# Proposition d'une méthode « générique » d'analyse de risques

## Evolution d'une approche analytique déterministe et probabiliste vers une vision systémique, sociétale et réglementaire

**Depuis une trentaine d'années la problématique des risques industriels a beaucoup évolué. Nous sommes passés d'une démarche déterministe et probabiliste, essentiellement centrée sur les procédés industriels, à une approche systémique qui souligne les points de vue quelquefois contradictoires des différents acteurs. L'importance du facteur humain et de la composante «gestion des risques» sont aujourd'hui reconnus. Les dysfonctionnements observés mettant en cause ces aspects sont de plus en plus nombreux et constituent les domaines où des progrès sensibles sont attendus.**

par **Pierre Perilhon,**
*ingénieur ENSAM*
et **Henry Londiche,**
*ingénieur civil des mines,*
*Ecole des mines de Saint-Etienne*

Les recherches récentes mettent en valeur les aspects organisationnels et l'acceptation sociale du risque par la société. Il apparaît nécessaire aujourd'hui de considérer les évolutions récentes et de proposer, pour aborder la prise en compte et la gestion des risques dans tout projet de conception ou de diagnostic, une méthode « générique » d'analyse de risques qui puisse s'adapter aux diverses situations rencontrées. Une telle méthode, qui sera décrite ici en vue d'une application industrielle, pourra également être mise en œuvre pour des activités liées au développement urbain, à l'aménagement du territoire ou à l'organisation de services ou de réseaux.

### Fondements d'une méthode « générique » d'analyse des risques

On appelle, dans la suite, méthode « générique » d'analyse de risques une démarche définissant le parcours général des différentes séquences (et de leurs relations) nécessaires pour analyser les risques d'une installation (et définir leur prévention). Cette installation, (usine, service, aménagement, etc.) peut être préexistante ou à l'état de projet (phase de conception). Dès lors, «analyser les risques» consiste, notamment en milieu industriel, à identifier, évaluer, maîtriser, manager et gérer les dysfonctionnements des systèmes.

Une première modélisation simple d'une installation industrielle permet de faire apparaître la problématique générale de cette analyse. On considère fondamentalement qu'une installation est un système ouvert sur son environnement (voir la figure 1). Le schéma montre immédiatement un champ de complexité caractérisé par la multiplicité des relations (entre sous systèmes matériels M1, M2,… sous-systèmes vivants O1, O2,…et avec l'environnement) et par le caractère incertain de beaucoup d'entre elles, particulièrement celles qui sont issues des systèmes vivants (les opérateurs O1, O2, O3, …).

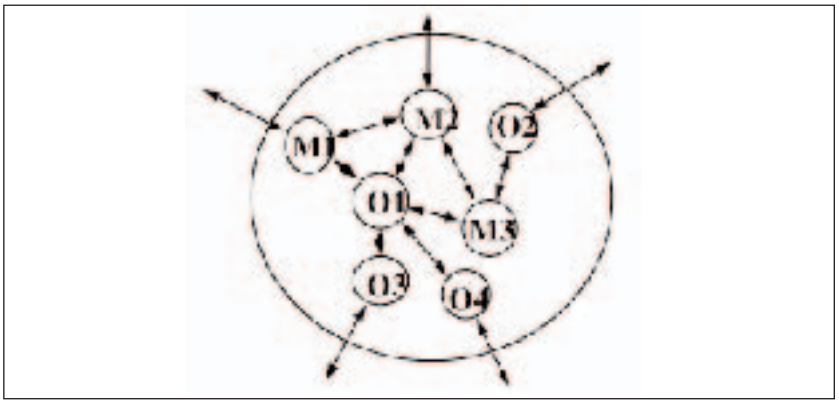


*Figure 1 : Modèle d'un système ouvert (installation industrielle ou autre)*

Pour entrer dans ce champ de complexité, il est nécessaire d'adopter une démarche systémique et de faire appel à la modélisation systémique. La première étape de l'analyse des risques consiste donc à décomposer l'installation en systèmes et sous-systèmes. On fait appel ici à une vision en « zoom », fonction de la nature et de l'importance de l'installation.

Pour une installation isolée, on distinguera le système I à analyser (*système 1*), les opérateurs mis sous forme d'un système unique OP dans un premier temps (*système 2*) et l'environnement mis aussi sous forme d'un système unique E (*système 3*). Après avoir défini le système à étudier 1, on le décompose en sous-systèmes: 1-1 à 1-4, par exemple de manière fonctionnelle (figure 2). La règle générale est de ne pas dépasser une dizaine de sous-systèmes, ce qui détermine les échelles du « zoom » c'est-à-dire la manière dont sera décomposé le contexte. On étudie ensuite les interactions entre les systèmes 2 et 3 et avec les sous-systèmes 1-1 à 1-4.

Les dysfonctionnements peuvent dès lors provenir des matériels, de leurs liaisons, de leurs proximités, des opérateurs et des liaisons entre eux et avec les matériels, de l'environnement et de ses interactions avec les opérateurs et les matériels.

Dans le cas où on se trouve dans une situation plus complexe, par exemple un ensemble d'établissements, on décomposera chaque établissement en ateliers constituant une installation isolée I. On peut alors étudier les interactions au sein de chaque atelier, puis entre ateliers et enfin entre établissements (mise en évidence de scénarios dominos) (Cf. figure 2).

Analyser les risques d'une installation consiste alors essentiellement à identifier les dysfonctionnements de nature technique (défaillance matérielle) d'une part , et de nature opératoire (défaillance opérationnelle, relationnelle ou organisationnelle) d'autre part, dont l'enchaînement (ou la conjonction) peut conduire à des effets non souhaités sur quatre types de cibles possibles. Ces cibles sont représentées par les individus, les populations, les écosystèmes et les systèmes matériels ou symboliques.

