INRS CDU 168.4 : 614.8

Bilan des méthodes d'analyse a priori des risques

2. Principales méthodes de la sécurité des systèmes

M. Favaro et M. Monteau, service Accidentologie, centre de recherche de l'INRS, Nancy

Ce travail s'inscrit dans le cadre d'un bilan consacré aux méthodes d'analyse prévisionnelle des risques. La première note documentaire (ND 1768-138-90 « 1. Des contrôles à l'ergonomie des systèmes ») a développé plus particulièrement les procédures de contrôle des risques ainsi que les méthodes d'inspiration ergonomique (études de poste, analyses globales).

Cette seconde partie présente le domaine des méthodes et des outils généralement regroupés sous la dénomination de « sécurité des systèmes ». Sous une forme nécessairement condensée, le lecteur y trouvera les éléments d'information indispensables pour appréhender l'essentiel de ce qu'il convient de connaître de cette approche à dominante technique du risque industriel.

Outre des développements d'ordre méthodologique et technique, il est apparu utile de se prononcer sur les questions qui doivent être soulevées par la mise en œuvre de ces méthodes : fiabilité des données, interprétation des probabilités, introduction de la « fiabilité humaine ».

Analyse des risques / Sécurité des systèmes / Méthodologie / Fiabilité / Facteur humain

Evaluation of a priori risk analysis methods. 2 – Principal methods of the systems safety

This report is part of a general review of a priori risk analysis methods. The first part (ND 1768-138-90 : « 1. From inspection and checking to system ergonomics ») focussed more on risk control procedures and ergonomic methods (workplace analysis, general analysis).

This second part takes a look at methods and tools generally grouped under the heading « systems safety ». In condensed form it covers the essentials of this predominantly technical approach to occupational risk prevention.

As well as a methodological and technical review of the subject, it addresses the questions raised by the implementation of these methods : data reliability, probability evaluation, the notion of « human reliability ».

Risk analysis / Systems safety / Methodology / Failure / Human factor

1. NAISSANCE ET DEVELOPPEMENT

1.1. Repères historiques

1.1.1. La méthode de l'arbre des défauts

La sécurité des systèmes s'est constituée comme discipline par suite d'un besoin croissant de maîtriser les risques nouveaux et mal connus. La complexité des systèmes techniques à haut risque (systèmes d'armes, électronucléaire, aéronautique) a activement contribué au développement d'une approche systémique (1) des installations. C'est, en effet, la capacité de prise en considération des

(1) Pour mémoire, l'« approche systémique » désigne une démarche d'analyse conçue pour répondre à la complexité caractérisant de nombreuses formes d'organisations (biologiques, sociales, sociotechniques, etc.). L'examen des interactions y tient une place centrale.

phénomènes d'interactions entre les éléments d'un système technique (unités fonctionnelles, composants) qui caractérise l'originalité méthodologique de la sécurité des systèmes.

Mais, à l'origine de cette démarche, les préoccupations concernaient d'une façon plus restrictive la fiabilité des techniques mises en œuvre. Le manque d'expérience concernant l'existence de certains risques de défaillance a naturellement conduit les responsables de programmes techniques complexes à concentrer leurs efforts sur la mise au point d'une méthode, ou plutôt d'un outil d'analyse, qui permettrait de procéder à l'examen systématique des risques.

La méthode de l'arbre des défauts ou arbre des défaillances (Fault Tree Analysis) (2), élaborée par la compagnie des téléphones Bell pour le compte de l'armée de l'air américaine, répondra à cette exigence première de maîtriser analytiquement le risque. Cette méthode fut expérimentée pour l'évaluation de la sécurité des systèmes de tir des missiles ICBM Minuteman au début des années 1960.

Le développement de la méthode de l'arbre des défauts sera poursuivi par la Compagnie Boeing (3). Courant 1965, elle subventionnera avec l'université de Washington un symposium sur la sécurité des systèmes à Seattle : la diffusion de la méthode était lancée.

Cette dernière trouvera un important terrain d'application dix ans plus tard, avec la parution du « rapport Rasmussen » (1975) ou « rapport Wash-1400 » concernant la sûreté des centrales nucléaires américaines. Commencée au début des années 1970, cette étude représentait la première analyse exhaustive des risques pour les centrales nucléaires. Elle contribuera au développement de l'analyse probabiliste du risque en privilégiant délibérément, à travers l'utilisation de l'arbre des défauts, la quantification du risque (4).

1.1.2. Le devenir des méthodes quantitatives

La polémique qui suivit la publication de cette étude résulta d'ailleurs en partie de cette attitude. Il y manquait l'utilisation « d'une méthodologie cohérente organisée au niveau du système complet, qui tienne compte à la fois de son environnement (technologique, naturel, humain) et de sa vie (mise en service, maintenance, etc.) » (Deschanels et Lavedrine, 1984, p. 32).

L'« American Institute of Physics » adressa effectivement un certain nombre de reproches méthodologiques et techniques à l'encontre du rapport Wash-1400, réaction qui conduisit à l'élaboration d'une deuxième version. Cette dernière sera elle-même remise en question par le « rapport Lewis » (1978), effectué à la demande du Congrès des Etats-Unis. Ce dossier, qui passe en revue les acquis et les limites de l'étude Wash-1400, émet de nombreuses critiques, portant notamment sur la validité des données de base et sur les moyens méthodologiques et statistiques utilisés. Il insiste enfin sur la nécessité de disposer de méthodes plus sûres de quantification de l'incertitude.

