La défense en profondeur ou comment limiter les dégâts

Réduire la probabilité et les conséquences de tout accident technologique est l'objectif affiché de la maîtrise des risques. Mais les progrès accomplis rendent exigeants, et nous sommes scandalisés par des accidents comme AZF, le « Prestige », voire la crise de la vache folle. Un nouvel enjeu consiste à mettre en place des politiques de « défense en profondeur » garantissant que les conséquences de tout accident, si accident il y a, restent dans des limites acceptables. Le respect des exigences de sécurité ne devrait plus être vécu comme une contrainte de production mais comme une véritable liberté d'action.

par Jean-Louis Nicolet
Expert en maîtrise des risques

Quelle est la gravité de l'incident qui vient de se produire dans cet atelier fabriquant du phosgène sachant qu'il n'y a ni mort ni blessé ? A quoi sert d'analyser les incidents qui se produisent si l'on ne peut mettre en place des dispositifs de protection fiables et sûrs ? Parmi ces dix incidents quels sont ceux qui ont fait courir un réel danger à mes opérateurs ? A qui incombe la responsabilité de l'accident qui vient de se produire ? A celui qui en est la cause ? A l'organisation ? A la défaillance des dispositifs de protection en place ? Que vaut mon système de défense et de sauvegarde ? L'organisation en place est-elle capable de prévenir les différents dangers qui peuvent se produire au sein de mon usine ? La formation de sécurité que je viens de donner à mes agents est-elle adaptée, opérationnelle ? Parmi toutes les exigences arrêtées lors de la conception de cet atelier chimique quelles sont celles qui doivent être impérativement connues et respectées par mes responsables tant en conduite qu'en maintenance ? Comment mesurer, au fil des restructurations et des départs à la retraite qui se sont produits durant ces trois dernières années, la dégradation des dispositifs de sécurité mises en place ?

Tout manager, avant de se lancer dans un investissement de quelque ampleur qu'il soit, souhaite connaître les bénéfices qu'il va en retirer. Pourquoi faire des études de prévention, de retour d'expérience, de fiabilité humaine, d'analyse systémique si l'on n'a pas, au moins, une idée de l'ordre de grandeur des gains espérés, tant économiques qu'humains ?

Zéro défaut, zéro risque

« Si l'automobile a joué un rôle pionnier dans ces campagnes de rappel des produits, celles-ci touchent en réalité tous les pans de l'économie ; cauchemar des industriels, de telles campagnes se paient de plus en plus cher. Le coût en est technique, juridique, financier, sans parler des pertes d'image qui peuvent s'avérer catastrophiques. Aux yeux des consommateurs, apparaît de plus en plus l'écart grandissant entre le discours des entreprises sur la qualité, le zéro défaut et les produits apparemment de plus en plus défaillants mis sur le marché » [1].

Trois raisons majeures expliquent cet état de fait.

La première tient au fait que « la perception du risque par le public a radicalement changé. Le seuil de tolérance aux risques tend vers zéro. Surinformé, averti de ses droits, mieux éduqué, le consommateur du XXIe siècle devient très exigeant d'autant qu'il est devenu le centre de l'économie » [1].

« La seconde raison résulte de l'extrême sophistication et de l'accélération du cycle de conception, réalisation, commercialisation des nouveaux produits et services. Engagées dans un processus de mondialisation, les entreprises multiplient les lancements, tentent de se doubler dans une course folle à la conquête de nouveaux marchés, alors que la conception des produits devient de plus en plus complexe du fait des performances recherchées et des normes de plus en plus sévères » [1].

La troisième raison a pour nom « externalisation ». Pour des raisons économiques et fiscales, les entreprises sont amenées à transférer une part croissante de la valeur ajoutée de leurs produits dans des pays à faible coût de main d'œuvre ou à fiscalité plus intéressante. Ce phénomène d'externalisation crée des ruptures de contrôle et, plus grave, de responsabilité, sans parler des incompréhensions dues aux différences culturelles. Les cas de « l'Erika » et du « Prestige », et aussi celui de l'AZF, illustrent combien le recours à des sous-traitances et à des personnels d'origines variées diluent les responsabilités au point qu'elles ne peuvent même plus être identifiées.

