considérée par le groupe, (voir l'exemple en Figure 3 au chapitre 3).

7) Pour un enchaînement Cause-ERC-Phénomène Dangereux donné, identification des **barrières de sécurité existantes** sur l'installation.

8) Evaluation préliminaire du **niveau de confiance** des barrières de sécurité listées en considérant aussi leur indépendance, leur capacité de réalisation ou efficacité et leur de temps de réponse.

9) Si l'analyse montre l'apparition de nouveaux phénomènes dangereux induits par le fonctionnement, voire le dysfonctionnement de certaines barrières de sécurité (ex : soupapes), une nouvelle ligne est créée dans le tableau d'APR traduisant un nouveau scénario d'accident, potentiellement majeur.

10) Si tous les enchaînements ont été étudiés, choix d'un **nouvel ERC,** ou d'une nouvelle dérive, pour le même équipement et retour au point 4).

11) Lorsque toutes les situations de dangers ont été passées en revue pour l'équipement considéré, choix d'un **nouvel équipement** et retour au point 3) précédent.

12) Le cas échéant, lorsque tous les équipements ont été examinés, choix d'**un nouveau système ou fonction** et retour au point 2).

6.1.2 PRODUITS DE SORTIE DE L'APR

En fin d'Analyse Préliminaire des Risques, l'industriel dispose donc des données suivantes :

- cotation en intensité des phénomènes dangereux, permettant d'identifier ceux qui peuvent potentiellement conduire à un accident majeur ;
- liste des phénomènes dangereux pouvant avoir des effets à l'extérieur du site ;
- liste des scénarios (et donc des causes) pouvant induire chaque phénomène dangereux ;
- cotation des scénarios, en terme de fréquence, d'apparition des causes (en l'absence de mesures préventives ou protectrices) conduisant à l'occurrence des scénarios accidentels ;
- liste des barrières de sécurité performantes mises en œuvre pour la maîtrise des scénarios accidentels considérés, et niveaux de confiance éventuellement déterminés (selon le type d'approche choisi).

6.2 L'ETUDE DETAILLEE DES RISQUES

La finalité de l'étude détaillée est de porter un examen approfondi sur les phénomènes dangereux susceptibles de conduire à un accident majeur, c'est-à-dire, ceux dont les effets peuvent atteindre des enjeux à l'extérieur de l'établissement, et de vérifier la maîtrise des risques associés.

Du point de vue pratique, l'INERIS réalise cette étape en partie avec le groupe de travail, notamment pour ce qui est relatif à l'évaluation des barrières de sécurité et aux itérations rendues nécessaires par la démarche de réduction des risques.

A l'issue de ce travail, l'industriel doit disposer d'une vision globale des risques résiduels associés à ses installations se traduisant par une caractérisation de la probabilité d'occurrence et de la cinétique d'apparition des phénomènes dangereux susceptibles de conduire à un accident majeur. Celle-ci s'obtient en agrégeant l'ensemble des scénarios autour d'un même phénomène dangereux, en prenant en compte les barrières de sécurité performantes. Pour ce faire, l'INERIS utilise le nœud papillon.

Cette étape sera ensuite complétée par une caractérisation des effets associés aux phénomènes dangereux considérés en prenant en compte les barrières jugées performantes, nécessitant des modélisations à l'aide d'outils de calcul adaptés.

Concernant la caractérisation en probabilité, celle-ci est réalisée en reportant sur le nœud papillon les valeurs qualitatives, semi-quantitatives ou quantitatives de fréquence d'occurrence de chaque événement initiateur ou cause, ainsi que les taux de défaillance ou niveaux de confiance des barrières de sécurité. La probabilité de l'événement critique est obtenue en appliquant soit les règles classiques de calcul dans les arbres de défaillance soit leur traduction simplifiée pour une approche semi-quantitative qualifiée « d'approche barrière ».

Ceci est illustré dans l'exemple qui suit (Figure 17). Dans cet exemple, le niveau de confiance des barrières de sécurité a été estimé et retranscrit en terme de probabilité de défaillance à la sollicitation suivant la règle suivante :

$$P = 10^{-NC}$$

Ces probabilités de défaillance des barrières à la sollicitation viennent pondérer la fréquence de la cause sur laquelle elles agissent.

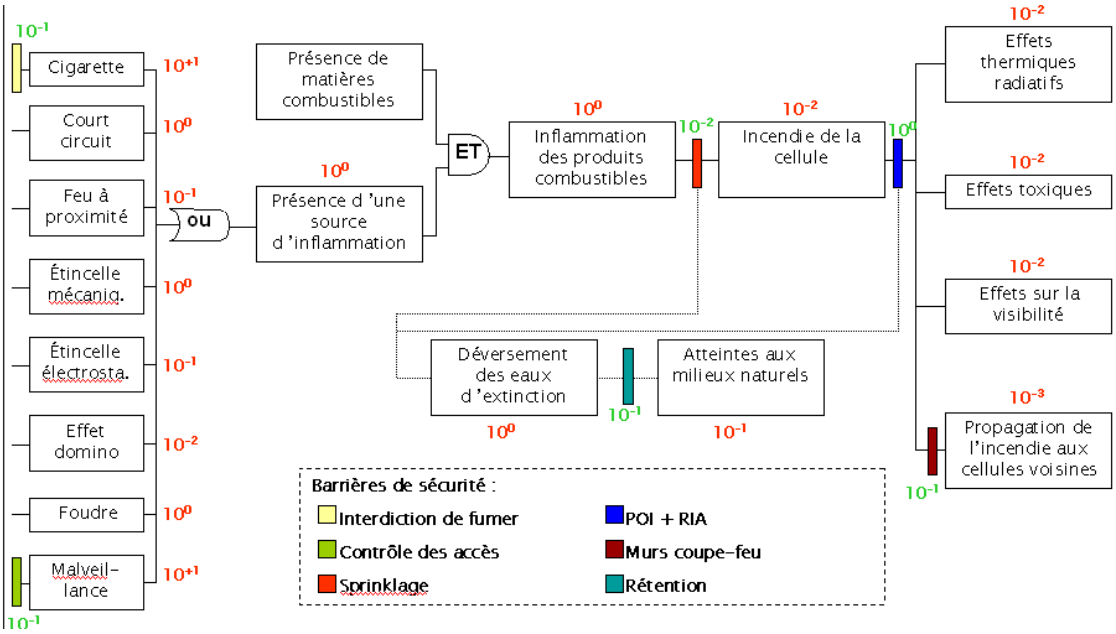


Figure 17 : Exemple de détermination de la probabilité résiduelle d'un phénomène dangereux

A l'issue de l'étude détaillée de réduction des risques, le groupe de travail propose, le cas échéant (pour les établissements AS), une première liste de barrières Importantes Pour la Sécurité, avec leurs éléments constitutifs.

A l'issue de l'étape d'étude détaillée de réduction des risques, l'exploitant dispose :

- de la caractérisation en probabilité et cinétique des phénomènes dangereux susceptibles de conduire à un accident majeur ;
- d'une démonstration de la maîtrise des risques d'accidents majeurs par la mise en place de barrières de sécurité adaptées et performantes, prenant en compte toutes les combinaisons d'événements envisagées ; le cas échéant, des mesures complémentaires de réduction des risques auront été suggérées.
- d'une liste de fonctions IPS et barrières associées.

7 POINTS FORTS ET LIMITES DES METHODES D'ANALYSE DES RISQUES

7.1 POINTS FORTS DES METHODES CLASSIQUES D'ANALYSE DES RISQUES

Les chapitres précédents ont présenté les avantages et les limites associés à chacune des méthodes d'analyse des risques présentées dans ce document dont nous proposons une synthèse dans ce septième chapitre.

7.1.1 CARACTERE SYSTEMATIQUE

Le premier avantage des méthodes d'analyse des risques réside dans leur **caractère systématique**.

En effet, ces dernières permettent d'envisager de manière méthodique, les différentes situations de danger et évènements redoutés ainsi que leurs causes et conséquences.

Cet aspect systématique est particulièrement important en vue d'identifier les situations de danger de la manière la plus exhaustive possible.

Par ailleurs, ces méthodes permettent d'apporter des éléments techniques pour juger de la maîtrise des risques à la source, grâce notamment à l'identification de barrières de sécurité existantes ou à envisager face aux risques considérés. Cette maîtrise des risques ne peut effectivement être démontrée que si l'ensemble des causes et conséquences physiquement envisageables a été envisagé. A l'échelle d'un site industriel, ce travail peut s'avérer complexe et ces méthodes constituent ainsi une aide précieuse pour guider la réflexion.