## Un dispositif formel et opératoire

La méthode élaborée compte deux modules : le premier module (module A) permet de réaliser une analyse des risques principaux, le second (module B), une analyse détaillée de l'installation ; il met notamment en œuvre les outils de la sûreté de fonctionnement pour la recherche des dysfonctionnements techniques des machines et appareils.

Le «module A» vise à identifier les dangers, les scénarios de risques majeurs (en considérant que la proximité des sources de dangers entraîne leur possibilité d'interaction). La méthode conduit à établir des objectifs pour hiérarchiser les scénarios et à identifier les moyens de prévention et de protection permettant de neutraliser les scénarios.

L'identification des sources de danger se fait en utilisant un modèle général développé par ailleurs et appelé MADS (Méthodologie d'analyse de dysfonctionnement des systèmes) représenté par la figure 3.

Ce modèle considère qu'un événement non souhaité (ENS) est un enchaînement d'événements (initiateurs, principal, renforçateurs) issus d'un système source de danger, et du champ environnant, ayant un impact sur un des quatre systèmes cibles de danger. C'est un modèle de représentation qui permet

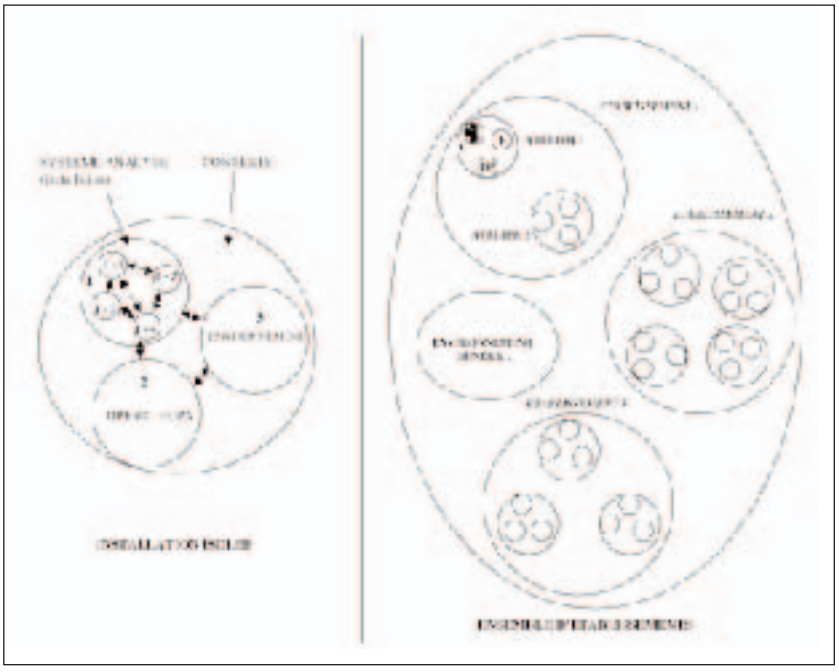

***Figure 2 : Décomposition d'une installation isolée et d'un ensemble d'établissements***

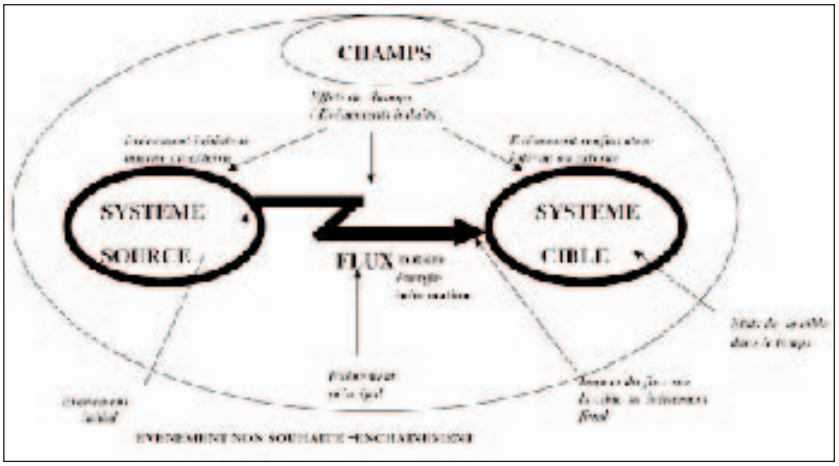


***Figure 3 : MADS comme modèle de l'événement non souhaité***

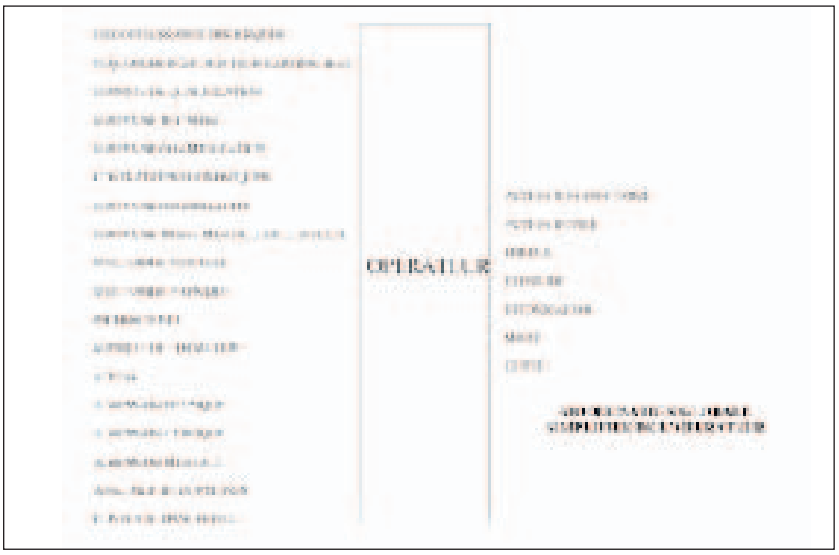

*Figure 4 : Boîte noire représentant le système opérateur*

d'identifier en quoi un système peut être source de danger.