Dans un tel contexte, concilier productivité, rentabilité, qualité et sécurité devient pour tout manager un impératif majeur ; la maîtrise des risques doit être considérée comme « un processus de prévention et de protection permettant à une entreprise, un réseau ou une entité donnée, placée dans un contexte de compétitivité, de prendre toutes les décisions qui s'imposent en vue d'optimiser son activité (industrielle et commerciale) sans subir ou faire subir à ses clients et à son environnement des dommages technologiques, économiques et humains qui mettraient en péril de façon durable et irréversible sa pérennité ». [2]

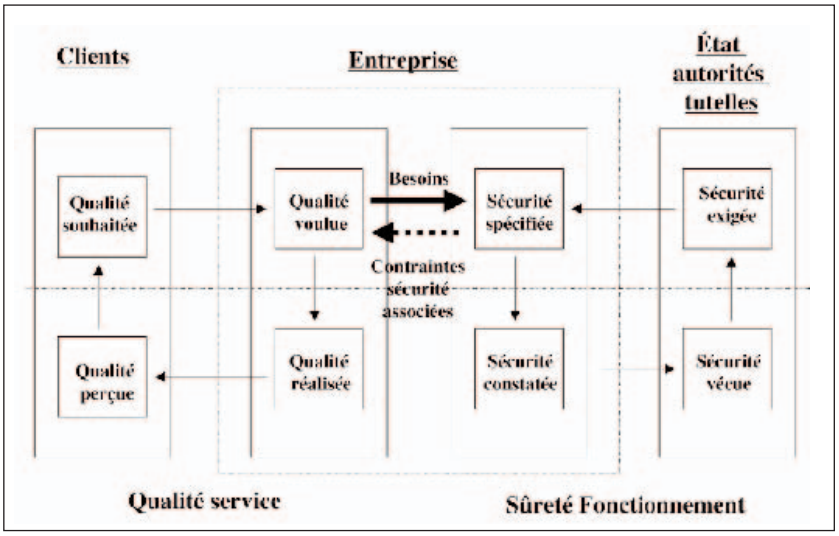

Fig. 1.- Qualité-Sûreté

La dualité : qualité-sécurité

Les deux démarches de qualité et de sécurité se sont longtemps ignorées, chacune ayant suivi son chemin propre, tâtonné, forgé son vocabulaire, acquis ses certitudes. Essayons de comprendre comment, sous la contrainte de la production, est apparue cette dualité et comment la qualité a pris peu à peu le pas sur la sécurité, qui est vécue comme une contrainte peu supportable.

Le cycle de la qualité, comme l'expliquent Bernard et Danielle Averous [3], repose sur quatre piliers fondamentaux, à savoir :

- la qualité attendue par le client, qui amène les hommes de l'entreprise à chausser les lunettes du client, du consommateur et leur permet de remettre en cause leurs propres logiques de travail ;
- la qualité voulue par l'entreprise, résultat d'un arbitrage entre les attentes des clients et ce qu'a décidé de faire l'entreprise, compte tenu des possibilités techniques et technologiques du marché et de ses propres contraintes économiques et sociales ;
- la qualité réalisée par l'entreprise, qui, de fait, mesure l'écart entre la qualité qu'elle a voulue et le niveau de performance réellement atteint (les rappels de produits sont un exemple de cet écart) ;
- la qualité perçue par le client qui mesure son degré de satisfaction par rapport à ses attentes (voir la figure 1).

Le processus de maîtrise de la sécurité, bien que similaire, procède d'un autre esprit. Avant de réaliser ou faire construire un nouveau système, un nouvel équipement, tout maître d'ouvrage se doit de rédiger un cahier des charges dans lequel il fixe les caractéristiques des produits et services qu'il désire mettre sur le marché en précisant les niveaux de risques qu'il juge acceptables, le risque zéro n'existant pas. Pour certaines industries telles le nucléaire, l'aéronautique, le ferroviaire, une autorité de tutelle fixe au préalable les normes à respecter, puis s'assure tout au long de la réalisation du projet que celles-ci le sont bien et que les risques encourus resteront bien à l'intérieur des limites réglementaires fixées par elle-même et les instances internationales. A ce stade, nous parlerons de « sécurité exigée ». Ce peut être, par exemple, la nécessité de confiner tout gaz toxique, ou la résistance de tel type de process à un séisme force 5 sur l'échelle de Richter…