Ces conclusions contribuèrent à la décision prise début 1979 par la « Nuclear Regulatory Commission » (NRC) de rejeter les résultats fournis par le rapport Wash-1400.

Une telle situation faillit bien condamner les techniques naissantes de quantification probabiliste du risque et par conséquent menacer l'existence de la méthode de l'arbre des défauts qui autorisait la poursuite de cet objectif.

L'accident survenu au mois de mars de la même année à la centrale nucléaire de Three Mile Island enraya cette évolution. Le scénario de l'accident tel qu'il fut reconstitué par la suite avait en effet été prévu par le rapport Rasmussen (bien que celui-ci affirmait que le cœur détérioré devait fondre et bien que les probabilités calculées, notamment celles concernant l'erreur humaine, apparurent rétrospectivement dénuées de fondement). L'accident de Three Mile Island ne réhabilitera jamais totalement ce rapport, mais il contribuera à relancer l'intérêt pour les analyses probabilistes des risques dans le nucléaire.

(2) Cf. plus loin § 3.4.1 pour la définition détaillée de la méthode.

(3) A la même époque, la compagnie Boeing développera la méthode de l'« analyse préliminaire des risques » (cf. § 3.1).

(4) Une autre méthode d'analyse sera développée à l'occasion de cette étude : la méthode de l'« arbre d'événements » (Event tree), présentée comme complémentaire de l'analyse par arbre des défauts (cf. § 3.3).

Toutefois, parallèlement à ces événements, les méthodes d'analyse de sécurité des systèmes se sont rapidement développées. Elles trouveront des applications diversifiées, tant à l'échelle d'importants sites industriels (analyse de sécurité du complexe pétrochimique de Canvey Island, 1978 et 1981) que pour l'étude de la sécurité d'utilisation de produits industriels comme les aéronefs (Wanner, 1969).

1.2. Les facteurs de développement

La sécurité des systèmes s'est progressivement constituée comme discipline selon une logique propre de conception et d'amélioration progressive d'outils d'analyse, conçus à l'origine pour améliorer la fiabilité de fonctionnement de systèmes techniques complexes et porteurs de risques élevés pour la sécurité des personnes.

Le développement et la diffusion de ces méthodes et techniques nouvelles ont en outre été renforcés par l'évolution prise par une industrie génératrice de risques de plus en plus importants et à l'origine d'accidents majeurs.

La figure 1 présente schématiquement les différents éléments qui contribuent à rendre compte de l'importance prise actuellement par les méthodes de sécurité des systèmes.

Outre les facteurs d'origine essentiellement historique (technologies complexes et peu fiables, outils disponibles) déjà évoqués au paragraphe précédent, deux autres données doivent être prises en considération :

– l'impact des catastrophes industrielles,

– le développement des grands sites industriels.

1.2.1. Les catastrophes industrielles

Les catastrophes industrielles (Feyzin, Flixborough, Three Mile Island, etc.) contribuent indéniablement à favoriser le développement de méthodes d'analyse prévisionnelle des risques. Les pertes humaines et matérielles consécutives à ces accidents entraînent en effet des conséquences sociales (inacceptabilité du risque majeur) et économiques (exigences de sécurité accrues de la part des compagnies d'assurance) qui nécessitent de trouver rapidement des solutions efficaces. L'élaboration de la