Pour rendre systématique cette identification, la méthode propose d'établir une typologie des systèmes sources de danger en milieu industriel en s'appuyant sur une grille générale. Cette grille répertorie les sources d'origine mécanique (systèmes sous pression, sous contraintes mécaniques, en mouvement etc.), chimique (réactions chimiques, sources d'explosions, de toxicité et d'agressivité etc.), électrique (courant continu ou alternatif, électricité statique, condensateurs etc.), biologique (micro-organismes et prions, modifications génétiques, animaux, opérateur humain etc.), économique (finances, migrations, conflits etc.). On distingue aussi les sources de danger liées au développement d'incendie (allumage, cloisonnements, matériaux etc.), au rayonnement (ionisant, UV, IR, éclairage etc.) et à l'environnement (transports, installations industrielles, phénomènes climatiques et géologiques etc.).

Dans une première étape, l'identification conduit à analyser pas à pas chaque système à étudier au travers de cette grille et à repérer en quoi chaque sous-système peut être une source de danger. Le résultat est consigné dans la première colonne d'un tableau, selon la phase de vie considérée. On identifie ainsi, de manière systématique, tous les «systèmes sources de danger» figurant dans la grille et présents dans le système étudié.

Dans une deuxième étape, le tableau est rempli ligne par ligne : pour chaque «système source de danger» qui a été identifié, l'analyse consiste à rechercher quels sont les événements initiaux (liés au contenant ou à la «structure» et au contenu ou au «facteur de danger») que peut générer ce système par le fait qu'il est source du danger identifié. On recherche ensuite quels sont les événements initiateurs (externes et internes) qui peuvent être à l'origine de ces événements initiaux et enfin on détermine quels sont les événements principaux que généreront les événements initiaux identifiés, en prenant en compte les événements renforçateurs éventuels.

Dans une troisième étape, chaque système ainsi analysé est alors modélisé sous forme d'une boîte noire avec en entrée les événements initiateurs et en sortie les événements principaux. A titre d'exemple, on a modélisé de manière simple un opérateur, ce qui conduit à la boîte noire représentée par la figure 4.

Ceci n'évacue pas du tout la nécessité de traiter par la suite l'opérateur d'une toute autre manière, car c'est un système complexe. Dans un premier temps, à ce niveau de l'analyse, cette simplification, qui peut paraître outrancière, aide à trouver les scénarios majeurs. L'identification des scénarios de danger s'obtient en imaginant des liens sur les boîtes selon les schémas suivants (figure 5).

Pour une boîte noire isolée, il est possible de créer des liaisons directes par feed-back en combinant les sorties des lignes du tableau avec les entrées d'autres lignes, ce qui conduit à élaborer des scénarios courts ou d'autodestruction pour chaque système. En considérant les sorties d'une boîte noire comme les entrées potentielles d'autres boîtes, on construit alors des scénarios longs qui font intervenir les interactions entre systèmes (effet domino ou séquences complexes).

Bien que fastidieux, ce travail permet avec de l'expérience et un peu de temps de découvrir des scénarios plausibles auxquels on n'avait pas songé ou qui ne se sont encore jamais produits.