7.1.2 OUTILS D'ECHANGE ET DE COMMUNICATION

La plupart des méthodes d'analyse des risques trouvent leur pleine efficacité lorsqu'elles sont mises en œuvre au sein d'un groupe de travail pluridisciplinaire. A ce titre, elles constituent un outil d'échange et de communication entre des personnes de sensibilités et de métiers différents.

Ainsi, la richesse de ces méthodes ne se trouve pas dans leurs principes de base, mais bien dans l'expérience réunie au sein de ce groupe de travail. Les réunions ainsi menées permettent donc de partager des expériences diverses et de réfléchir de manière globale et réaliste à la sécurité de l'installation examinée.

7.1.3 COMPLEMENTARITE DES METHODES

Comme nous l'avons vu précédemment, ces méthodes d'analyse des risques sont généralement complémentaires.

Des méthodes assez simples telles que l'APR permettent d'identifier les risques principaux associés à une installation ainsi que les barrières de sécurité qui y sont adjointes. Cette première analyse peut être utilement complétée par une analyse plus fine grâce à des méthodes comme l'AMDEC ou l'HAZOP, en faisant porter l'étude sur les parties particulièrement critiques de l'installation. En dernier lieu, les résultats de cette nouvelle phase d'analyse peuvent donner matière à l'examen d'évènements jugés critiques grâce à des outils permettant de combiner les défaillances tels que l'analyse par arbre des défaillances ou arbre des causes.

Cette diversité permet donc de retenir les outils les plus adaptés au cas particulier à traiter et de pouvoir assurer une analyse en profondeur d'une installation en utilisant des outils de plus en plus dédiés à des parties bien définies de ce système.

7.2 LIMITES INHERENTES AUX METHODES CLASSIQUES D'ANALYSE DES RISQUES

7.2.1 RISQUES D'AGRESSIONS EXTERNES

Bien que les méthodes présentées dans ce document puissent considérer l'éventualité d'agressions externes affectant l'installation étudiée, elles sont principalement dédiées à l'identification des risques générés par cette installation sur son environnement.

En d'autres termes, il est indispensable de mener au préalable une phase d'identification des sources d'agressions externes comme celles associées à la possibilité d'effets dominos, aux conditions climatiques ou environnementales (foudre, séismes…) ou aux actes de malveillance.

Par exemple, dans le cadre d'une étude des dangers qui vise à l'identification et la maîtrise de tous les risques possiblement envisageables, l'analyse des risques ne se résume pas à l'utilisation d'une APR ou d'une AMDEC par exemple, mais doit également intégrer l'utilisation d'outils dédiés aux risques d'origine externe. A titre d'exemple, signalons que l'étude des dangers doit s'accompagner d'une étude foudre lors d'une procédure de demande d'autorisation d'exploiter.

7.2.2 ESTIMATION DU RISQUE

Les méthodes d'analyse des risques permettent au groupe de travail d'estimer les risques en terme de probabilité et de gravité. Au niveau de l'analyse des risques, cette estimation des risques est effectuée de manière simplifiée et ne doit pas être considérée comme un outil précis d'évaluation. Cette phase vise simplement à donner des indications sur les risques jugés a priori les plus importants en vue d'envisager de la manière la plus efficace possible, les mesures de prévention et de protection devant être engagées.

En effet, il est parfois impossible de juger a priori de la gravité d'un accident potentiel tant le nombre de paramètres intervenant dans les résultats est important. C'est notamment le cas pour les rejets à l'atmosphère de gaz toxiques.

En résumé, la phase d'estimation des risques suite à l'utilisation de ces méthodes permet notamment d'identifier les risques les plus importants. Pour ces risques jugés les plus critiques, une évaluation plus fine de la gravité peut demeurer indispensable. Cette évaluation est effectuée à partir de scénarios d'accident et moyennant l'utilisation de modélisations plus ou moins complexes selon les phénomènes à traiter et l'environnement du site.

7.2.3 EXHAUSTIVITE

Tous les outils systématiques d'analyse des risques visent à tendre vers le plus d'exhaustivité possible. Néanmoins, force est de constater qu'il est impossible de garantir une exhaustivité totale. En d'autres termes, leur utilisation ne garantit pas une identification complète de toutes les causes potentielles d'un accident majeur car :

- La richesse de ces méthodes s'appuie sur l'expérience acquise au sein du groupe de travail. Il semble néanmoins humainement impossible d'envisager toutes les causes possibles d'un accident potentiel. Ce constat apparaît d'autant plus vrai que l'on traite le plus souvent d'évènements ou de combinaisons d'évènements particulièrement rares.
- La qualité des résultats et leur caractère exhaustif dépendent également du temps et des moyens consacrés à l'analyse. Plus ces moyens seront importants, plus on tendra vers une exhaustivité totale. Cette remarque met en outre en lumière l'importance du caractère itératif de l'analyse des risques.

En résumé, retenons donc que l'utilisation de méthodes d'analyse des risques tels que celles présentées dans ce document constitue une aide précieuse pour l'identification des risques mais ne garantit pas à 100 % que tous les accidents susceptibles de survenir auront bien été identifiés.

7.3 POINTS FORTS DES METHODES INTEGREES D'ANALYSE DE RISQUES

Les méthodes intégrées présentées au chapitre précédent ont été développées pour compenser certaines limites des outils d'analyse simples tels que l'AMDEC, l'HAZOP.

Elles visent avant tout à organiser l'utilisation des outils dans une démarche globale d'estimation des risques. Elles ne se limitent donc pas à l'identification des scénarios et à l'estimation rapide de la probabilité mais intègrent des étapes d'estimation de l'intensité des phénomènes, d'identification et de qualification des barrières de sécurité, de présentation des résultats dans des formats adaptés à une utilisation dans le cadre d'un processus décisionnel donné.

Les méthodes intégrées proposent généralement des outils supports à leur mise en œuvre : listes guides, outils logiciels, systèmes d'information géographique. Elles précisent la manière d'opérer pour certaines estimations qui demeurent non définies dans les outils de base : estimation de la probabilité, de la fiabilité des barrières de sécurité, etc.

7.4 LIMITES DES METHODES INTEGREES D'ANALYSE DE RISQUES

La contrepartie des points forts des méthodes intégrées est une lourdeur apparente de mise en oeuvre. Elle tient au nombre d'étapes composant ces méthodes, notamment des étapes de mise en forme et de présentation des résultats. Cette lourdeur doit cependant être relativisée dans la mesure où les résultats des outils classiques d'analyse doivent aussi faire l'objet d'une mise en forme et d'un traitement pour répondre aux besoins des décideurs dans les processus complexes tels que ceux conduisant à la maîtrise de l'urbanisation, par exemple.

7.5 SYNTHESE DES AVANTAGES ET DOMAINES D'APLICATION DES METHODES PRESENTEES

Le Tableau 16 présente une synthèse des principales caractéristiques des méthodes présentées dans ce document : domaine d'application, objectif, facilité de mise en œuvre, niveau d'intégration, prise en compte de la vulnérabilité et prise en compte des barrières de sécurité.

La facilité de mise en œuvre est cotée dans une échelle à quatre niveaux allant de 1= facile à 4= difficile. Cette cotation tient compte essentiellement de la complexité de la méthode et du temps nécessaire à sa mise en œuvre. En revanche des méthodes en apparence simples, comme la méthode APR nécessitent une grande expertise de la part de l'analyste pour fournir des résultats pertinents.

Le niveau d'intégration représente la maille à laquelle s'appliquent les résultats de l'analyse. Les méthodes intégrées permettent généralement d'agréger à l'échelle d'une installation des résultats obtenus avec des méthodes élémentaires pour les sous-systèmes composant l'installation.

Tableau 16 : Principales caractéristiques des méthodes d'analyse de risques

	Type d'industrie	Objectif	Facilité de mise en œuvre*	Niveau d'intégration*	Remarque	Intègre une analyse de vulnérabilité des enjeux externes pour l'évaluation des conséquences	Approche barrière
Méthodes élémentaires inductives (recherche des conséquences potentielles d'un événement)							
Analyse Préliminaire des Risques (APR)	Tout type, installations simples	Identifier les dérives et leurs conséquences potentielles	1	Installation (voire site)		Implicite	Non quantifiée
AMDE et AMDEC	Systèmes techniques, processus discrets	Analyser finement les modes de défaillance des composants d'un système technique et leurs conséquences	2	Sous-système	Nécessite une décomposition poussée du sous-système	Non	Non quantifiée
HAZOP	Systèmes techniques thermo-hydrauliques	Analyser finement les causes et conséquences potentielles de dérives d'un système (adapté aux procédés)	3	Sous-système	Nécessite une décomposition poussée du sous-système	Non	Non quantifiée
What-If	Tout type, installations simples, systèmes techniques	Identifier les dérives et leurs conséquences potentielles	2	Installation ou sous-système	Nécessite une bonne connaissance du système, pas d'analyse des causes	Non	Non quantifiée
Analyse par arbre des évènements (AdE)	Tous	Analyse inductive : Représenter les conséquences possibles d'un événement Généralement en analysant les conséquences des fonctionnements et dysfonctionnements des barrières	3	Sous-système	Utile pour une visualisation et une analyse systématique des conséquences de dysfonctionnements des barrières.	Non	Les événements sont souvent des fonctionnements ou dysfonctionnements d'éléments de contrôle du procédé ou de barrières de sécurité.