La conception étant un processus itératif, le maître d'ouvrage doit identifier, à chaque étape du développement du projet, tous les dangers que le futur système risque d'induire pour les hommes et l'environnement, tout en précisant pour chacun d'eux la probabilité d'occurrence et la gravité. Les risques identifiés, il doit mettre en œuvre une politique de sécurité permettant de réduire chaque danger à des valeurs socialement acceptables, par exemple en modifiant les process initialement envisagés et en prévoyant des systèmes de sauvegarde ne présentant pas de modes communs… c'est le cas de la tour de neutralisation et de la torchère prévue sur l'usine chimique implantée à Bhôpal en Inde par Union Carbide. Sur la base des spécifications fournies par le maître d'ouvrage, l'ingénierie, les équipementiers, les ensembliers doivent concevoir, fabriquer, monter, tester des dispositifs de sécurité, les fonctions de sauvegarde et les barrières technologiques nécessaires pour que les objectifs de sécurité fixés soient respectés. L'ensemble des exigences arrêté à la fin de ce processus itératif constitue ce que nous appellerons la « sécurité spécifiée ». Elles constituent autant de paramètres, de facteurs que l'exploitant devra prendre en compte et respecter. C'est ainsi qu'à Bhôpal il était prévu, par exemple, que sur les trois cuves de stockage en service, une devrait toujours être vide pour permettre, en cas de besoin, de transférer le contenu d'une autre cuve. De même, un certain nombre d'essais devaient être faits périodiquement pour tester l'aptitude à fonctionner des systèmes de sauvegarde mis en place.

En phase d'exploitation, ces exigences ne sont pas toujours respectées : tel fut le cas à Bhôpal où les essais périodiques n'étaient plus réalisés depuis longtemps, au motif que l'usine ne produisait pas et que cela permettait de réaliser des économies. On parlera ici de « sécurité constatée ».

Utilisant les produits et services mis à leur disposition, les clients, les consommateurs, peuvent subir certains désagréments, certains dommages, sans parler des riverains des usines à risques (1). On parlera alors de «sécurité vécue». La figure n° 1 schématise ces deux boucles : qualité-sécurité.

La maîtrise des risques au sein de nos systèmes et réseaux socio-techniques repose essentiellement sur le respect des exigences fixées, que celles-ci concernent la construction proprement dite du système (par exemple : respect des normes antisismiques), la conduite (par exemple : respect d'une plage de pressions) et la maintenance (par exemple : remplacement au bout d'un temps donné de certaines pièces). Il est donc essentiel que la recherche d'une meilleure qualité, ou d'une augmentation momentanée de la production, ne conduise pas à remettre en cause la sécurité. Force est de constater que les impératifs de qualité et de rapidité prennent souvent le pas sur les exigences de sécurité.

Pour obtenir une véritable synergie entre qualité de service et sécurité, il est donc essentiel que le maître d'ouvrage et l'exploitant précisent aux concepteurs et aux constructeurs, dès la phase de lancement du projet, la nature et la spécificité des services à fournir aux clients. En retour, l'équipe projet devra indiquer avec précision à l'exploitant :

- les caractéristiques techniques du système ;
- les exigences de sécurité à respecter ;
- les dispositifs de « défense en profondeur » et de sauvegarde à mettre en place ;
- et les dispositifs de contrôle quotidien.

Ce n'est qu'à ce prix que le risque résiduel jugé acceptable peut être garanti. En d'autres termes, pour que toute exigence de service s'efface devant une exigence de sécurité, encore faut-il que celle-ci soit connue de l'exploitant.