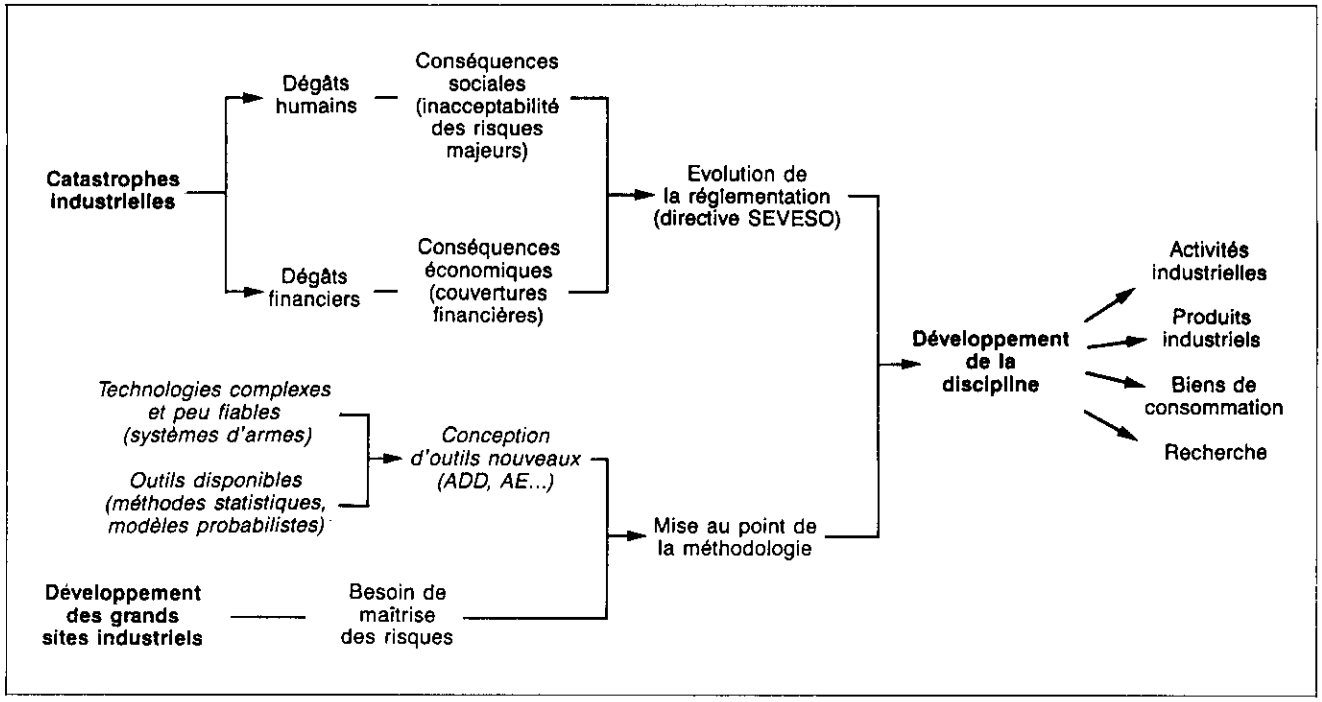


Fig. 1. Facteurs de développement de la sécurité des systèmes – *Safety system factors of expansion*
ADD = arbre des défauts – Fault tree; AE = arbre d'événements – Event tree

directive européenne Seveso ([5]) et pour la France de la loi sur les « installations classées » ([6]) constituent des réponses réglementaires qui, bien que formulant des obligations de résultats et non de moyens, conduisent les industriels à rechercher et à adopter des procédures efficaces d'analyse des risques.

Les méthodes issues de la sécurité des systèmes peuvent alors répondre à leurs attentes.

1.2.2. Le développement des grands sites industriels

Il induit des risques importants, notamment par suite des énergies mises en jeu (nucléaire, chimie). En outre, l'accélération de l'évolution des techniques réduisant de plus en plus l'expérience acquise, des risques nouveaux et mal connus apparaissent (émission de produits nocifs par exemple). Ce manque ou même cette absence d'expérience fait naître le besoin de concevoir ou de développer des outils qui permettent de maîtriser le risque de façon prévisionnelle.

Les méthodes existantes, expérimentées dans des secteurs très spécialisés ou de « pointe » (armement, nucléaire), mobilisent l'intérêt d'autres secteurs industriels (chimie et pétrochimie par exemple). Le plus souvent, les responsables devront adapter ces outils à leurs besoins et à leurs possibilités, notamment économiques. Ainsi, la mise en œuvre des méthodes de sécurité des systèmes pour des besoins industriels très diversifiés reste souvent relativement éloignée de la procédure lourde et complexe qui est appliquée dans les domaines spécifiques de l'armement, du nucléaire ou encore de l'aéronautique.

([5]) La directive Seveso du 24 juin 1982 fait obligation aux états membres de la Communauté européenne de prendre toutes mesures nécessaires pour que les responsables de certaines activités industrielles (sont notamment exclues les installations nucléaires et militaires) puissent prouver qu'ils ont déterminé « les risques d'accidents majeurs existants, pris les mesures de sécurité appropriées et informé, formé et équipé, afin d'assurer leur sécurité, les personnes qui travaillent sur le site » (article 4 de la directive).

([6]) En France, c'est au moyen de la législation sur les « installations classées » (loi du 19 juillet 1976 et décret d'application du 21 septembre 1977) que cette directive s'applique. Cette législation soumet les installations « pouvant présenter des dangers ou des inconvénients soit pour la commodité du voisinage, soit pour la santé, la sécurité, la salubrité publiques... » à autorisation ou déclaration » suivant la gravité des dangers ou inconvénients que peut présenter leur exploitation » (concernant les installations classées, voir Ferauge (1984) et Charbonneau (1987)).

2. MISE EN ŒUVRE

2.1. Critères pour la définition du « seuil de risque acceptable »

L'objectif fondamental d'une étude de sécurité des systèmes est l'atteinte d'un niveau de sécurité jugé satisfaisant. Il repose par conséquent sur une comparaison entre un niveau de sécurité évalué et un niveau de sécurité normatif.

La définition d'une norme de sécurité pour un système technique complexe (une exploitation industrielle) est concrétisée par une mesure de risque maximal admissible d'accident, mesure qui doit faire l'objet d'un certain consensus préalable.

2.1.1. Définition formelle du risque

La notion de risque (qu'il s'agisse de risques d'atteinte de l'outil d'exploitation, de l'environnement ou des individus) est caractérisée par un couple « probabilité d'occurrence/gravité des conséquences » appliqué à un événement redouté.

D'un point de vue théorique, une courbe d'acceptabilité du risque peut alors être définie (fig. 2).

Cette courbe permet de distinguer le risque acceptable et non acceptable. Un événement redouté peut ainsi être représenté à l'aide d'un point défini par les deux coordonnées de « probabilité » (axe des X) et de « gravité » (axe des Y) : l'événement A, aux conséquences graves mais peu probables, représenterait un risque acceptable ; à l'inverse, l'événement B de gravité moindre mais plus probable, correspondrait à un risque jugé inacceptable (7).

Cette représentation du risque soulève deux questions :

– comment évaluer la probabilité d'occurrence d'un événement ?

– quels sont les critères permettant de délimiter la « frontière de l'acceptable » ?