	Type d'industrie	Objectif	Facilité de mise en œuvre	Niveau d'intégration	Remarque	Intègre une analyse de vulnérabilité des enjeux externes pour l'évaluation des conséquences	Approche barrière
Méthodes élémentaires déductives (recherche des causes potentielles d'un événement)							
Analyse par arbre des défaillances (AdD)	Tous	Analyse déductive : rechercher les causes d'un événement Représenter le scénario d'accident : analyse des causes. Effectuer des calculs probabilistes Plus récemment : représenter les barrières de sécurité et leur impact sur un scénario	3	Sous-système	Souvent (mais pas obligatoirement) construit suite à une APR, AMDEC ou HAZOP	Non	Deux approches possibles : représentation des défaillances des barrières comme des événements Représentation des barrières comme obstacles à la propagation du scénario
Méthode élémentaire mixte							
Analyse par nœud papillon	Tous	Analyser des scénarios complets d'accident majeur des événements initiateurs aux conséquences sur les éléments vulnérables environnants.	3	Sous-système	Le nœud papillon est l'assemblage de deux arbres inspirés d'un arbre de défaillances et d'un arbre d'événements.	Non	Représentation des barrières comme obstacle à la propagation du scénario. Très adapté à la démonstration de la maîtrise du risque par les barrières de sécurité.

	Type d'industrie	Objectif	Facilité de mise en œuvre	Niveau d'intégration	Remarque	Intègre une analyse de vulnérabilité des enjeux externes pour l'évaluation des conséquences	Approche barrière
Méthodes intégrées							
MOSAR	Tous	Analyser les risques d'un système industriel à différents niveaux d'analyse , mettre en évidence les moyens de maîtrise du risque	4	Installation	Utilise les AdD et des outils dérivés de l'APR et de l'AMDEC	Implicite	Approche uniquement qualitative
LOPA	Industries des procédés	Analyser les risques d'un système industriel à différents niveaux d'analyse , mettre en évidence les moyens de maîtrise du risque, produire des résultats utiles pour les décisions d'autorisation et de maîtrise de l'urbanisation	4	Site	Utilise les AdD et AdE	Non	Approche quantifiée fondée sur la notion de SIL Issue de la norme CEI 61508
ARAMIS	Industrie des procédés (soumises à la directive SEVESO)	Analyser les risques d'un système industriel à différents niveaux d'analyse , mettre en évidence les moyens de maîtrise du risque, produire des résultats utiles pour les décisions d'autorisation et de maîtrise de l'urbanisation	4	Site	Utilise le nœud papillon	Oui (évaluation découplée de la sévérité et de la vulnérabilité)	Approche quantifiée fondée sur la notion de SIL Issue de la norme CEI 61508
QRA	Tous	Estimer le risque individuel et sociétal associé à une installation industrielle	4	Site	Utilise des données génériques	Oui (pour le risque sociétal)	Pas de prise en compte explicite des barrières dans la méthode décrite dans le "Purple book"

8 CONCLUSION

Les méthodes d'analyse des risques décrites dans ce document sont fréquemment utilisées dans le domaine de la prévention des risques. Procurant un caractère systématique à l'analyse, elles permettent :

- d'identifier les causes et les conséquences potentielles d'évènements liés à l'exploitation d'installations industrielles,
- de mettre en lumière les barrières de sécurité existantes ou pouvant être envisagées au regard du risque.

Fréquemment associées à une démarche d'évaluation semi-quantitative, elles visent à identifier les risques les plus importants et à envisager en conséquence des propositions d'améliorations.

L'utilisation de ces méthodes est particulièrement recommandée pour l'analyse des risques dans le cadre d'une étude des dangers, puisqu'elles permettent de viser à plus d'exhaustivité pour l'identification et tendre ainsi vers la maîtrise des risques majeurs.

Il n'existe pas de bonne ou de mauvaise méthode d'analyse des risques. Chacune possède des avantages et des inconvénients qui lui sont propres. Une méthode particulière est donc généralement plus ou moins adaptée au contexte de l'installation étudiée et aux objectifs recherchés.

Par ailleurs, il ne s'agit en définitive que d'outils permettant de guider la réflexion menée au sein d'un groupe de travail pluridisciplinaire. La véritable richesse de l'analyse des risques réside précisément dans la réunion de personnes de compétences variées.

Rappelons enfin que ces outils ne peuvent assurer une exhaustivité totale de l'identification des causes potentielles de sinistres.

Ce dernier constat met en avant la nécessité d'une démarche itérative conduisant à utiliser, lorsque le contexte le justifie[21], des outils de plus en plus complexes pour une analyse de plus en plus fine des risques, en combinant par exemple plusieurs des méthodes présentées dans ce document. C'est ce que permettent de faire les méthodes intégrées présentées au chapitre 6.

[21] Il est bon de rappeler ici le principe de proportionnalité qui stipule que les efforts réalisés pour l'analyse de risques doivent être en rapport avec le niveau de risque global de l'installation. L'utilisation des méthodes simples permet une première estimation de ce niveau. Si le niveau de risque (en particulier le niveau de danger) est élevé et combiné à un niveau élevé de vulnérabilité des éléments environnants, une analyse détaillée à l'aide de méthodes plus complexes se justifie.

9 GLOSSAIRE

Les définitions présentées dans les paragraphes suivants s'appuient autant que possible sur des normes et textes réglementaires traitant des aspects liés à la sécurité et la prévention des accidents majeurs. En particulier, le glossaire technique des risques technologiques, annexé à la Circulaire n° DPPR/SEI2/MM-05-0316 du 7 octobre 2005 relative aux Installations classées, a été pris comme référence.

Pour plus de clarté, les définitions issues de textes réglementaires ou de normes sont encadrées. Les définitions proposées dans le cadre de ce document sont, quant à elles, présentées sans encadrement.

9.1 RISQUE ET DANGER

Il existe de nombreuses définitions pour caractériser le sens du mot « risque ». Dans le vocabulaire courant, ce terme est d'ailleurs souvent confondu avec la notion de « danger ».

Dans le cadre de ce document, la définition de « risque » donnée dans le Guide ISO/CEI 51 :1999 « Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes » a été prise comme référence.

Risque (Guide ISO/CEI 51 :1999)

Combinaison de la probabilité d'un dommage et de sa gravité.

Le terme dommage répond quant à lui à la définition suivante, également extraite du Guide ISO/CEI 51.

Dommage (Guide ISO/CEI 51 :1999)

Blessure physique ou atteinte à la santé des personnes, ou atteinte aux biens ou à l'environnement.

Pour ce qui concerne le concept « danger », il est possible de se référer à la Directive 96/82/CE dite « SEVESO II », concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses. Ce texte propose la définition suivante :

Danger (Directive 96/82/CE)

Propriété intrinsèque d'une substance dangereuse ou d'une situation physique de pouvoir provoquer des dommages pour la santé humaine et/ou l'environnement.

Aléa (Circulaire n° DPPR/SEI2/MM-05-0316 du 7 octobre 2005)

Probabilité qu'un phénomène accidentel produise en un point donné des effets d'une intensité donnée, au cours d'une période déterminée. L'aléa est donc l'expression, pour un type d'accident donné, du couple (Probabilité d'occurrence x Intensité des effets). Il est spatialisé et peut être cartographié. (Circulaire du 02/10/03 du MEDD sur les mesures d'application immédiate introduites par la loi n° 2003-699 en matière de prévention des risques technologiques dans les installations classées).

Probabilité d'occurrence (Circulaire n° DPPR/SEI2/MM-05-0316 du 7 octobre 2005)

Au sens de l'article L.512-1 du code de l'environnement, la probabilité d'occurrence d'un accident est assimilée à sa fréquence d'occurrence future estimée sur l'installation considérée. Elle est en général différente de la fréquence historique et peut s'écarter, pour une installation donnée, de la probabilité d'occurrence moyenne évaluée sur un ensemble d'installations similaires.