La maîtrise des risques

Maîtriser les risques a toujours été une préoccupation de tous ceux qui conçoivent et exploitent l'ensemble des systèmes et réseaux technologiques indispensables. Au fil des années, suite aux conséquences des accidents et catastrophes survenues, de nouveau process, de nouvelles architectures, technologies, méthodes, organisations ont vu le jour et ont été affinées. Ainsi, la recherche des responsabilités, lors de tout dysfonctionnement technologique grave, a conduit à la mise en place de services d'Inspection chargés d'identifier lors de toute séquence accidentelle tous les écarts significatifs par rapport aux procédures en vigueur puis, en fonction de l'importance de ceux-ci, de sanctionner les contrevenants. Dans le même esprit, mais à titre préventif, ont été créés des services d'audit ayant pour missions de détecter toutes les dérives susceptibles d'engendrer des incidents, voire des accidents graves.

Si la sanction est dissuasive vis-à-vis des hommes, elle est de bien peu d'effet sur les composants technologiques défaillants , encore moins sur une organisation déficiente. Comprendre comment la séquence accidentelle redoutée s'est produite ? Quelles en étaient les causes ? Comment celles-ci se sont-elles enchaînées ? Ainsi est né le « retour d'expérience ». Si, au début, les analystes ne s'intéressaient qu'à la fiabilité, la « maintenabilité » et la disponibilité des composants technologiques, il est ensuite apparu nécessaire de s'intéresser à l'homme, à ses caractéristiques physiques, physiologiques, psychologiques pour mieux comprendre ses réactions face aux différentes situations auxquelles il était soumis. Avec l'augmentation continue des énergies mises en jeu, l'utilisation de produits de plus en plus sophistiqués et nocifs, le nombre croissant de passagers embarqués, la nature des risques, leur nombre - sans parler de leur gravité - n'a fait que croître, au point que ceux-ci ne sont plus toujours assurables.

Pour être à même de mieux évaluer, quantifier, comparer, hiérarchiser les différents événements redoutés qui peuvent survenir au sein d'une entreprise ou de son environnement, une première approche, devenue classique bien que délicate, consiste à associer à chacun d'eux un niveau de risque défini comme le produit de deux variables caractéristiques, la probabilité d'occurrence de l'événement redouté (Pr) par la gravité de ses conséquences ou de son impact (C) :

$$R = Pr \times C.$$

Des barrières emboitées

Comment éviter que les matières radioactives mises en œuvre dans les réacteurs civils et militaires ne contaminent plus ou moins gravement les hommes et l'environnement immédiat ? Comment limiter l'impact d'une irradiation ou d'une contamination dans des limites ne mettant en cause la vie des opérateurs et des riverains ? Comment être en mesure de garantir le respect de ces seuils en cas de dysfonctionnement d'un ou plusieurs équipements ? Telles étaient, entre autres, les questions auxquelles étaient confrontés les hommes du nucléaire à son début. Progressivement, ils sont arrivés à la conclusion qu'il fallait mettre entre l'agent agressif (la matière nucléaire) et les cibles sensibles (les hommes et l'environnement) un certain nombre de barrières technologiques conçues en fonction des dangers à maîtriser, s'emboîtant comme les pelures d'un oignon et capables de s'opposer à la propagation des matières radioactives et d'arrêter des rayonnements émis.

C'est ainsi que la première barrière était constituée d'une gaine métallique à base de zirconium contenant la matière nucléaire. La seconde était matérialisée par l'enveloppe en inox du réacteur, renfermant les éléments combustibles gainés, eux-mêmes immergés dans une eau présentant des caractéristiques chimiques draconiennes. La troisième barrière était constituée par une enceinte de confinement. Parallèlement, d'autres dispositifs de sécurité et de sauvegarde étaient mis en place pour limiter les conséquences du développement non contrôlé de toute réaction nucléaire, comme, par exemple, le dispositif permettant de faire chuter automatiquement un certain nombre de barres capables d'absorber les neutrons émis par le cœur du réacteur et, donc, de ralentir la réaction en chaîne, ou le dispositif d'injection d'eau sous pression dans le cœur du réacteur en cas de rupture d'une tuyauterie primaire.