Cette genèse de scénarios conduit à la structuration d'arbres logiques dont

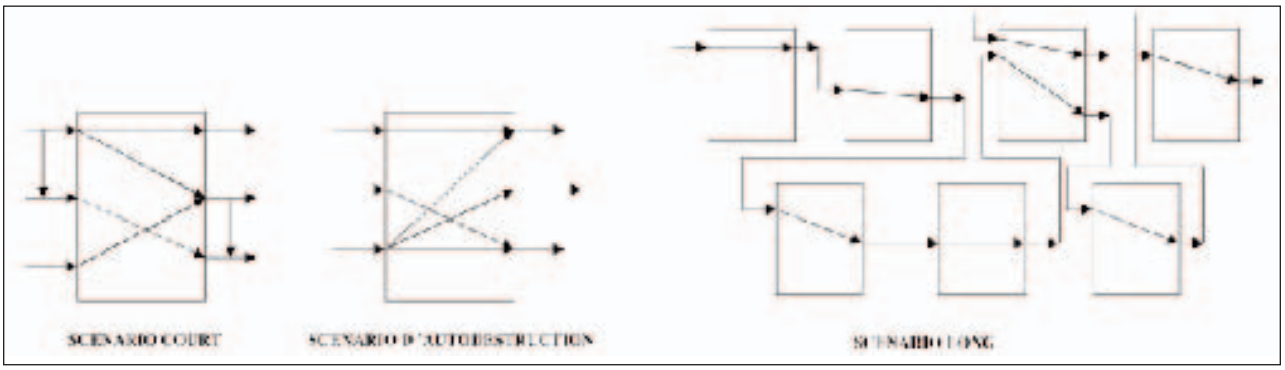

*Figure 5 : Méthode d'identification des scénarios de dangers.*

l'événement final est un accident majeur. Un tel arbre est une sorte de pré-arbre de défaillances qui facilite la construction de l'arbre usuel de défaillances. C'est un peu son squelette.
En milieu industriel, les événements majeurs sont essentiellement des explosions, des incendies, des libérations de gaz toxiques, des pollutions de l'air ou des eaux ou des sols. Il est aussi possible de construire des scénarios en les centrant sur des risques professionnels.
Il faut noter que la construction du tableau se fait sans tenir compte des moyens de prévention, ce qui permettra par la suite de voir comment évolue la sécurité quand on introduit ces moyens et de porter un jugement sur ceux existant (situation de diagnostic) ou proposés (situation de conception.). D'autre part, il n'est pas obligatoire de mettre en œuvre cette méthode pour générer des scénarios bien que cette façon de faire soit assez démonstrative. Le retour d'expérience peut aussi suggérer des scénarios. Une autre méthode consiste à construire les différents états d'un système source de danger dans le temps, états liés à l'évolution de ses paramètres. Cette approche est en cours de développement. De plus, au lieu d'utiliser le modèle MADS, on pourrait très bien faire une AMDEC, outil pragmatique par ailleurs normalisé. Un tableau d'AMDEC est un condensé d'analyse complète puisqu'il intègre les moyens de prévention et une première estimation probabiliste. On voit cependant l'intérêt du modèle MADS, à la fois pour bien faire apparaître ce qui peut survenir au niveau du système source de danger et ce que cela va entraîner sur les autres systèmes. Le modèle MADS peut être vu aussi comme une théorisation de l'AMDEC.
Il est également possible dès cette étape, qui correspond au module A, de construire des arbres de défaillances à partir des arbres logiques car suffisamment d'informations ont été acquises pour le faire. On peut identifier aussi les éléments importants pour la sécurité (EIS) qui feront l'objet de mesures particulières. Ce sont des éléments (matériels, procédures) critiques dans la genèse d'un scénario. Enfin, remarque importante, la prise en compte de l'environnement et sa modélisation sous

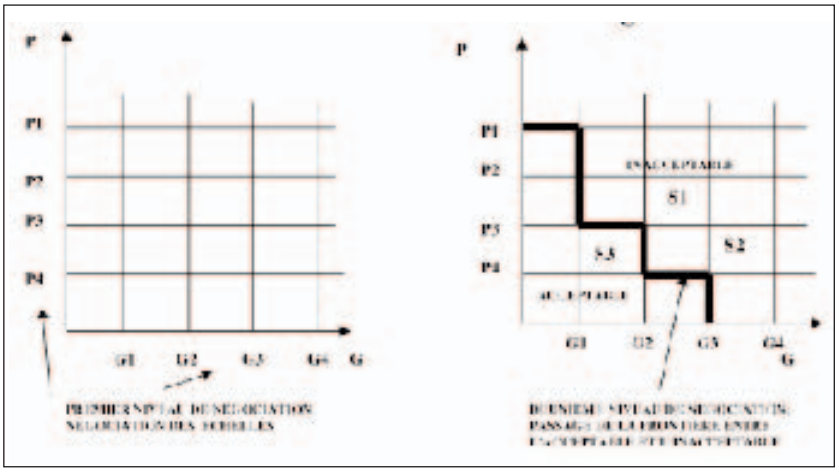


***Figure 6 : Négociation de grilles gravité-probabilité et situation de trois scénarios S1, S2, S3***

forme de boîte noire se fait aussi par rapport à la typologie de référence décrite dans la grille.

## Objectifs quantifiés

La quantification des risques, étape suivante de l'analyse, se base sur les scénarios qui ont été construits. L'évaluation de ces scénarios permet de déterminer leur gravité par rapport aux cibles concernées. Pour ceux qui peuvent faire l'objet de calculs, de nombreux logiciels existent (explosions, incendies, dispersion de gaz…) Pour les autres il est toujours possible d'en effectuer une évaluation qualitative avec des jugements d'experts auxquels il est très fructueux d'adjoindre des opérateurs ou des cibles potentielles.
Les objectifs sont fixés *a priori*, soit de manière réglementaire, soit de manière volontaire, par un responsable, un groupe de responsables, une autorité ou une structure industrielle. Il suffit alors de situer les scénarios évalués par rapport à ces objectifs pour les hiérarchiser.
Si aucun objectif n'a été fixé a priori, on peut construire, pour classer les scénarios, des grilles gravité X probabilités. Cette construction peut être faite par des experts ou des décideurs mais elle prend tout son sens si elle se fait sous forme de négociation entre les acteurs concernés et, notamment, avec les victimes potentielles. Apparaît alors un consensus.
Une fois les grilles établies, les scénarios sont situés dans celles-ci. Leur évaluation en probabilité est le plus souvent qualitative, sauf s'il a été possible de construire des arbres de défaillance quantifiés, ce qui est rare. Notons, à ce stade, qu'il est parfois difficile d'utiliser une seule grille. En effet les conséquences d'un scénario donné sur les différentes cibles (individus, population environnante, matériel et écosystème) ne sont pas d'un même niveau de gravité et ne sont pas toujours évaluables sur une échelle commune. Concaténer les effets d'un même scénario sur les différentes cibles serait envisageable en utilisant des techniques d'agrégation multicritères. Cela demeure encore un champ ouvert qui reste du domaine de la recherche car il semble bien difficile d'accorder des points de vue parfois contradictoires : ceci devient un problème de gouvernance (figure 6).
Une autre manière de se fixer des objectifs consiste à fixer le domaine de fonctionnement autorisé de l'installation à partir des scénarios d'accidents. Cela se traduit par la fixation de puissances maximales, ou par la fixation de quantités maximales mises en œuvre ou stockées ou encore, par la fixation de paramètres (températures, débits…).
La phase suivante concerne la définition et la qualification des moyens de prévention et de protection nécessaires pour éviter les scénarios d'accidents majeurs et ceci, dans toutes les phases de vie de l'installation notamment en conception et en exploitation. On appelle ces moyens des barrières, dont on peut dresser une typologie. Ces dernières peuvent être physiques (techniques ou technologiques) symbolisées