Attention aux confusions possibles :

1. assimilation entre probabilité d'un accident et celle du phénomène dangereux correspondant, la première intégrant déjà la probabilité conditionnelle d'exposition des cibles. L'assimilation sous-entend que les cibles sont effectivement exposées, ce qui n'est pas toujours le cas, notamment si la cinétique permet une mise à l'abri.

2. probabilité d'occurrence d'un accident x sur un site donné et probabilité d'occurrence de l'accident x, en moyenne, dans l'une des N installations du même type (approche statistique)

Probabilité d'occurrence d'un phénomène dangereux(Circulaire n° DPPR/SEI2/MM-05-0316 du 7 octobre 2005)

Cette probabilité est obtenue par agrégation des probabilités des scénarios conduisant à un même phénomène, ce qui correspond à la combinaison des probabilités de ces scénarios selon des règles logiques (ET/OU). Elle correspond à la probabilité d'avoir des effets d'une intensité donnée (et non des conséquences)

Attention aux confusion avec : probabilité d'accident.

9.2 CONSEQUENCES ET ACCIDENTS MAJEURS

Accident Majeur (Directive 96/82/CE) (Circulaire n° DPPR/SEI2/MM-05-0316 du 7 octobre 2005)

Événement tel qu'une émission, un incendie ou une explosion d'importance majeure résultant de développements incontrôlés survenus au cours de l'exploitation d'un établissement […], entraînant pour la santé humaine, à l'intérieur ou à l'extérieur de l'établissement, et/ou pour l'environnement, un danger grave, immédiat ou différé, et faisant intervenir une ou plusieurs substances dangereuses.

Phénomène dangereux (ou phénomène redouté) (Circulaire n° DPPR/SEI2/MM-05-0316 du 7 octobre 2005)

Libération d'énergie ou de substance produisant des effets, au sens de l'arrêté du 29/09/2005, susceptibles d'infliger un dommage à des cibles (ou éléments vulnérables) vivantes ou matérielles, sans préjuger l'existance de ces dernières. C'est une « Source potentielle de dommages » (ISO/CEI 51)

Note : un phénomène est une libération de tout ou partie d'un potentiel de danger, la concrétisation d'un aléa.

Ex de phénomènes : « incendie d'un réservoir de 100 tonnes de fuel provoquant une zone de rayonnement thermique de 3 kW/m2 à 70 mètres pendant 2 heures. », feu de nappe, feu torche, BLEVE, Boil Over, explosion, (U)VCE, dispersion d'un nuage de gaz toxique...

Ne pas confondre avec « accident » : Un phénomène produit des effets alors qu'un accident entraîne des conséquences/dommages.

Dans le domaine des risques industriels d'origine accidentelle, ce terme se rapportera le plus souvent à des phénomènes physiques tels qu'un incendie, une explosion, une dispersion de gaz toxique…

Eléments vulnérables (ou enjeux) (Circulaire n° DPPR/SEI2/MM-05-0316 du 7 octobre 2005)

Eléments tels que les personnes, les biens ou les différentes composantes de l'environnement susceptibles, du fait de l'exposition au danger, de subir, en certaines circonstances, des dommages. Le terme de « cible » est parfois utilisé à la place d'élément vulnérable. Cette définition est à rapprocher de la notion « d'intérêt à protéger » de la législation sur les installations classée (art. L.511-1 du Code de l'Environnement).

Vulnérabilité (Circulaire n° DPPR/SEI2/MM-05-0316 du 7 octobre 2005)

1/ « vulnérabilité d'une cible à un effet x » (ou « sensibilité ») : facteur de proportionnalité entre les effets auxquels est exposé un élément vulnérable (ou cible) et les dommages qu'il subit.

2/ « vulnérabilité d'une zone » : appréciation de la présence ou non de cibles ; vulnérabilité moyenne des cibles présentes dans la zone.

La vulnérabilité d'une zone ou d'un point donné est l'appréciation de la sensibilité des éléments vulnérables [ou cibles] présents dans la zone à un type d'effet donné.

Par exemple, on distinguera des zones d'habitat, des zones de terres agricoles, les premières étant plus vulnérables que les secondes face à un aléa d'explosion en raison de la présence de constructions et de personnes. (Circulaire du 02/10/03 du MEDD sur les mesures d'application immédiate introduites par la loi n° 2003-699 en matière de prévention des risques technologiques dans les installations classées).

(NB : zone d'habitat et zone de terres agricoles sont deux types d'enjeux. On peut différencier la vulnérabilité d'une maison en parpaings de celle d'un bâtiment largement vitré.)

9.3 DEFAILLANCES, DERIVES ET EVENEMENTS REDOUTES

Défaillance (Norme NF X60-500)

Cessation de l'aptitude d'une entité à accomplir une fonction requise.

Mode de défaillance (CEI 60812 :1995)

Effet par lequel une défaillance est observée sur une entité.

En pratique, il est souvent délicat de distinguer défaillance et mode de défaillance. Pour plus de clarté, prenons l'exemple d'une pompe dont la fonction principale est de fournir un certain débit. La défaillance de cette pompe concerne donc l'absence du débit désiré à la sortie de la pompe. Cette défaillance est notamment observée si la pompe ne démarre pas. L'effet « Ne démarre pas » est un mode de défaillance possible pour cet équipement.

Paramètre

Un paramètre sera ici défini comme une grandeur physiquement mesurable ou bien une action ou opération à réaliser.

En règle générale, les paramètres les plus fréquemment rencontrés dans des systèmes thermo-hydrauliques sont la température, la pression, le débit, la concentration, la densité, la viscosité, le temps…

Dérive (d'un paramètre)

Dans le cadre de ce document, la dérive d'un paramètre sera définie comme l'écart d'un paramètre par rapport à une valeur ou une intention de référence. Cet état de référence dépend notamment de l'état du système considéré (fonctionnement normal, arrêt, démarrage…). Une dérive est généralement le résultat d'une défaillance.

9.4 EVENEMENTS ET SITUATIONS DE DANGERS

Situation dangereuse (Guide ISO/CEI 51)

Situation dans laquelle des personnes, des biens ou l'environnement sont exposés à un ou plusieurs phénomènes dangereux (cf. 9.2).

Cette définition semble peu adaptée au cadre fixé dans ce document, dans la mesure où, pour ce qui concerne les accidents majeurs sur des sites industriels, l'exposition de éléments vulnérables est quasi automatique dès lors qu'un phénomène dangereux survient, en considérant par exemple l'exposition du personnel ou des autres équipements du site considéré.

Dans ce document, il sera fait mention de situation de danger, répondant à la définition suivante.

Situation de danger

Situation qui, si elle n'est pas maîtrisée, peut conduire à l'exposition de éléments vulnérables à un ou plusieurs phénomènes dangereux.

Evènement Redouté Central

Perte de confinement sur un équipement dangereux ou perte d'intégrité physique d'une substance dangereuse.

Evènement Initiateur

Cause directe d'une perte de confinement ou d'intégrité physique. Une montée en pression, une agression mécanique externe, la corrosion sont le plus souvent des évènements initiateurs.

Evènement Courant

Evènement dont on admet qu'il survienne de façon récurrente dans la vie d'une installation. L'événement courant est connu et géré via la mise en place de moyens spécifiques. Les actions de test, de maintenance ou la fatigue d'équipements sont généralement des évènements courants.

Evènement Indésirable

Dérive ou défaillance sortant du cadre des conditions d'exploitation usuelles définies. Le surremplissage ou un départ d'incendie à proximité d'un équipement dangereux peuvent être des évènements indésirables.

10 SIGLES ET ABREVIATIONS

AMDE : Analyse des Modes de Défaillance et de leurs Effets

AMDEC : Analyse des Modes de Défaillances, de leurs Effets et de leur Criticité.

APR : Analyse Préliminaire des Risques

ARIA : Analyse, Recherche et Information sur les Accidents

BARPI : Bureau d'Analyse des Risques et Pollutions Industrielles

BLEVE : Boiling Liquid Expanding Vapour Explosion

MEDD : Ministère de l'Ecologie et du Développement Durable

UIC : Union des Industries Chimiques

11 BIBLIOGRAPHIE

Les rapport INERIS cités dans cette bibliographie sont tous téléchargeables sur le site Internet de l'INERIS : http://www.ineris.fr

AYRAULT 2005
N. AYRAULT, Evaluation des dispositifs de prévention et de protection utilisés pour réduire les risques d'accidents majeurs (DRA-039) Oméga 10, Evaluation des Barrières Techniques de Sécurité, INERIS, DRA, 2005

AFNOR 2006
FASCICULE DE DOCUMENTATION, "MANAGEMENT DU RISQUE : LIGNES DIRECTRICES POUR L'ESTIMATION DES RISQUES", FD X50-252, AFNOR, SAINT-DENIS, FEVRIER 2006, 23 P.