A chaque barrière était associé un certain nombre de dispositifs de mesure

(1) A Bhôpal, du fait du non-respect d'un certain nombre d'exigences d'exploitation et de maintenance, il y eut plus de 2500 morts et des milliers d'intoxiqués.

permettant aux opérateurs de savoir, directement ou indirectement, si elle était ou non opérationnelle. Ce point est essentiel, car il permet à l'exploitant de connaître en permanence l'état des lignes de défense mises en œuvre et donc d'engager sans délai, en fonction de la perte de telle ou telle barrière, les actions qui s'imposent pour maintenir la menace à l'intérieur des seuils fixés. Cette approche à caractère déterministe implique de décrire le processus de danger et les dispositions prises pour le contenir dans des limites acceptables et acceptées au moins par les autorités de tutelle. Elle permet, en outre, de mieux mettre en évidence les conséquences de la défaillance de telle ou telle barrière. A l'exception de l'accident de Tchernobyl, ayant pour cause la violation plus ou moins consciente de six consignes de sûreté, ce concept s'est avéré d'une remarquable efficacité pour le parc électronucléaire mondial. Du fait de son efficacité, ce concept de défense en profondeur a donc été repris par nombre d'industries à risques.

Comme nous venons de le voir, la mise en place d'une défense en profondeur implique de définir, dès la phase de conception, un ensemble architectural de lignes de défense composées de barrières de natures différentes, capables d'annuler et de limiter les effets des agresseurs recensés à des valeurs objectives fixées au départ. Ces lignes de défense sont essentiellement technologiques.

Or l'expérience prouve que sur la plupart des unités de production nombre de systèmes de défense et de sauvegarde prévus par les concepteurs, tombent en désuétude : en l'absence d'accident, la mémoire collective et individuelle oublie, au fil des mutations et transformations de l'entreprise, pourquoi ces systèmes avaient été installés, quelles étaient leurs fonctions et leurs rôles opérationnels !

A l'image de l'archéologue, nous nous sommes efforcés, au cours de ces dernières années, notamment lors d'études de retour d'expérience suite à des incidents fréquents ou d'accidents graves, de dégager de leur gangue ces défenses oubliées, de leur redonner leur sens initial, d'en montrer les limites dans le contexte actuel et de les faire évoluer pour leur rendre toute leur efficacité.

C'est ainsi que progressivement nous avons été amenés à définir un certain nombre de caractéristiques technologiques, organisationnelles et humaines auxquelles devrait répondre toute ligne de défense pour assurer pleinement son rôle, inventaire que nous présentons rapidement ci-après et dont nous avons pu mesurer l'efficacité opérationnelle, notamment sur un grand réseau ferroviaire.

Barrières statiques et dynamiques

D'une façon générale, toutes les barrières envisageables peuvent être regroupées en deux grandes catégories :

- les barrières statiques ou passives, qui défendent en permanence le système face à ses agresseurs, comme par exemple les murs antisismiques d'une centrale nucléaire ou un heurtoir absorbeur d'énergie situé en bout de ligne ferroviaire ;
- les barrières dynamiques, qui ne sont activées qu'une fois l'événement redouté ou le danger détecté : ce peut être un automatisme qui coupe le courant sur une ligne dès qu'un court circuit est enregistré ou une batterie de sprinklers qui inonde un local dès qu'un feu ou une fumée est détecté.

A noter que les barrières statiques, à l'inverse des barrières dynamiques, ne tombent pas en panne, mais se dégradent au fil du temps en l'absence d'entretien adéquat.

Toute barrière dynamique peut prendre trois états à savoir :

- un état, dit de réussite, qui traduit le fait qu'après avoir été sollicitée la barrière a été capable de contrôler, de maîtriser le danger qui lui était associé, c'est-à-dire d'éviter qu'il atteigne la ou les cibles sensibles ;
- un état, dit d'échec, qui traduit le fait que la barrière en cause a été incapable pour différentes raisons de résister aux assauts des éléments redoutés qui ont pu ainsi atteindre leur cible ;
- un état, dit de panne, qui traduit le fait que la barrière n'est plus en mesure d'agir ou de répondre aux sollicitations de danger pour laquelle elle est prévue.