2.1.2. Probabilité d'occurrence d'un événement

Elle est généralement évaluée à partir d'estimations statistiques. Ainsi pour déterminer la probabilité de défaillance d'un composant simple (une pièce mécanique ou électronique par exemple), il est possible de recourir à des données statistiques issues d'essais effectués en laboratoire ou établies à partir des acquis de l'expérience (données d'utilisation opérationnelle). A tel composant électronique sera par exemple attribuée une probabilité de panne de 1/1000e par heure (10^{-3}/h).

Les difficultés surviennent lorsqu'il s'agit d'évaluer des probabilités très faibles, autrement dit inaccessibles à l'exploitation statistique. Les évaluations pourront par exemple se fonder non plus sur la fiabilité d'un élément mais, ainsi que le suggère Lievens (1976), sur la fiabilité d'une méthode (8). Mais, d'une façon générale, il est certain que lorsque l'on fait référence à des événements indésirables très rares (critère de probabilité), les évaluations peuvent être entachées d'une grande incertitude, due en particulier à l'arbitraire des scénarios imaginés et au cumul des marges d'erreurs.

Ce constat vaut aussi pour les accidents très graves (critère de gravité), pour lesquels il est malaisé d'évaluer par anticipation les conséquences financières et sociales.

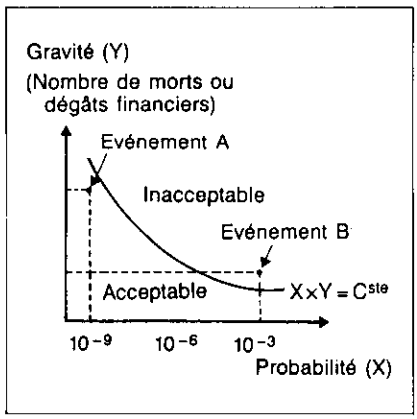


Fig. 2. Courbe d'acceptabilité du risque – *Curve of risk acceptability*

(7) Le produit « gravité x probabilité » n'est constant que d'un point de vue théorique (valeurs inversement proportionnelles caractérisant le tracé de l'hyperbole équilatère, de la forme Y = a/X). Il serait cependant nécessaire de se demander si l'événement B sur la figure 2, événement dont la gravité et la rareté ne sont pas extrêmes, concerne réellement la sécurité des systèmes.

(8) « Ainsi, le nombre total des heures de vol effectuées par l'ensemble de tous les avions permet de dire que la méthode de dimensionnement des longerons de voilure est suffisamment fiable pour qu'on évalue la probabilité de rupture de cet élément à moins de 10^{-9}/h » (Lievens, op cit., p. 53).

2.1.3. Délimitation des « frontières de l'acceptable »

Elle résulte d'une décision à caractère politique. Certaines considérations peuvent cependant apporter leur contribution à la fixation de ce seuil. Les deux méthodes d'évaluation habituellement évoquées pour fonder des décisions et les justifier si besoin sont les suivantes :

a) l'évaluation à partir du coût de la vie humaine. Elle conduit à traduire en termes monétaires les avantages tirés d'une réduction du risque. Cette méthode d'évaluation (par exemple en actualisant le total des gains nets futurs des individus, valeur reflétant leur contribution au produit national) permettra d'allouer des ressources de telle sorte qu'étant données les contraintes budgétaires, on maximise le nombre de vies sauvées ;

b) l'évaluation à partir d'une comparaison des différents risques déjà « acceptés ». Elle concerne non plus des coûts mais des niveaux de risque.

> A notre connaissance, le premier travail d'importance qui ait été consacré à de telles questions est celui de Starr (1969).
>
> Cet auteur distingue deux types d'activités :
>
> – les activités volontaires. Ce sont celles pour lesquelles un individu fait usage de son échelle de valeur propre pour prendre des décisions (ex. la consommation de tabac) ;
>
> – les activités involontaires. Il s'agit d'activités dont le choix, le contrôle ou la maîtrise échappent généralement à l'individu. Elles doivent par conséquent être considérées comme imposées par la société (ex. l'utilisation de l'électricité).
>
> Il a d'autre part évalué l'« avantage annuel moyen » procuré par ces diverses activités :
>
> – pour les activités volontaires, l'avantage est mesuré au moyen des sommes que l'individu est disposé à dépenser pour chacune de ces activités ;
>
> – l'avantage associé aux activités involontaires (imposées) correspond à la contribution de chacune d'elles au revenu annuel moyen par individu.
>
> Enfin, Starr a établi une corrélation entre la « probabilité d'accident

mortel par heure d'exposition » et cet « avantage annuel moyen ».

Les résultats obtenus ont conduit l'auteur à proposer les deux interprétations suivantes :

1) pour un avantage équivalent, les individus acceptent un risque environ mille fois plus élevé lorsqu'il résulte d'une activité volontaire que lorsqu'il est lié à une activité involontaire ;

2) pour chaque catégorie d'activité, le risque croît beaucoup plus vite que l'avantage associé. Ainsi, un avantage économique doublé entraînera un risque huit fois plus élevé (9).

Ce travail montrerait en outre que la probabilité moyenne de décès par maladie (environ 10^{-7} par personne et par heure) constitue une valeur limite d'acceptabilité du risque. Cette valeur est en effet souvent utilisée dans la pratique comme une limite inférieure à l'acceptation de la probabilité d'occurrence d'une situation très grave.

2.1.4. Représentation des objectifs de sécurité

Les niveaux de probabilité et de gravité caractérisant les différents seuils de risques sont rarement représentés de façon continue. Les praticiens définissent plutôt des classes pour chaque niveau.