AICHE
GUIDE LINES FOR HAZARD EVALUATION PROCEDURES
Center for Chemical Process Safety, American Institute of Chemical Engineers (AICHE), Wiley-AIChE; 2eme edition, (April 15, 1992)

ARAMIS 2005
User guide, Projet européen n°EVG1 – CT – 2001 – 00036, disponible sur http://aramis.jrc.it

BEDFORD 2001
T. BEDFORD, R. COOKE, Probabilistic Risk Analysis, Foundation and Methods, Cambridge University Press, 2001

BOUISSOU 2006
C. BOUISSOU, R. FARRET, Programme EAT- DRA-34 - Opération j - Intégration de la dimension probabiliste dans l'analyse des risques, Partie 1 : Principes et pratiques, INERIS, DRA, 2006

CCPS 2001
Layer of Protection Analysis: Simplified Process Risk Assessment (CCPS Concept Book), Center for Chemical Process Safety, 2001.

CPR 18^{E}, 1999
"Purple book", Guidelines for quantitative risk assessment, CPR 18E, Committee for the Prevention of Disasters, Den Haag, 1999.

CPR14E, 1997
"Yellow book", Methods for the Calculation of Physical Effects, CPR 14^{E}, Committee for the Prevention of Disasters, Den Haag, 1997

CPR 16^{e}, 1992
"Green book", Methods for the determination of the possible damages, CPR 16^{E}, Committee for the Prevention of Disasters, Den Haag, 1992

DE DIANOUS 2006
V.De DIANOUS, Programme EAT-DRA-34 - Opération j, Intégration de la dimension probabiliste dans l'analyse des risques – partie 2 : données quantifiées, INERIS, DRA, 2006

DEMISSY 2005
M. DEMISSY, D. CARSON, Formalisation des connaissances et des outils dans le domaine des risques majeurs, rapport Oméga 17, La sécurité des procédés chimiques, INERIS, 2005

GUIDE ISO/CEI 51 : 1999
« ASPECTS LIES A LA SECURITE – PRINCIPES DIRECTEURS POUR LES INCLURE DANS LES NORMES »

GUIDE ISO/CEI 73 : 2002 :
« MANAGEMENT DU RISQUE – VOCABULAIRE – PRINCIPES DIRECTEURS POUR L'UTILISATION DANS LES NORMES »

GRUET P., 2001
Formalisation du savoir et des méthodes dans le domaine des risques majeurs (DRA-35), *Ω-3 : Le risque foudre et les Installations Classées pour la Protection de l'Environnement,* INERIS, DRA, 2001

GOWLAND 2006
R.GOWLAND, The accidental risk assessment methodology for industries (ARAMIS)/layer of protection analysis (LOPA) methodology: A step forward towards convergent practices in risk assessment?, Journal of Hazardous Materials, Volume 130, Issue 3, 31 March 2006, Pages 307-310

HOURTOLOU 2002
D.HOURTOLOU, 2002. ASSURANCE – Assessment of the Uncertainties in Risk ANalysis of Chemical Establishments. E.C. Project ENV4-CT97-0627. Rapport final opération a DRA-07. Ref. INERIS-DHo- 2002-26824

HOURTOLOU 2004
D. Hourtolou, ARAMIS, développement d'une méthode intégrée d'analyse des risques pour la prévention des accidents majeurs, rapport final du BCRD AP 2001 – Conv – 2001 – 01 111 –INERIS DRA-04-35132, 2004

HUBIN 2005
S. HUBIN, T. BALOUIN, Analyse des Risques et Prévention des Accidents Majeurs (DRA-34), Concepts et méthodes de détermination des effets dominos, Aspects méthodologiques et seuils d'effets pour le traitement des effets dominos, INERIS, DRA, 2005

JOLY 2006
C.Joly, Formalisation du savoir et des outils dans le domaine des risques majeurs, Rapport Oméga 9, L'étude de dangers d'une installation classée, INERIS, DRA, 2006

KIRCHSTEIGER 1999
C. Kirchsteiger, On the use of probabilistic and deterministic methods in risk analysis, Journal of Loss Prevention in the Process Industries 12 (1999) 399–419

MICHE 2006
E.MICHE, F.PRATS, S.CHAUMETTE, Formalisation des savoirs et des outils dans le domaine des risques majeurs, Démarche d'évaluation des barrières humaines de sécurité - Ω20, INERIS, DRA, 2006

MONTEAU 1990-1
M.MONTEAU, M. FAVARO, Bilan des méthodes d'analyse a priori des risques,1- des contrôles à l'ergonomie des systèmes, INRS, CDU 614.8-02, cahiers des notes documentaires n°138, 1er trimestre 1990

MONTEAU 1990-2
M.MONTEAU, M. FAVARO, Bilan des méthodes d'analyse a priori des risques, 2- principales méthodes de la sécurité des systèmes, INRS, CDU 168.4 : 614.8, cahiers des notes documentaires n°139, 2eme trimestre 1990

Accessible sur www.inrs.fr

MORTUREUX 2001
Yves MORTUREUX, La sûreté de fonctionnement : méthodes pour maîtriser les risques, Techniques de l'Ingénieur, traité L'entreprise industrielle, AG 4 670, 2001

MORTUREUX 2002
Yves MORTUREUX,Analyse préliminaire de risques, Techniques de l'Ingénieur, traité L'entreprise industrielle, SE4010, 2002

MORTUREUX 2005
Yves MORTUREUX, AMDE (C), Techniques de l'Ingénieur, traité L'entreprise industrielle,SE4040, 2005

MORTUREUX 2003
Yves MORTUREUX, Arbres de défaillance, des causes et d'événement Techniques de l'Ingénieur, traité L'entreprise industrielle,SE4050, 2002

NORME NF X60-500 : 1988 :
« TERMINOLOGIE RELATIVE A LA FIABILITE – MAINTENABILITE – DISPONIBILITE »

NORME CEI 60812: 1985:
« TECHNIQUES D'ANALYSE DE LA FIABILITE DES SYSTEMES – PROCEDURE D'ANALYSE DES MODES DE DEFAILLANCES ET DE LEURS EFFETS (AMDE) »

NORME CEI 61882 : 2001
« ETUDES DE DANGER ET D'EXPLOITABILITE (ETUDES HAZOP) – GUIDE D'APPLICATION »

NORME CEI 61025 : 1990
« ANALYSE PAR ARBRE DE PANNE (APP) »

PERILHON 2003
Pierre PERILHON, MOSAR - Présentation de la méthode Techniques de l'Ingénieur, traité L'entreprise industrielle,SE4060, 2003

PERILHON 2004

Pierre PERILHON, MOSAR - Cas industriel, Techniques de l'Ingénieur, traité L'entreprise industrielle,SE40612004

PERILHON 2003
MOSAR- Présentation de la méthode, Techniques de l'Ingénieur, article SE4060, octobre 2003.

TIXIER 2002
J. Tixier, G. Dusserre, O. Salvi, D. Gaston, Review of 62 risk analysis methodologies of industrial plants, Journal of Loss Prevention in the Process Industries 15 (2002) 291–303

UIC, 1998
LES CAHIERS DE LA SECURITE N°13 - SECURITE DES INSTALLATIONS – METHODOLOGIE DE L'ANALYSE DES RISQUES, UNION DES INDUSTRIES CHIMIQUES, Document Technique DT 54, Mars 1998

VILLEMEUR, 1988
SURETE DE FONCTIONNEMENT DES SYSTEMES INDUSTRIELS
A. VILLEMEUR, Collection de la Direction des Etudes et Recherches d'Electricité de France, n°67, Ed. Eyrolles, 1988

VALLEE 2003
A. VALLEE, O. DOLLADILLE, Analyse des risques et prévention des accidents majeurs (DRA-34), Rapport Partiel d'Opération f, Impact des inondations du Sud-Est (septembre 2002) sur les activités présentant un risque technologique, INERIS, DRA, 2003

VALLEE 2004
Analyse des Risques et Prévention, des Accidents Majeurs, (DRA-34), Rapport Partiel d'Opération f, Guide pour la prise en compte du risque inondation, (Version 2004), INERIS, DRA 2004

12 LISTE DES ANNEXES

Repère	Désignation précise	Nb pages
1	Eléments d'aide pour l'APR	4
2	Eléments d'aide pour l'HAZOP	4
3	Eléments de la méthode ARAMIS	4

ANNEXE 1

ELEMENTS D'AIDE POUR L'ANALYSE PRELIMINAIRE DES RISQUES (APR)

QUESTIONS PRELIMINAIRES A L'ANALYSE PRELIMINAIRE DES RISQUES (PROPOSITIONS)

DESCRIPTION GENERALE

1. Les plans :
   - un plan de localisation au 1/25000 des environs du site (extrait de carte IGN, par exemple) ;
   - un plan d'implantation à l'échelle de 1/ 2.500 des abords de l'installation. Sur ce plan seront indiqués tous bâtiments avec leur affectation, les voies de chemin de fer, les voies publiques, les points d'eau, canaux et cours d'eau ;
   - un plan de masse à l'échelle de 1/200 au minimum indiquant les dispositions de l'installation ainsi que l'affectation des constructions et terrains avoisinants et le tracé des égouts existants.
2. Quelle est la superficie du terrain où sont implantés vos bâtiments ?
3. Quel est le chiffre d'affaire de l'entreprise ?
4. Quel est le nombre de personnes travaillant sur le site ?
5. Quel sont les horaires d'ouverture ?
6. Existe-t-il des lignes électriques au voisinage ou traversant le site ?
7. Existe-t-il des conduites enterrées ?
8. Existe-t-il des lignes ou relais de télécommunication à proximité ?
9. Quelles sont les installations industrielles proches ?
10. Distance des aérodrome, aéroport et éventuellement base militaire les plus proches ?
11. Copie des arrêtés préfectoraux en vigueur sur le site.
12. Etudes diverses (sismique, foudre, ...).