Selon leur nature, les barrières peuvent présenter des fiabilités très différentes. Deux catégories principales sont à considérer :

- les barrières technologiques composées uniquement de composants mécaniques, électriques, électroniques, comme, par exemple, un système d'arrêt automatique des trains dès franchissement d'un signal fermé ; selon leur conception et les technologies mises en œuvre, elles peuvent avoir des taux de défaillance extrêmement faibles qui peuvent avoisiner les 10^{-6} / an ;
- les barrières mixtes composées d'éléments technologiques, procéduraux et humains dont la fiabilité est beaucoup plus faible, leur taux de défaillance étant de l'ordre de 10^{-3} ; dans de tels ensembles, l'homme doit agir conformément aux instructions qui lui sont données par des procédures ou des modes opératoires, dès qu'il est mis en alerte par un signal ; c'est le cas du mécanicien conduisant un TGV qui doit actionner son système de freinage dès qu'il perçoit un signal de ralentissement ou d'arrêt, mais ce peut être aussi une directive européenne qui peut s'avérer, pour des raisons d'éthique (fraude), de peu d'efficacité, par exemple à propos de la crise de la vache folle.

Pour être efficace, toute barrière doit être capable de détecter les dangers qu'elle est chargée de maîtriser. Cette détection peut et doit porter sur les différents éléments caractéristiques du risque à maîtriser. Par exemple, dans le cas de la protection d'espacement des trains, le danger est matérialisé par l'énergie cinétique du train qui arrive en amont d'un autre qui circule plus lentement ou qui est arrêté. Pour déterminer si celui-ci est ou non agressif par rapport aux autres, il est nécessaire de localiser tous les trains dans les différents cantons de la ligne et de vérifier si les distances entre chaque couple de mobiles sont ou non suffisantes pour que le mécanicien du train agresseur soit en mesure d'arrêter son convoi compte tenu des dispositifs de freinage dont il dispose. Cet exemple montre que la conception de toute barrière implique une analyse très fine et poussée du système socio-technique considéré.

Pour contenir un risque donné à des niveaux de probabilité très inférieurs à 10^{-6}/an, il est généralement nécessaire

de mettre en place plusieurs barrières successives, les premières étant mixtes (par exemple : signal, mécanicien, procédure) et les dernières technologiques (par exemple : dispositif type KVB).
Après avoir détecté le danger potentiel, la barrière doit être en mesure de ramener, avec la rapidité nécessaire, le système dans un état sûr. Pour ce faire, elle doit agir selon les spécificités du système et de son environnement sur l'élément agresseur, par exemple, en présentant au conducteur du train agresseur un signal d'arrêt impératif sachant qu'il dispose d'un système de freinage efficace et adapté.
Concevoir et mettre en place des barrières est bien, encore faut-il savoir si, une fois sollicitées, celles-ci ont pu ou non remplir le ou les rôles qui leur étaient assignés. Il est donc important que toute barrière de sécurité mise en place puisse, sans délai, signaler à l'exploitant, qu'elle vient, suite à une sollicitation, de mettre le système dans un état sûr ou qu'elle est tombée en panne en cours de fonctionnement, cas qui doit s'avérer extrêmement rare compte tenu des fiabilités recherchées et retenues. De façon plus générale, toute barrière doit être conçue pour être en mesure de signaler qu'elle n'est plus opérationnelle, par exemple suite à la défaillance soudaine de l'un ou l'autre de ses composants. Informé, l'exploitant peut alors prendre les mesures de sécurité qui s'imposent, par exemple arrêter momentanément l'installation, le temps de la remise en état de la barrière défaillante. Une question se pose pour les barrières mixtes : faut-il ou non prévoir systématiquement une barrière supplémentaire, à caractère technologique, pour pallier une éventuelle défaillance humaine dont la probabilité est de l'ordre de 10^{-3} ? De fait, tout dépend de la nature des dangers et du niveau de risque accepté et acceptable.