Voici pour illustration les seuils arrêtés dans le domaine de l'aéronautique civile (Lievens, op. cit.) :

Classes de gravité

– Conséquences *mineures* : il n'y a ni dégradation sensible des performances du système, ni interruption de la mission, ni blessure de personnes, ni endommagement notable des biens ou du système.

– Conséquences *significatives* : il y a dégradation sensible des performances du système, pouvant entraîner l'interruption de la mission. Mais il n'y a ni blessure de personnes, ni endommagement notable des biens ou du système.

– Conséquences *critiques* : il peut y avoir blessure de personnes et/ou endommagement notable des biens ou du système.

– Conséquences *catastrophiques* : il y a destruction du système et/ou plusieurs blessés graves et/ou mort de personnes.

Classes de probabilité

– Evénement fréquent : événement dont la probabilité d'apparition est supérieure à 10^{-3} par heure.

– Evénement peu fréquent : événement dont la probabilité d'apparition est comprise entre 10^{-5} et 10^{-3} par heure.

– Evénement rare : événement dont la probabilité d'apparition est comprise entre 10^{-7} et 10^{-5} par heure.

– Evénement extrêmement rare : événement dont la probabilité d'apparition est comprise entre 10^{-9} et 10^{-7} par heure.

– Evénement extrêmement improbable : événement dont la probabilité d'apparition est inférieure à 10^{-9} par heure.

Les objectifs globaux de sécurité relatifs à un système peuvent être exprimés par une grille du type présenté au tableau I. Des grilles plus simples d'évaluation du risque (elles ne font pas appel à la notion de probabilité quantifiée) sont aussi souvent utilisées. L'Union des industries chimiques (UIC) en propose une dans son « cahier de sécurité n° 4 » (cf. § 3.2).

2.2. Démarches « inductive » et « déductive »

L'application des méthodes de sécurité des systèmes fait appel aux raisonnements par induction et par déduction. Cette terminologie désigne deux procédures complémentaires d'identification et d'analyse du risque, qui s'expriment concrètement par l'utilisation de techniques particulières. Les plus connues sont l'« analyse des modes de défaillance et de leurs effets » (AMDE) pour la démarche inductive et l'« analyse par arbre des défauts » (ADD) pour la démarche déductive.

2.2.1. Démarche inductive

Elle consiste à représenter les différentes séquences d'événements susceptibles de conduire, à partir de causes identifiées au préalable, à un ou plusieurs effets préjudiciables au système. La démarche inductive

TABLEAU I

Objectifs globaux de sécurité (Lievens, 1976) – Overall safety goals

Probabilités / Conséquences	10^{-5}/h	10^{-7}/h	10^{-9}/h (*)	
	Fréquent ou peu fréquent	**Rare**	**Extrêmement rare**	**Extrêmement improbable**
Mineures ou significatives				
Critiques				
Catastrophiques				

(*) Les probabilités d'occurrence, de la forme 10 ^{a}/h signifient « par heure d'exposition aux risques générés par le système ».

(9) Villemeur (1988) observe cependant que « l'étude des relations entre les risques et les bénéfices escomptés (l'« avantage annuel moyen ») a donné lieu à de nombreuses discussions compte tenu des difficultés à apprécier le bénéfice escompté » (p. 524).

« descend » des causes vers les effets. Elle est aussi appelée *méthode directe*, expression qui traduit bien le sens de l'investigation (des causes vers les effets).

2.2.2. Démarche déductive

Elle consiste à remonter aux causes premières de défaillances données a priori, en reconstituant le déroulement des événements susceptibles de conduire à ces défailiances. La démarche déductive « remonte » des effets vers les causes, ce qui justifie l'appellation équivalente de *méthode inverse*.

2.2.3. Spécificité et complémentarité des deux démarches

Il est intéressant de remarquer que, contrairement à la démarche inductive qui caractérise de nombreuses méthodes d'analyses (AMDE, mais aussi analyse préliminaire des risques, analyse par arbre d'événements, etc.), la démarche déductive est généralement associée à une seule méthode, l'analyse par arbre des défauts [10].

En réalité, cette dernière n'a pas l'exclusivité de la démarche déductive. « Aucune des méthodes dites inductives n'est exclusivement inductive ; la démarche déductive, naturelle à toute personne qui connaît la finalité de son travail, n'en est jamais absente » (Lievens, op. cit., p. 262).

Les expressions « méthodes inductives » et « méthodes déductives », couramment utilisées, sont commodes car elles permettent de faire une distinction entre deux procédures d'analyse d'un système technique : progression du général vers le particulier et inversement.

Mais dans les faits, un examen plus attentif des critères permettant d'effectuer cette distinction conduit à mettre en évidence une ambiguïté concernant ce qui est réellement désigné : *le mode de raisonnement intrinsèque à chaque méthode ou le mode d'examen du système technique.*

Par exemple, un arbre d'événements (cf. § 3.3) et un arbre des défauts (cf. § 3.4) nécessitent tous deux un mode de raisonnement déductif (étant donné l'état du système à un niveau ou à un instant particulier, en déduire l'état suivant). Par contre, le mode d'examen du système sera inductif dans le premier cas (progression des événements élémentaires vers les événements finaux indésirables), déductif dans le second cas (progression inverse). D'autre part, les logiques utilisées sont elles aussi différentes (logiques binaire et booléenne).