DESCRIPTION DES INSTALLATIONS

1. Schémas et textes décrivant les principales étapes du procédé et les principales opérations réalisées sur le site.
2. Schémas descriptifs (flow sheet) présentant le fonctionnement des principaux équipements.
3. Procédures et consignes d'exploitation, de maintenance.
4. Comment est organisée la formation du personnel ?
5. Procédures et consignes de sécurité.
6. Y a t il un document de synthèse sur les accidents ou incidents déjà observés dans l'entreprise ?
7. Quantité, conditionnement et localisation des matières premières, des produits intermédiaires et des produits finis.
8. Fiches de données de sécurité des matières premières, des produits intermédiaires et des produits finis.
9. Y-a-t'il une unité de réfrigération ? Si oui,
   Nature et quantité du fluide frigorigène
   Puissance des compresseurs
   Description des dispositifs de sécurité
10. Y-a-t'il des unités de combustion (chaudière, four...) ? Si oui, nature des fluides combustibles ?
    Capacité des stockages associés
    Puissance des unités
    Description des dispositifs de sécurité
11. Quelles sont les utilités et leur mode d'approvisionnement : gaz naturel, fuel, air instrument, air comprimé, vapeur, eau chaude, eau froide, autres fluides.
12. Existe-t-il une équipe d'intervention parmi le personnel ?
13. Quels sont les dispositifs de sécurité existants sur le site (alarmes, détection incendie, moyens d'extinction,...) ?
14. Quels sont les équipements de sécurité disponibles sur les installations (soupapes, évents,...) ?
15. Quelles sont les dispositions architecturales de sécurité (murs coupe-feu, toiture incombustibles, exutoires,...) ?
16. Y a-t-il un gardiennage sur le site ?

LISTE DE QUELQUES MOTS-CLE UTILES

DESCRIPTION FONCTIONNELLE

L'objectif est d'identifier les fonctions principales.

Principales fonctions rencontrées sur un site :

- Stockage ;
- Concassage / broyage ;
- Transfert / transport ;
- Chauffage / réchauffage / combustion ;
- Lavage / épuration / filtration ;
- Condensation ;
- Vidange ;
- Décantation ;
- ...

ELEMENTS DANGEREUX

Produits dangereux :

- les matières premières solides, liquides, gazeuses ;
- les produits intermédiaires
- les produits finis ;
- les matières utilisées pour le traitement des gaz ou des fumées ;
- les produits pulvérulents combustibles ;
- les sources d'énergie (gaz naturel, fioul) ;
- ...

Equipements pouvant générer des situations dangereuses

- la zone de réception des matières premières ;
- le stockage de fioul ;
- les broyeurs ;
- les réacteurs ;
- les chaudières et les réseaux de vapeurs ;
- le dispositif de récupération des eaux d'extinction ;
- ...

Situations de danger :

- Accélération ;
- Contamination ;
- Corrosion ;
- Réactions chimiques ;
- Electricité (pannes, chocs, chaleur, action inopportune) ;
- Explosion ;
- Incendie ;
- Variations de température ;
- Fuites ;
- Perte de stabilité des terrains ou des ouvrages ;
- Venues d'eau ou inondations ;
- Accidents mécaniques ;
- ...

Causes :

- Conditions météo extrêmes (pluie, foudre, vent, gel, grêle, verglas, brouillard ...) ;
- Inondations de surface ;
- Séisme ;
- Incendie ;
- Chute d'avions ;
- Accident industriel / Effet mécanique ;
- Malveillance ;
- ...

Conséquences

- Arrêt de l’exploitation ;
- Epandage de produit ;
- Pollution des sols ;
- Pollution ou perturbation des eaux souterraines ;
- Pollution ou perturbation des eaux de surface ;
- Rejet de produit toxique ou inflammable : effets à l’intérieur du site ;
- Rejet de produit toxique ou inflammable : effets à l’extérieur du site ;
- ...

ANNEXE 2

ELEMENTS D'AIDE POUR L'HAZOP

QUESTIONS PRELIMINAIRES A LA REVUE HAZOP DES INSTALLATIONS

Certaines informations nécessaires à la réalisation d'une revue HAZOP doivent être disponibles et fiables au moment de la réunion de travail, soit connues par l'un au moins des participants, soit mentionnées dans les documents de travail. Il s'agit notamment des éléments suivants :

- s'il s'agit d'un projet, le cahier des charges et la proposition technique de l'installation (version à jour)
- les procédures d'exploitation
- les consignes de sécurité (fiches POI ou autres)
- un ou plusieurs schémas de fonctionnement de type PID (version à jour pour un projet ou conforme à l'existant) mentionnant :
  - les circuits des différents produits mis en œuvre,
  - les équipements et leurs caractéristiques de fonctionnement et de design (pression maximale de service - diamètre - température - capacité),
  - la position des piquages
  - les utilités (gaz, air comprimé, azote, eau, électricité,...)
  - les éventuels circuits de collecte et les caractéristiques de l'évacuation (hauteur, débit, diamètre)
  - les organes de sécurité (organes de mesure, capteurs, sécurités, alarmes, témoins de fonctionnement, soupapes, évents ...) et leur caractéristiques (seuils ou niveaux de déclenchement, action manuelle ou automatique, alimentation électrique ou pneumatique, redondances ...)
  - les actions de sécurité (automatiques ou manuelles) entraînées par les alarmes ou les détections,
  - les boucles, les régulations, les interactions permettant, dans le cadre de la conduite des installations, de contrôler les paramètres d'exploitation (température, pression, niveau)
  - la position des bâtiments, des parois
  - la nomenclature associée
- le plan du site
- une description des équipements spécifiques (condenseurs, échangeurs thermiques, compresseurs, pompes, capacités et réservoirs, réacteurs ...)
- les fiches de données de sécurité et les courbes pression-température des fluides,
- si possible, photographies du site et de l'installation,
- les dispositions architecturales de sécurité (murs coupe-feu, toiture incombustible, exutoires, parties soufflables ...),
- la table de schedule (dimensionnement des canalisations)

LISTE DE QUELQUES MOTS-CLE UTILES

Hypothèses de dérives	*Causes*	*Conséquences*
Débit Débit trop élevé	Emballement de pompe - Défaillance de compresseur, de ventilateur, de trémie d'alimentation - mise en parallèle d'une deuxième pompe - Chute de pression au refoulement - Mise en pression de l'aspiration - Introduction d'un autre fluide par fuite à travers une paroi - Défaillance du contrôle - Défaut sur une soupape de sécurité, un disque de rupture, une position de vanne automatique - Erreur opérateur.	Débordement aval - Erosion - Corrosion - Surpression - Mélange - Inversion d'écoulement - Modification des proportions, de température - Passage en zone d'explosivité - Changement de phase - Modification des conditions de réaction, de séparation.
Débit trop faible ou absence de débit	Défaillance de pompe, de compresseur, de ventilateur, de trémie d'alimentation, de transporteur - Défaut d'accouplement - Formation de dépôt dans tuyauterie - Présence de corps étrangers ou sédiments - Fuite vers un autre fluide à travers une paroi - Inversion - Défaut sur une soupape de sûreté, un disque de rupture, une vanne automatique, une purge - Cavitation - Défaillance du contrôle - Manque de produit - Joint plein laissé en place - Formation d'une poche de gaz - Erreur opérateur.	Dépôt en cas de suspension - Température produit - Modification des conditions de réaction, de séparation - Mélange - Inversion d'écoulement par introduction d'un fluide d'un autre réseau - Echauffement de pompe - Modification des proportions - Débordement amont - Changement de phase - Assèchement de garde hydraulique - Passage en zone d'explosivité.
Pression Pression haute	Mise en équilibre avec température extérieure en été - Apport excessif de chaleur (vapeur, chauffage électrique ...) - Refroidissement insuffisant - Emballement réaction ou arrêt réaction - Confinement - Dilatation - Défaillance du contrôle - Mélange - Fuite de l'appareillage - Inversion d'écoulement - Absence de dégazage - Vanne fermée ou joint plein laissé en place - Bouchage par corps étrangers ou sédiments - Variation pression, gel du fluide - Erreur opérateur.	Modification des propriétés physiques et chimiques - Condensation avec corrosion - Explosion appareillage - Emission produit toxique ou inflammable par organe limitateur de pression - Mélange - Fuite - Inversion d'écoulement.