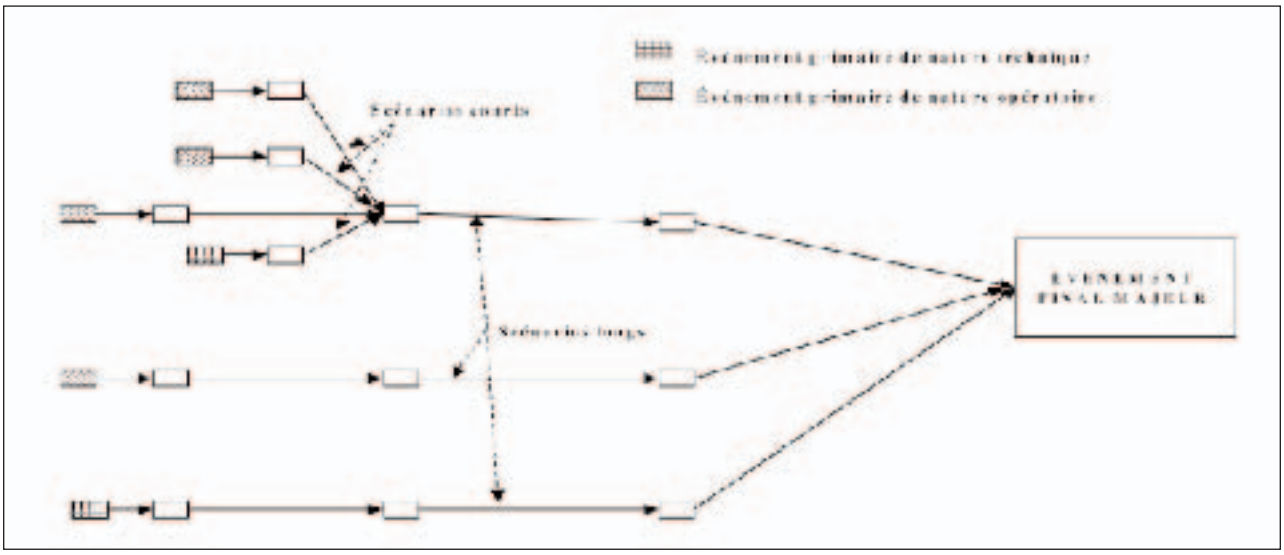

*Figure 7 : Arbre logique avec ses événements primaires*

BT (barrières techniques), virtuelles (symboliques ou normatives), procédurales (opératoires), passives ou actives, symbolisées BU (barrières d'utilisation). La méthode conduit à la mise en place d'une stratégie de défense en profondeur dans la mesure où l'étape de qualification permet de s'assurer que ces barrières restent pérennes en toutes circonstances ou qu'il est possible de leur substituer d'autres moyens si elles sont non opérantes. Ceci suppose des moyens de surveillance, de contrôle par la qualité et l'assurance qualité.

Pour réaliser cette phase, on construit d'abord des tableaux dans lesquels on introduit les scénarios et leurs événements ainsi que des informations comme les mesures spécifiques aux EIS (éléments importants pour la sécurité), les contrôles et vérifications techniques, les protections individuelles etc. On établit ensuite pour les barrières envisagées un tableau de qualification dans le temps décrivant les procédures de contrôle, de maintenance, de vérification de non-introduction de danger nouveau ou de nuisance. On précise aussi l'organisation propre, les consignations spécifiques, le balisage et la formation particulière des opérateurs liés à l'implantation des barrières.

L'opération suivante consiste à vérifier si tous les scénarios précédemment situés dans les grilles gravité X probabilité «restent ou migrent», une fois les barrières définies, dans la zone d'acceptabilité de ces grilles. Il n'y a pas de critères simples permettant de refaire ce classement. La solution la plus efficace consiste en une nouvelle négociation avec les experts et si possible les acteurs concernés. Les scénarios restant dans l'inacceptable constituent des risques résiduels.

Toute cette approche du module A est essentiellement déterministe. Elle permet d'identifier les principaux événements qui s'articulent dans des scénarios d'accidents et convergent vers les événements majeurs. Il est remarquable que dans les arbres logiques ainsi construits, les événements primaires sont de deux natures : des événements de nature technique (ou dysfonctionnements techniques) et des événements de nature opératoire qui impliquent les humains présents dans l'installation et à tous niveaux (appelés globalement opérateurs).

Le module B correspond à un second niveau d'analyse où pour rechercher les dysfonctionnements de nature technique on construit des AMDEC sur les appareillages identifiés comme étant à l'origine de ces dysfonctionnements. On peut aussi utiliser tout autre outil approprié de la sûreté de Fonctionnement. Pour rechercher les dysfonctionnements opératoires, on peut pareillement construire des AMDEC opératoires, utiliser tout autre outil d'analyse d'activité des opérateurs ou un outil mixte tel que HAZOP.

Chaque identification détaillée de dysfonctionnement fait ensuite l'objet d'une représentation de l'information ainsi recueillie sous forme d'un arbre de défaillances (arbre «secondaire»). On peut obtenir autant d'arbres de défaillances «secondaires» que de dysfonctionnements (figure 7).