La figure 3 resitue les deux démarches par rapport au mode d'analyse du système et au déroulement des événements dans le temps.

La méthode inductive (ou « directe »), qui part des événements primaires et conduit à identifier des événements indésirables, est « en phase » avec le déroulement virtuel de ces événements [11]. Au contraire, la méthode déductive (ou « inverse »), qui reconstitue la logique des enchaînements entre événements primaires et événements indésirables, est « en opposition de phase » par rapport au déroulement dans le temps.

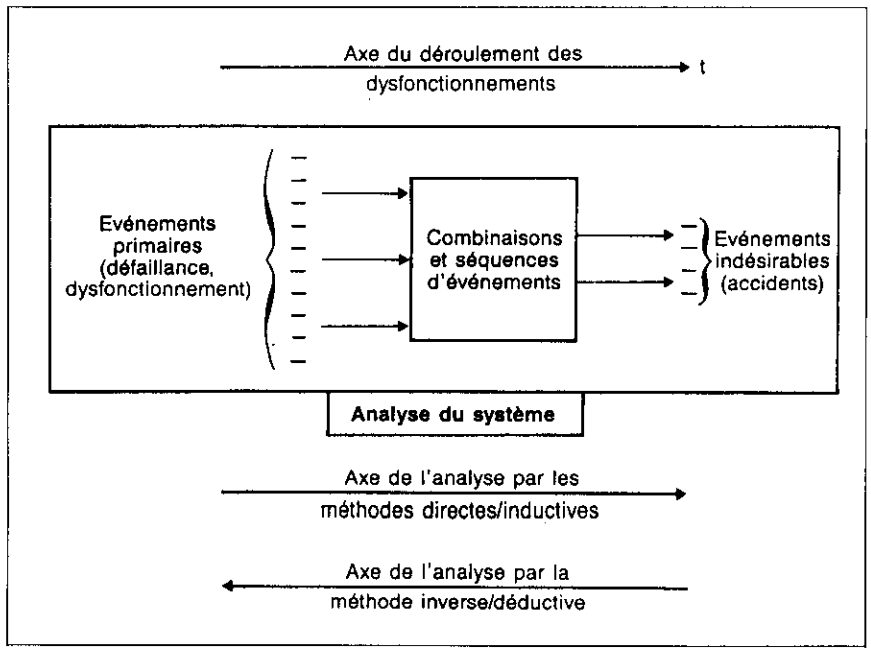


Fig. 3. Rapprochement entre l'axe du déroulement des événements et les deux modes d'analyse du système – *Parallels between the course of events and both system analysis modes*

[10] Le principe de l'ADD est le suivant : « à partir d'un événement indésirable, unique et bien défini, *(l'ADD consiste)* à identifier et à représenter logiquement les combinaisons d'événements primaires qui conduisent à la réalisation de l'événement indésirable » (Signoret et Leroy, 1986, p. 1602) (cf. exposé sur l'ADD au § 3.4).

[11] Cette caractéristique permet d'effectuer des simulations de dysfonctionnements pour des dispositifs techniques divers : études de sécurité des circuits de commande, étude des barrages immatériels, sécurité des systèmes à logique programmée, etc. (cf. par exemple Schweitzer et Gérardin, 1984).

2.3. Etapes principales d'une étude

La mise en œuvre d'une étude de sécurité d'un système comprend quatre phases principales (d'après Signoret et Leroy, 1986) ([12]) :

1) définitition du système étudié,

2) identification des risques présentés par le système,

3) modélisation de la logique de fonctionnement et des défaillances du système,

4) analyse qualitative et quantitative.

2.3.1. Définition du système étudié

Connaissance du système

Elle nécessite de réunir de la documentation concernant les objectifs de production et de sécurité, la réglementation en vigueur, la technicité (schémas de principe, plans détaillés, explications de spécialistes).

Description de l'environnement du système, spécialement en ce qui concerne les échanges avec l'extérieur (flux de matières premières et de produits finis).

Connaissance des objectifs de sécurité que le système doit respecter : définition de l'utilisation anormale (conditions d'emploi hors spécification) ([13]), apport d'informations concernant les événements redoutés pour le système, etc.

2.3.2. Identification des risques présentés par le système

La connaissance des risques par les spécialistes est rarement exhaustive (Signoret et Leroy, op. cit.) et ceci d'autant plus que le système technique considéré est nouveau ou très complexe. Des méthodes ont par conséquent été développées, qui permettent une identification plus systématique de ces risques. Les plus connues sont :

– l'analyse préliminaire des risques (Preliminary hazard analysis),

– l'analyse des modes de défaillance et de leurs effets (Failure modes and effect analysis),

– l'analyse par arbre d'événements (Event tree analysis).

Ces trois méthodes font l'objet d'une présentation détaillée au chapitre 3.

2.3.3. Modélisation de la logique de fonctionnement et des défaillances du système

La mise en œuvre de méthodes inductives pour l'identification des risques conduit à sélectionner parmi ces derniers les plus dommageables pour le système.

L'examen spécifique des risques les plus importants fait essentiellement appel à une démarche déductive qui permet de reconstituer les séquences d'événements virtuellement en cause dans l'apparition des dysfonctionnements redoutés. « Il s'agit alors d'établir un modèle représentant correctement les liaisons de causalité entre chacun de ces derniers et des événements primaires (défaillance d'un composant, événement extérieur, etc.) » (Signoret et Leroy, op. cit., p. 1602).