Conception d'une défense en profondeur

Comme nous venons de le voir, en fonction des dangers à maîtriser et plus précisément de leur impact, il peut être nécessaire de mettre en place, non pas une barrière mais plusieurs en série. De leur fiabilité individuelle dépendra l'efficacité de la défense mise en place. Celle-ci dépendra pour l'essentiel des architectures retenues et des technologies mises en œuvre. Dés lors, on comprend l'importance de la diversification des méthodes, par exemple en évitant d'alimenter toutes les barrières d'une ligne de défense à partir d'une même source d'énergie.
Voyons maintenant comment une ligne de défense composée par exemple de deux barrières successives fonctionne. La première barrière est activée dès que la ou les situations dangereuses sont détectées.
De deux choses l'une :
- ou la barrière réussit à contenir l'événement redouté et à ramener le système dans un état sûr différent de l'état de fonctionnement normal ;
- ou la barrière échoue et l'événement redouté devient réalité.
Dans le premier cas, le danger est maîtrisé, le système étant dans un état sûr. Il ne restera à l'exploitant qu'à remettre son installation en service. Dans le second cas, nous sommes face à un événement potentiellement dangereux. Heureusement que la deuxième barrière existe ! Là encore, de deux choses l'une :
- soit la deuxième barrière, une fois activée, résiste à l'événement redouté et le danger sera à nouveau maîtrisé ;
- soit elle est mise en échec et le danger n'étant plus maîtrisé, nous allons droit à l'accident, sauf si, au dernier moment, un homme qui se trouve là, par hasard ou non, interrompt la séquence infernale et stabilise le système dans un état dégradé stable en effectuant une action positive, non prévue ; on parlera, dans ce cas, de presque incident et de boucle de rattrapage humaine.
Dans tous les cas, il appartiendra aux opérateurs de ramener le système dans un état de fonctionnement normal en suivant les procédures en vigueur. S'en affranchir peut s'avérer catastrophique !
La figure 2 explicite le processus de fonctionnement qui vient d'être décrit.
La mise en place de toute politique de défense en profondeur implique de respecter les étapes suivantes :
- identifier tous les événements redoutés propres au système considéré, en précisant, pour chacun d'eux, le danger, le type d'agresseur, les cibles potentielles, les scénarios possibles et les caractéristiques de l'environnement ;
- évaluer la probabilité d'occurrence des différents scénarios envisageables ;
- définir la stratégie de défense retenue, par exemple rendre l'élément agresseur inoffensif, insensibiliser la cible, mettre en place une ligne de défense ;
- déterminer le nombre et la nature des barrières à mettre en place ;
- fixer la valeur du risque résiduel acceptable ;

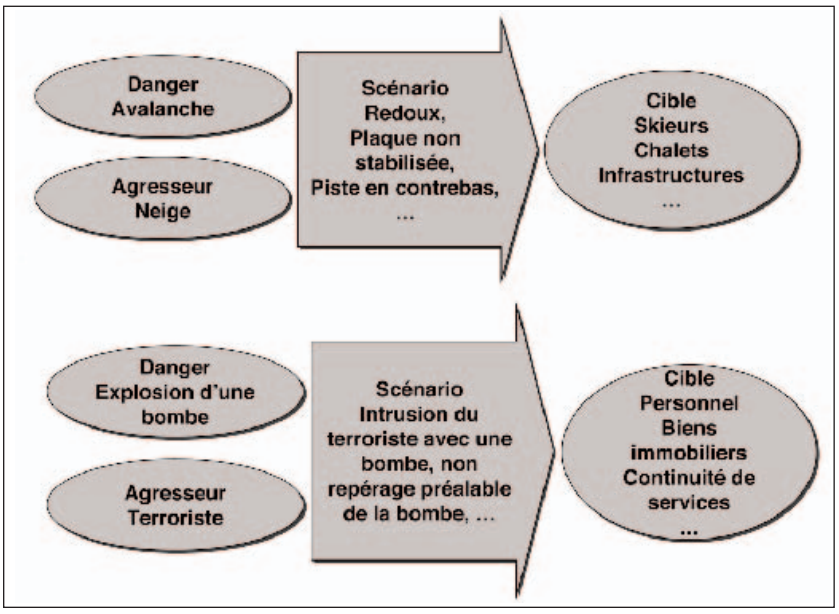

Fig. 2.- Le risque : illustrations

- expliciter, pour chaque barrière, les exigences de conception, de conduite et de maintenance à respecter ;
- former l'ensemble du collectif de travail sur la nature et les caractéristiques des lignes de défense mises en place ;
- suivre en permanence les causes et la fréquence de mise en échec des différentes barrières composant les différentes lignes de défense ;
- engager les actions qui s'imposent tant en conception qu'en exploitation pour atteindre les objectifs de sécurité recherchés.