Hypothèses de dérives	*Causes*	*Conséquences*
Pression basse	Mise en équilibre avec température extérieure en hiver - Refroidissement exagéré (gel ou pluie) - Fuite de l'appareillage - Arrêt réaction - Absorption - Position vanne - Bouchage par corps étrangers ou sédiments - Soutirage exagéré - Mise sous vide - Inhibition - Variation pression - Erreur opérateur.	Modification des propriétés physiques et chimiques - Corrosion - Evaporation avec abaissement de température et gel possible - Flash - Moussage - Implosion - Entrée d'air ou d'humidité extérieure - Pollution par un autre réseau à plus haute pression - Extinction flamme.
Température Température haute	Mise en équilibre avec température extérieure en été - Emballement réaction - Apport excessif de chaleur - Réaction parasite (introduction produit ou changement conditions) - Elimination insuffisante de chaleur - Défaillance du contrôle - Feu extérieur - Corrosion - Variation de pression - Erreur opérateur.	Modification des propriétés physiques - Evaporation et modification mélange réactionnel - Réaction parasite - Elévation de pression - Cavitation - Perte des propriétés mécaniques des matériaux de l'appareillage - Dilatation liquide confiné - Instabilité produits - Inflammation spontanée.
Température basse	Mise en équilibre avec température basse en hiver - Refroidissement excessif - Evaporation brutale par suite d'une fuite ou d'une détente brutale - Défaillance du contrôle - Erreur opérateur.	Modification des propriétés physiques, mécaniques (fragilisation) - Condensation avec corrosion - Cristallisation - Sédimentation - Bouchage - Gel.
Concentrations ou compositions chimiques anormales	Variation de débit, de température, de pression - Défaut du contrôle - Evaporation ou condensation anormale - Fuite - Introduction accidentelle - Défaut sur système d'agitation - Erreur opérateur.	Changement des conditions réactionnelles - Concentration anormale - Réactivité anormale - Réaction parasite - Emballement - Corrosion.
Contamination	Entrée d'air, d'eau, de vapeur, de fluide réfrigérant ou caloporteur, de fuel, de lubrifiant, de fluide provenant de l'appareillage de contrôle et de régulation - Introduction de produits de corrosion - Retour de produits - Fuite de l'appareillage - Entraînement solide, liquide ou gazeux d'une opération à l'autre - Défaut de nettoyage; de graissage - Confusion matières premières - Confusion circuits - Erreur opérateur.	Corrosion - Réaction parasite ou dangereuse - Sous-produit anormal ou dangereux - Inhibition - Emballement de la réaction.

Hypothèses de dérives	*Causes*	*Conséquences*
Agitation	Défaillance de l'agitation - Fuite de garniture - Corrosion - Niveau anormal - Viscosité anormale - Erreur opérateur.	Erosion - Sédimentation - Décantation - Phase anormale - Vibrations - Fuite - Contamination
Niveau	Fuite - Bouchage - Variation de débit, de température, de pression - Moussage, condensation - Evaporation - Densité anormale - Turbulence - Erreur opérateur.	Cavitation - Débordement ou vidange - Pression élevé ou excessive - Défaillance d'agitation - Modification échange thermique - Charge excessive sur supports.
Incompabilité	Mélange possible dans circuits par fuite d'appareillage - Ecoulement accidentel - Retour - Débordement - Réaction entre effluents gazeux, liquides, solides - Distance aux feux nus - Changement de composition - Erreur opérateur	Réaction parasite ou dangereuse - Inflammation - Retour de flamme - Explosion - Echauffement - Corrosion
Pannes utilités	Manque d'eau, d'énergie électrique, d'air, d'instrument, d'azote, de vapeur, de vide	Analyser les dérives résultant de la panne de chacun des éléments, soit isolés, soit couplés, soit pris en totalité, et examiner l'ensemble des conséquences possibles à l'aide en particulier de la présente liste.
Electricité statique	Perte ou défaut de la continuité électrique sur les mises à la terre - Foudre.	Etincelle et source d'ignition - Décharge électrique sur le personnel.
NOTA BENE : Tenir compte de l'influence aggravante des surcharges climatiques (vent maximum, neige, etc) dans les conséquences possibles de certaines hypothèses de dérive (niveau, perte des propriétés mécaniques des matériaux de construction, fragilisation, etc..).		

ANNEXE 3

TABLEAUX GUIDES DE LA METHODE ARAMIS

Principaux tableaux utilisés dans la méthode ARAMIS pour servir de base au développement des nœuds papillons

N	Type d'équipements	Définition
	Unités de stockage	
EQ1	Stockage en vrac solide	Stockage de substances sous forme solide (poudres ou billes). Les substances y sont stockées en vrac ou en siols (les stockages en sous forme de sacs ne font pas partie de cette catégorie)
EQ2	Stockage de solides en petits contenants	Stockage de solides sous forme de petits contenants ou réservoirs de capacité inférieure à ≅ 1 m³.
EQ3	Stockage de liquides en petits contenants	Stockage de liquides sous forme de petits contenants ou réservoirs de capacité inférieure à ≅ 1 m³.
EQ4	Stockage sous pression	Réservoirs de stockage à température ambiante et à une pression supérieure à 1 bar. La pression est celle du fluide à saturation ou peut être celle d'un gaz inerte. La substance peut être un gaz liquifié sous pression (deux phases en équilibre) ou un gaz sous pression (une phase gaz).
EQ5	Stockage à pression supérieure à la pression de saturation	Réservoirs de stockage fonctionnant à température ambiante à une pression supérieure à 1 bar. La pression est exercée par un gaz inerte par exemple et maintient le stockage à une pression supérieure à sa pression de saturation. Le stockage contient une substance en phase liquide.
EQ6	Stockage atmosphérique	Stockage à pression et température ambiante, contenant un liquide. La substance peut être un gaz liquifié sous pression (deux phases en équilibre) ou un gaz sous pression (une phase gaz).
EQ7	Stockage cryogénique	Stockage fonctionnant à pression atmosphérique (ou moins) et basse température La substance est un gaz liquéfié réfrigéré.
	Unités de (dé)chargement	
EQ8	Equipement de transport sous pression	Equipement de transport à température ambiante et pression supérieure à 1 bar (pression exercé par la substance elle-même).
EQ9	Equipement de transport atmosphérique	Equipement de transport à pression et température ambiante comportant une substance liquide.
	Réseaux de canalisations	
EQ10	Canalisation	Canalisations entre deux unités, les canalisations dans l'unité sont liées aux divers équipements
	Equipements process	
EQ11	Stockage intermédiaire dans le procédé	Equipement de stockage dans l'unité (peut être stockage sous pression, cryogénique..)
EQ12	Equipement avec réactions chimiques	Equipement avec réaction chimique, par exemple réacteur.
EQ13	Equipement séparation physique ou chimique	Equipement séparation physique ou chimique (par exemple colonne de distillation, filtres, sécheurs..).
EQ14	Equipement de production et fourniture d'énergie	Equipement de production et fourniture d'énergie (par exemple fours, chaudières..)
EQ15	Equipement de conditionnement	Equipement dédiés au packaging des substances (exclut les packages eux-mêmes)
EQ16	Autres équipements	Autres équipements (pompes..)