La méthode de représentation la plus utilisée est celle de l'arbre des défauts (Fault tree analysis), dont l'historique a été évoqué au § 1.1 (elle fait d'autre part l'objet d'une présentation détaillée au § 3.4).

2.3.4. Analyse qualitative et quantitative

Cette dernière étape « consiste à évaluer, à partir des modèles, la probabilité de matérialisation des risques envisagés » (Signoret et Leroy, op. cit., p. 1599). Analyse qualitative (classement des événements indésirables en fonction de leur importance relative, de leur modalité d'apparition, etc.) ou quantitative (attribution de probabilités d'occurrence pour chacun de ces mêmes événements) conduisent toutes deux à évaluer le niveau de risque inhérent au système.

Les résultats obtenus constitueront une aide précieuse lors de la décision de procéder si nécessaire à des modifications du système pour l'amélioration de la sécurité.

Les auteurs indiquent en outre que l'analyse de risque permet aux responsables d'un projet, et ceci dès la phase de conception, sinon de supprimer les risques présentés par une installation, « du moins de les prévoir, afin de minimiser les conséquences en modifiant les caractéristiques initialement prévues pour le système » (Signoret et Leroy, op. cit., p. 1599).

Cette remarque est importante car elle met l'accent sur l'intérêt présenté par une étude de sécurité des systèmes en phase de conception. En ce sens, les quatre étapes qui viennent d'être présentées décrivent en quelque sorte une démarche exhaustive et idéale. Dans la pratique, on imagine difficilement qu'une procédure aussi complexe puisse toujours convenir en cours d'exploitation d'un système technique, ceci pour d'évidentes raisons de faisabilité et de coût...

La figure 4 résume les différentes étapes présentées par les auteurs.

2.4. Principes et usages

L'expression « sécurité des systèmes » sert à désigner des applications extrêmement dissemblables, aussi bien quant aux objectifs retenus qu'en ce qui concerne les moyens (techniques, humains, financiers) engagés. Qu'y a-t-il en effet de commun entre une étude de sécurité des systèmes appliquée d'une part à un grand complexe industriel et d'autre part à un circuit de commande de machine-outil ?

([12]) De nombreux auteurs proposent une description des étapes de mise en œuvre d'une étude de sécurité des systèmes (Barbet et Guyonnet, 1984 ; Sutter et Tröxler, 1987). La démarche présentée par Signoret et Leroy (1986) a été choisie car elle résume assez bien l'essentiel des positions.

([13]) Cet aspect pose en particulier des problèmes de répartition des responsabilités en cas de dysfonctionnement ou de destruction du système (pour information, cf. Deschanels et Lavedrine, 1984). Ajoutons que les spécifications relatives à la maintenance peuvent engager directement la sécurité. L'exemple rapporté dans le cadre d'un travail collectif consacré aux « accidents technologiques » (CNPP-AFNOR, 1988) est à cet égard illustratif. Il concerne l'accident survenu à Chicago, en 1979. Un avion qui décollait a perdu un de ses réacteurs, s'est déséquilibré et écrasé en bout de piste. « L'enquête a découvert pourquoi la liaison entre aile et « mât » avait lâché. Cette liaison travaille beaucoup, ce qui impose de la démonter, vérifier et remonter périodiquement. La procédure prévue par le constructeur est de désassembler d'abord le moteur du mât, puis le mât de l'aile, et inversement au remontage. Mais l'exploitant avait décidé, dans un but d'économie, de ne pas désassembler mât et moteur. De la sorte, il détachait de l'aile, puis y refixait, une masse de 7 tonnes au lieu de 600 kg ; une erreur de manœuvre quelconque a dû déformer l'aile (pièce légère et souple), ce qui a rendu la liaison fragile » (p. 44).