## Arbres de défaillance

L'étape suivante consiste à évaluer les risques par une approche probabiliste. Si des arbres de défaillances «globaux» ont été construits dans le premier module à partir des arbres logiques, le raccordement de tous les arbres «secondaires» ci-dessus, sur les événements primaires de ces arbres «globaux», nous donne des arbres de défaillances généraux pour les événements majeurs. Si cette opération n'a pas été faite dans le premier module, alors elle est entreprise en une seule étape, à ce niveau de l'analyse. En toute hypothèse, la construction d'arbres de défaillances à partir des arbres logiques du premier module permet de faire apparaître de nouveaux événements.

Les propriétés des arbres permettent d'établir tous les chemins qui conduisent à l'événement final (coupes minimales de l'arbre) et d'identifier des modes communs (défauts de modes communs) ayant une importance majeure car communs à plusieurs groupes d'événements (branches de l'arbre) conduisant à l'événement final. S'il n'existe pas de logiciel permettant de construire automatiquement un

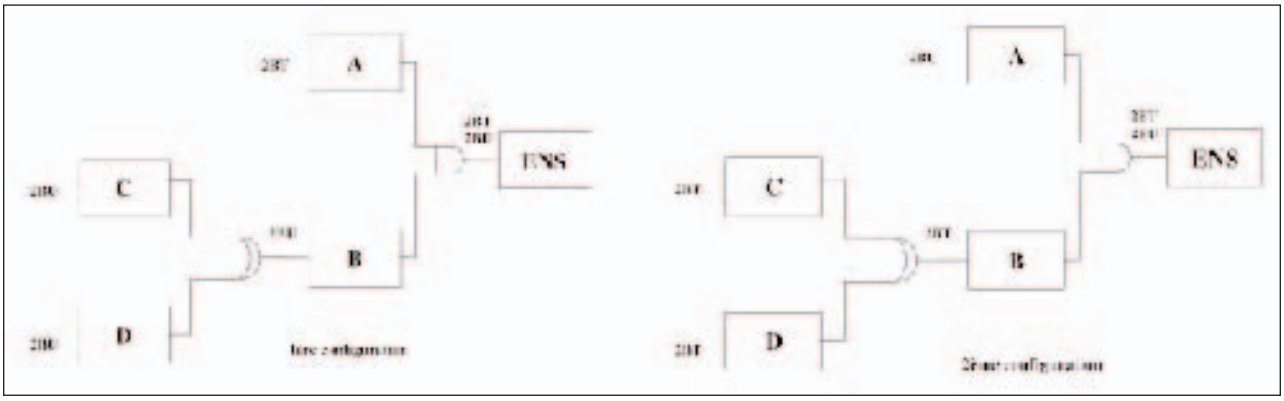


*Figure 8 : Arbres de défaillance avec les barrières techniques «BT» et les barrièreopératoires ou d'utilisation «BU».*

arbre de défaillances, de nombreux logiciels permettent de travailler sur l'arbre une fois celui-ci construit.

Dans la mesure où on connaît la probabilité des événements élémentaires de ces arbres généraux, on peut calculer la probabilité de l'événement final majeur. Cependant, en milieu industriel, il est encore assez rare de pouvoir conduire ce calcul car il y a peu de données de retour d'expérience concernant les défaillances élémentaires d'appareillages (peu sont reproductibles d'une installation à l'autre.) Et que dire des données concernant les dysfonctionnements opératoires, l'homme étant un système complexe par excellence ? On ne peut donc conduire que des calculs approchés qui donnent une idée des probabilités des événement finaux et permettent de les comparer entre eux ou avec des événements connus. Il est en tout cas exclu de se référer à des seuils de probabilités absolus. Que veut dire un seuil de $10^{-6}$ par an si l'on n'a pas d'élément comparatif ?

La définition d'objectifs complémentaires de prévention consiste à fixer a priori un nombre de barrières à mettre en place:

- par une méthode ascendante en neutralisant chaque événement élémentaire des arbres de défaillance et éventuellement certains événements intermédiaires. Dans le travail fait dans le premier module de l'analyse, certains de ces événements intermédiaires ont déjà été neutralisés.
- par une méthode descendante en utilisant les propriétés des arbres de défaillances avec leurs portes combinatoires pour, après avoir fixé un nombre de barrières sur l'événement final, répartir de proche en proche ces dernières jusqu'aux événements élémentaires.

On peut alors choisir, parmi différentes répartitions possibles, la meilleure répartition coût /efficacité en évaluant le coût des barrières. Cette technique, bien que très intéressante, est cependant encore peu appliquée (figure 8).

Pour le calcul du nombre de barrières, la règle est que chaque fois que l'on franchit une porte ET, les barrières s'additionnent alors que chaque fois que l'on franchit une porte OU, le nombre de barrières sur l'événement aval de la porte doit être le même que celui que l'on attribue à chaque événement en amont. Le nombre de barrières et leur répartition en nature (barrières techniques «BT» et barrières opératoires ou d'utilisation «BU») indiquent aussi la confiance que l'on accorde à la technique et aux opérateurs. Par exemple, pour un même niveau de gravité de l'événement final, implanter 1 barrière technique et deux barrières opératoires revient à faire plus confiance à la technique alors qu'instaurer 1 barrière opératoire et deux barrières techniques traduit l'attitude inverse.