Tableau 17 : Typologie d'équipements considérée dans MIMAH

Evénements redoutés critiques		*Commentaires*
ERC1	Décomposition	Cet événement critique ne concerne que les substances solides . Il correspond à un changement d'état physique de la substance par apport d'énergie/chaleur ou par réaction avec une substance chimique incompatible. La décomposition de la substance conduit à une émission de gaz toxiques ou à l'explosion retardée des gaz inflammables formés (la réaction n'est pas spontanée mais peut être violente). Cet ERC ne concerne que les stockages vrac de produits solides.
ERC2	Explosion	Cet ERC ne concerne que les stockages vrac de produits solides **explosifs** (phrases R2, R3, R6..). Il correspond à un changement d'état physique de la substance par apport d'énergie/chaleur ou par réaction avec une substance chimique incompatible. Le changement d'état entraine une combustion solide avec effets de surpression (ou explosion) due à une réaction violente et spontanée. Dans le cas d'un solide stocké dans un récipient fermé, l'explosion est considérée comme une cause de surpression interne pouvant conduire à une perte de confinement (rupture catastrophique ou brèche).
ERC3	Mise en mouvement (entrainement par l'air)	Cet ERC est réservé aux poussières et pulvérulents exposés à l'atmosphère (stockage ouvert ou convoyeurs..). L'événement se produit par déplacement d'air (par exemple trop forte ventilation).
ERC4	Mise en mouvement (entrainement par un liquide)	Cet ERC est réservé aux poussières et pulvérulents exposés à l'atmosphère (stockage ouvert ou convoyeurs..). L'événement se produit par déplacement de liquide (par exemple inondation ou débordement d'un liquide d'un autre équipement).
ERC5	Inflammation – départ de feu	Cet ERC correspond à une réaction entre un produit oxidant et un produit inflammable ou combustible ou à une décomposition d'un péroxyde organique conduisant à un feu. Cet ERC concerne les substances dont une perte d'intégrité physique (décomposition, contamination) conduit à un incendie.Cet ERC peut être associé aux substances pyrotechniques.
ERC6	Brèche en phase gaz	Cet ERC correspond à un trou de diamètre donné dans la paroi en phase gaz d'un équipement, conduisant à un rejet continu. Cet ERC s'applique aussi aux équipements contenant un solide en suspension dans une phase gazeuse.
ERC7	Brèche en phase liquide	Cet ERC correspond à un trou de diamètre donné dans la paroi en phase liquide d'un équipement, conduisant à un rejet continu.
ERC8	Fuite sur canalisation en phase liquide	Cet ERC correspond à un trou de diamètre égal à un certain pourcentage du diamètre nominal d'une canalisation véhiculant un liquide. L'ERC peut être une ouverture « fonctionnelle » sur la canalisation : fuites de joints sur pompes, sur vannes, sur bouchons pleins, etc.
ERC9	Fuite sur canalisation en phase gaz	Cet ERC correspond à un trou de diamètre égal à un certain pourcentage du diamètre nominal d'une canalisation véhiculant un gaz. L'ERC peut être une ouverture « fonctionnelle » sur la canalisation : fuites de joints sur pompes, sur vannes, sur bouchons pleins, etc. Cet ERC s'applique aussi aux canalisations véhiculant un solide en suspension dans une phase gazeuse.
ERC10	Rupture catastrophique	La rupture catastrophique correspond à la perte complète de l'équipement conduisant à un rejet complet et instantané de la substance. Le BLEVE est aussi considéré comme une rupture catastrophique particulière. Dans certains cas, la rupture catastrophique peut conduire à l'éjection de missiles et une onde de surpression.
ERC11	Effondrement de réservoir	L'effondrement de réservoir correspond à la perte complète de l'équipement conduisant à un rejet complet et instantané de la substance. L'ERC est dû à une réduction de pression du réservoir, conduisant à son effondrement par action de la ression atmosphérique. Cet ERC ne conduit pas à l'éjection de missiles ou la production d'une onde de surpression.
ERC12	Effondrement du toit de réservoir	L'effondrement du toit peut être dû à une réduction de la pression interne conduisant à l'effondrement du toit mobile sous l'effet de la pression atmosphérique. Cas spécifique des stockages atmosphériques aériens.

Tableau 18 : Typologie des événements critiques considérée dans MIMAH

	Barrière	Exemples	Détection	Diagnostic / Activation	Action
1	*Permanente – passive*	Peinture anti-corrosion, support de cuve, écran flottant, …	-	-	Matériel
2	*Permanente – passive*	Rétention, mur coupe-feu, disque de rupture, …	-	-	Matériel
3	*Temporaire – passive* Mis en place (ou retirée) par une personne	Barrières de protection d'une zone de travaux, casques/gants, inhibiteur dans une solution, …	-	-	Matériel
4	*Permanente – active*	Protection anti-corrosion catalytique, système de chauffage, refroidissement, ventilation, évent d'explosion, système d'inertage, …	-	(peut nécessiter l'activation par un opérateur)	Matériel
5	*Active – matériel fonctionnant à la demande et réutilisable*	Soupape de sécurité, installation de sprincklage, …	Matériel	Matériel	Matériel
6	*Active – automatique*	Système de mise en sécurité automatique	Matériel	Matériel / logiciel	Matériel
7	*Active – manuelle* L'action humaine est déclenchée par un système de détection	Arrêt d'urgence, ajustement de paramètre sur alarme de production, évacuation ou appel service de secours sur alarme, …	Matériel	Humain	Humain / système de régulation
8	*Active – avertissement passif* L'action humaine est conditionnée par un avertissement passif	Interdiction de fumer, panneau d'indication de danger (travaux, circulation…)	Matériel	Humain	Humain
9	*Active – assistée* Un logiciel présente un diagnostic à un opérateur	Utilisation d'un système expert	Matériel	Logiciel – humain	Humain / système de régulation
10	*Active – procédure* Observation des conditions locales par un opérateur	Procédure de démarrage ou d'installation, étalonnage d'un appareil, opération de dépotage, …	Humain	Humain	Humain / système de régulation
11	*Active – situations d'urgence* Réponse humaine improvisée suite à l'observation des conditions locales	Réponse à une urgence non prévue, combat du feu, …	Humain	Humain	Humain / système de régulation

Tableau 19 : Classification des barrières préalablement à l'audit du système de management

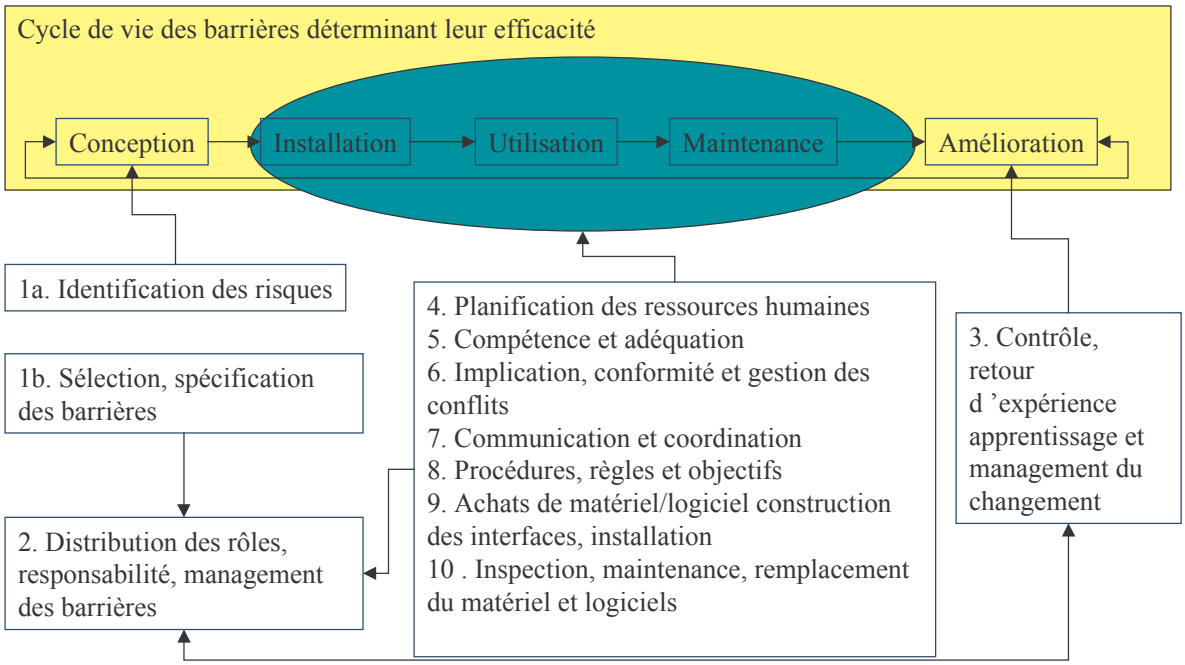


Figure 18 : Cycle de vie des barrières de sécurité et processus du système de management concernés par l'audit du système de management.

INERIS

Institut national de l'environnement industriel et des risques

Parc technologique Alata
BP 2 - 60550 Verneuil-en-Halatte

Tél. : +33 (0)3 44 55 66 77 - Fax : +33 (0)3 44 55 66 99

E-mail : ineris@ineris.fr - **Internet :** http://www.ineris.fr