Potentiel de gravité des incidents précurseurs

Ne pouvant apprécier le potentiel de criticité de chaque incident, il nous est apparu utile de classer ces derniers par rapport au nombre de barrières restantes. Pour un risque donné, franchir une barrière dans une ligne de défense qui en comporte trois, n'est pas très grave. A l'inverse, franchir la dernière signifie que l'ensemble de la ligne de défense en place a failli et que les risques encourus ne sont plus maîtrisés, sauf si les bons génies du système interviennent à temps. Mais peut-on faire toujours confiance à ces bons génies ? La catastrophe évitée, l'incident précurseur est vite oublié, minimisé, et l'exploitation reprend ses droits jusqu'à l'alerte suivante qui, malheureusement, n'est pas plus prise au sérieux jusqu'au jour où la catastrophe survient. Identifier tous les événements potentiellement dangereux qui ont pu se développer sans trouver en face d'eux des barrières mixtes et technologiques fiables est un objectif prioritaire pour tout manager ; encore faut-il mettre à sa disposition des indicateurs spécifiques et significatifs.

Pour commencer, nous recommandons de présenter les incidents précurseurs, sous forme d'histogramme en les classant suivant leur niveau de dangerosité. Au niveau A, nous classons les incidents au cours desquels une seule barrière a été franchie dans une ligne de défense qui en comporte au moins trois. Au niveau B, nous classons les incidents au cours desquels plusieurs barrières ont été franchies mais qui n'ont été arrêtés que par la dernière ; à l'évidence de tels incidents sont beaucoup plus graves que ceux de la classe A, car la sécurité du système n'a reposé que sur la résistance de la dernière barrière. Enfin, les incidents au cours desquels toutes les barrières de la ligne de défense ont été franchies seront classés C. Ici, le risque est maximum. Seule une intervention adéquate de dernière minute, par un agent se trouvant là, conscient des risques encourus, a pu éviter que la situation ne tourne au drame. Si les incidents de la classe A peuvent relever de la responsabilité des chefs d'unité, ceux de classe B devraient remonter au niveau des départements et ceux de classe C faire systématiquement l'objet d'une information de la direction générale. Bien entendu, il appartient à chaque échelon la responsabilité d'engager les actions qui s'imposent pour éviter que de telles situations ne se reproduisent et risquent de compromettre gravement la vie de l'entreprise.

Une source de liberté

Loin d'être une contrainte supplémentaire à la production, la mise en place d'une défense en profondeur efficace, sûre, doit être considérée par tous les acteurs de l'entreprise, qu'il s'agisse de la direction générale, des financiers, des chefs de départements et d'unités, des opérateurs, des agents de maintenance, comme une source de liberté permettant à chacun d'exercer pleinement ses responsabilités.

Car, comme le dit Jean-Pierre Dupuy [4] : « En vérité, il n'y a pas d'action qui exprime plus hautement la liberté de l'homme que de fixer des limites à sa capacité individuelle d'agir, sous forme d'impératifs, de normes et de règles à validité universelle et de s'y tenir. Car c'est par cette autolimitation que les individus deviennent des personnes autonomes entrant en communication les uns avec les autres ». ●

BIBLIOGRAPHIE

[1] Guillermard V. (2000). « L'entreprise face à l'exigence zéro défaut », *Le Figaro,* 12 septembre.
[2] Planchette G. - Nicolet J.L. – Valancogne J. (2002). « Et si les risques m'étaient comptés ! » Toulouse, OCTARES.
[3] Averous B, Averous D (1998) « Mesurer et manager la qualité de service » Condé-sur-Noireau, INSEP.
[4] Dupuy JP, (2002). « Pour un catastrophisme éclairé », SEUIL (La couleur des idées).