Il reste ensuite à organiser la gestion des risques et à construire, à partir des scénarios identifiés, les plans d'intervention et notamment le plan d'organisation interne (dans le cas d'une installation industriel-

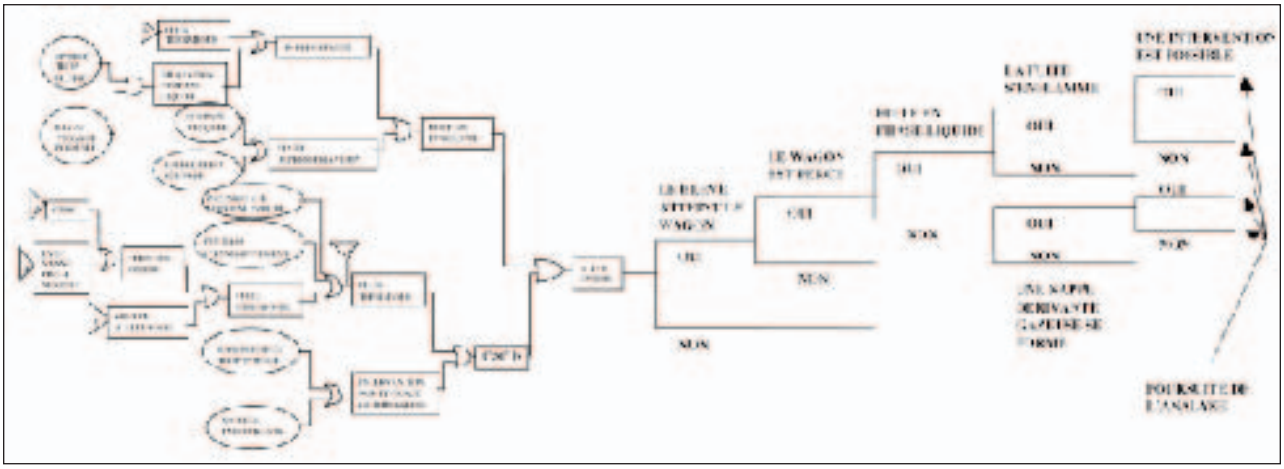

*Figure 9 : Arbre causes-conséquences*

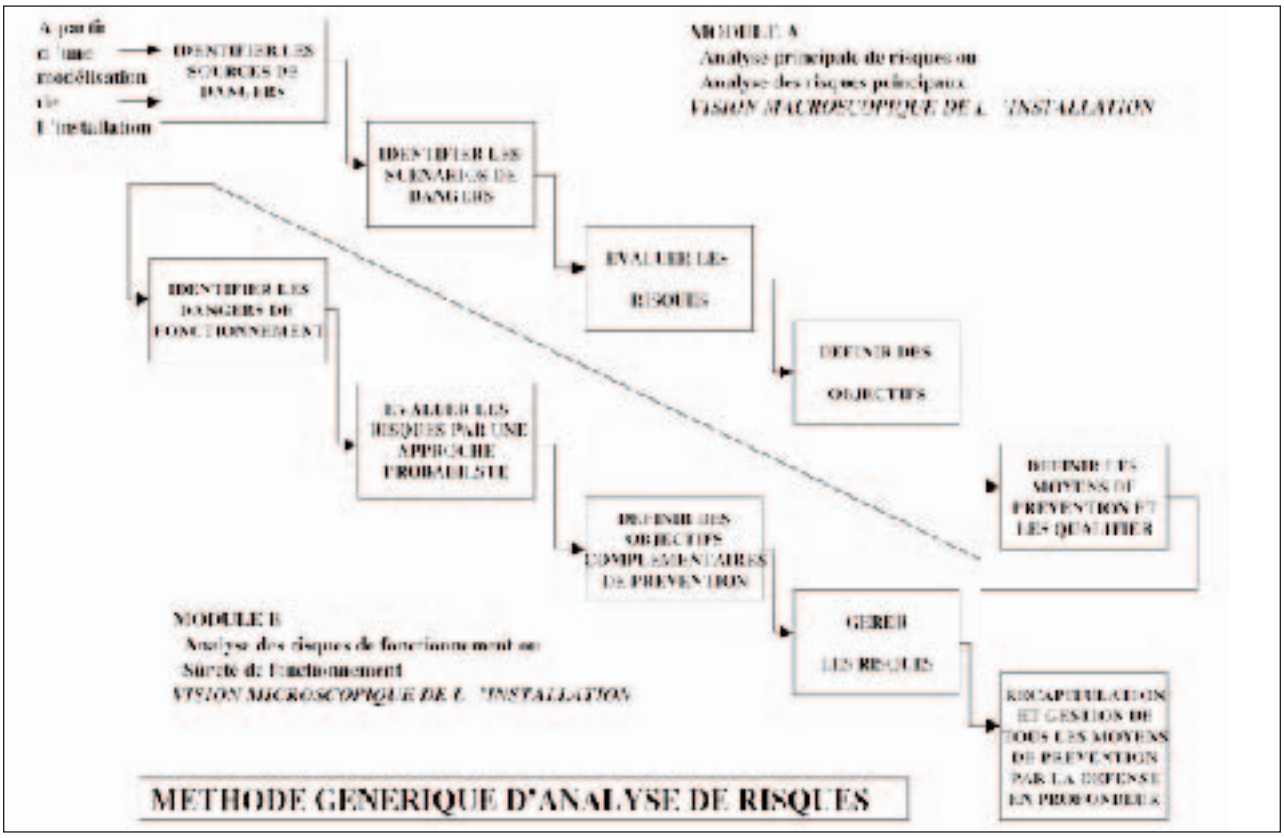


***Figure 10 : Schéma récapitulatif de la méthode générique d'analyse des risques.***

le). La construction d'arbre causes conséquences à partir des arbres de défaillances, auxquels on adjoint des arbres d'événements, facilite le travail. Cette démarche plus complète est aussi appelée « *Bow tie approach* », approche «nœud papillon» à cause de la forme globale de cet arbre (figure 9).

A ce stade toutes les barrières ont été définies pour neutraliser les événements et éviter que leur enchaînement conduise à un événement final majeur. Il reste maintenant à les gérer et toute barrière nouvelle devra être rendue pérenne en la traitant avec le tableau de qualification des barrières.

Dans tous les cas, organiser les barrières amène à poursuivre la stratégie de défense en profondeur qui repose sur le principe que les dispositions préventives restent insuffisantes si les défaillances prises en compte surviennent et si leurs conséquences apparaissent inacceptables Dans ce cas il y a nécessité de prendre des mesures de maîtrise des conséquences si celles-ci se réalisent d'où le besoin de prévoir finalement la gestion des situations accidentelles sortant du dimensionnement de l'installation. Cette défense en profondeur fait appel à des lignes ou niveaux de défense successifs ou progressifs allant de la maîtrise des événements mineurs à la maîtrise des événements majeurs par :

- la prévention des événements initiateurs ou précurseurs d'événements plus graves (anomalies de fonctionnement, défaillances de systèmes matériels, défaillances humaines…) ;
- le maintien de l'installation dans son domaine de fonctionnement autorisé. Ce domaine est défini lors de la conception de l'installation et fixe les paramètres notamment quantitatifs à ne pas dépasser (par exemple puissance maximale, quantités de produits…) ;
- la maîtrise des accidents à l'intérieur des hypothèses de conception appelées aussi hypothèses de dimensionnement par la définition des mesures de sauvegarde en cas d'accident ;
- la prévention de la dégradation des situations accidentelles pouvant conduire à des événements encore plus graves dits accidents hors dimensionnement et la limitation de leurs conséquences ;
- la construction des plans d'urgence incluant notamment les procédures ultimes en cas d'accident grave.

Cette stratégie s'applique aussi bien en conception des installations que pendant leur exploitation et jusqu'à leur déconstruction (ou démantèlement). Elle met en œuvre la prévention centrée sur la qualité de conception, de réalisation et d'exploitation afin de conférer à l'installation une résistance intrinsèque à ses propres défaillances et aux agressions internes (notamment les incendies) et externes (notamment celles d'origine naturelle : séismes, inondations… ; et celles liées à l'activité humaine : transports, industries…). Cette stratégie implique aussi la surveillance, la protection et les moyens d'action afin notamment de détecter et caractériser les situations anormales et ramener l'installation dans son domaine de fonctionnement autorisé ou dans son domaine de fonctionnement normal.

La stratégie de défense en profondeur est donc fondamentalement déterministe et elle s'appuie sur les notions de risque acceptable, de risque inacceptable et de risque résiduel. La gestion

des barrières entrera dans les trois domaines fondamentaux de l'entreprise que sont l'organisation (cela se traduira par des règles générales du type règles générales d'exploitation des installations), le management (cela se traduira par l'introduction de procédures découlant de l'analyse de risques dans les règles de management sécurité de l'entreprise déjà mises sous forme de normes) et l'assurance qualité (cela se traduira par les règles d'assurance qualité de la sécurité des installations).

## Du global au détail

La méthode ainsi décrite répond à une éthique permettant de s'assurer qu'une installation a pris en compte les risques qu'elle peut générer. Pour cela, la démarche procède à une approche déterministe complétée par une approche probabiliste dans la mesure où il a été possible de quantifier les probabilités de scénarios d'accidents majeurs mis en évidence. Elle permet d'introduire une phase de négociation sur les objectifs à atteindre impliquant si possible tous les acteurs concernés et facilitant ainsi la communication à tous les niveaux.

Elle intègre la réglementation applicable mais va plus loin en identifiant des moyens de prévention et de protection pour des événements qui ne sont pas pris en compte par la réglementation. Elle intègre le retour d'expérience dans la genèse de scénarios et dans la recherche de barrières permettant de les neutraliser. Elle construit une forme de démonstration de la sécurité d'une installation qui permet d'établir une confiance aussi bien des acteurs internes que des acteurs externes. Elle permet de disposer d'un document de référence qu'il est possible de tenir à jour en cas de modification et qui constitue un suivi de performance à travers l'assurance de la pérennité des barrières par leur qualification dans le temps. Elle fait apparaître les modalités de management et d'organisation nécessaires pour le choix des barrières et leur pérennité. Elle conduit tout naturellement à la construction du POI (ou d'autres plans d'urgence) à partir des scénarios construits et retenus. Elle permet aussi de coordonner les outils mis en oeuvre dans les démarches d'analyse des risques (voir la figure 10).

Grâce à la démarche systémique on n'entre pas dans l'analyse des risques directement avec des outils tels que l'AMDEC ou HAZOP ou les arbres logiques, ce qui évite de travailler tout de suite dans le détail avec le risque de dispersion que cela entraîne. L'approche systémique a aussi pour avantage de créer plusieurs niveaux de l'analyse, du global au détail, avec possibilité de s'arrêter à une profondeur préalablement choisie et donc de consacrer un temps donné à cette dernière. Le module A nécessite quelques jours d'analyse suivant la complexité de l'installation, tandis que le module B durera plusieurs semaines, voire plusieurs mois. ●

## BIBLIOGRAPHIE


[1] - J.L. LE MOIGNE, Théorie du Système Général, théorie de la modélisation. Ed. PUF, Paris.

[2] - Actes des Assises Internationales des formations universitaires et avancées dans le domaine des sciences et des techniques du danger, Université Bordeaux 1, IUT A, Département Hygiène, Sécurité, Environnement. 1993.

[3] - Actes de l'école d'été d'Albi «Gestion scientifique du risque : sciences du danger, concepts, enseignements et applications», Albi, 6-10 septembre 1999.

[4] – P. PERILHON, «Analyse des risques, éléments méthodiques», Phoebus n° 12, 1er trimestre 2000, pages 31 - 49.