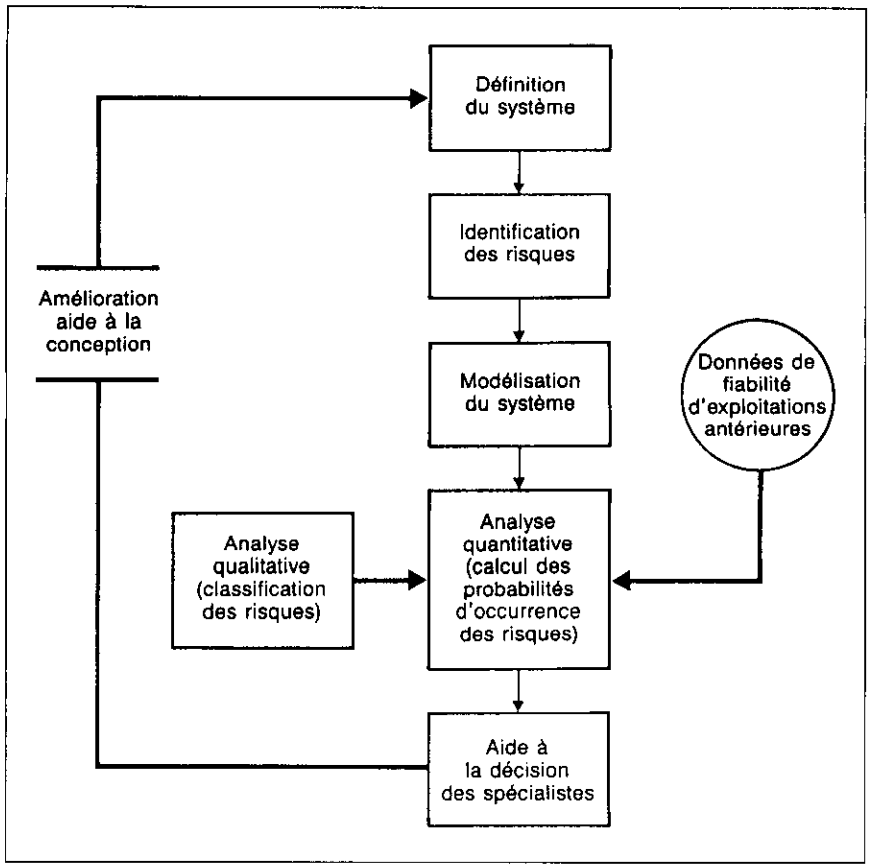


Fig. 4. Étapes de la sécurité des systèmes (Signoret et Leroy, 1986) – *Stages for safety system*

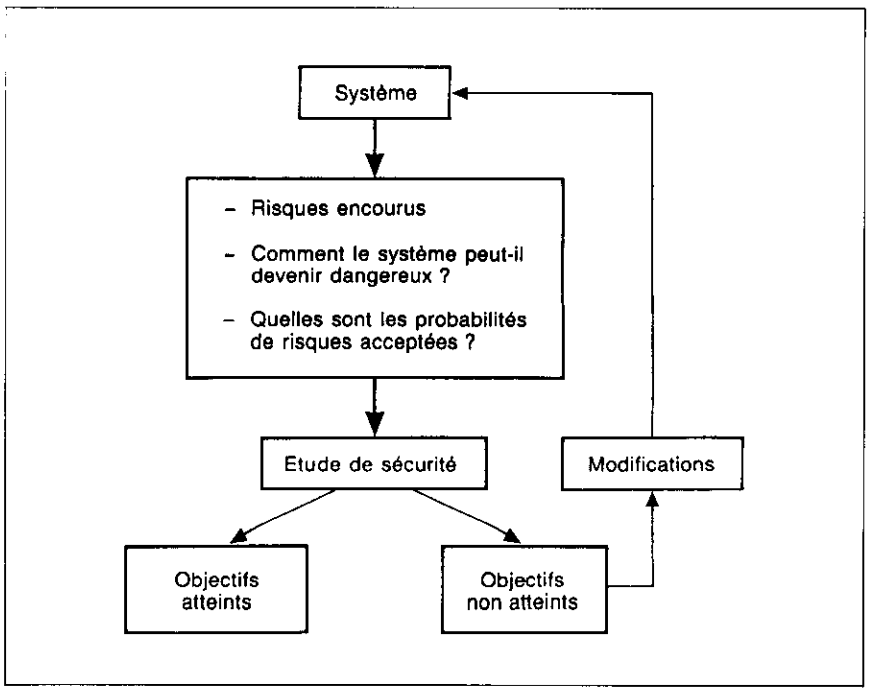


Fig. 5. Etapes pour l'étude de la sécurité appliquée à un système de missile embarqué (Louet et Barrault, 1986) – *Stages for the study of safety applied on an aboard missile device*

Trois remarques apporteront une nuance de réalisme à propos de la mise en œuvre de la méthode.

2.4.1. Respect des objectifs fondamentaux

L'examen comparatif entre le risque acceptable et le risque évalué ne caractérise le plus souvent que certaines études très poussées, concernant soit des activités industrielles qui comportent des risques très importants pour les populations (problème du risque technologique majeur), soit des secteurs d'activités privilégiés (budgets importants, concurrence faible ou absente, recherche très développée, etc.) et de haute technicité.

Les systèmes d'armes sont illustratifs de ce dernier point. Par exemple, Louet et Barrault (1986) présentent une étude de sécurité appliquée à un système de missile embarqué à bord de sous-marins. Cette étude respecte parfaitement les principes de base de la sécurité des systèmes : examen comparatif entre risques acceptés et risques évalués et décision (fig. 5).

2.4.2. Nature du système étudié

La plupart des études concernent des systèmes fermés plus ou moins complexes et non pas des systèmes ouverts sur l'environnement. Les systèmes fermés comportent peu d'échanges ou seulement des échanges simples avec l'extérieur (sous forme d'information ou d'énergie). Ils sont peu aptes à réagir aux perturbations extérieures et a fortiori inaptes à modifier leurs comportements en fonction des circonstances : l'essentiel des mécanismes techniques traditionnels de l'industrie entrent dans cette catégorie. Motivées le plus souvent par des préoccupations de prévention générale, c'est-à-dire limitées à la sécurité des personnels de l'industrie, ces études utilisent toutefois les méthodes d'analyse (AMDE et ADD surtout) développées dans le cadre de la sécurité des systèmes [14].

[14] Pour une présentation générale de la sécurité des systèmes appliquée plus particulièrement aux systèmes fermés (sécurité des machines), cf. Ho (1976).

L'expression désigne alors plus l'utilisation d'outils que la mise en œuvre d'une méthodologie à proprement parler. Dans ce contexte, les analyses restent en général qualitatives ou semi-quantitatives pour certaines applications.

2.4.3. Critères de choix des méthodes

Le paragraphe 2.2 a donné l'occasion de nuancer la distinction formelle entre procédures inductive et déductive. Lievens (op. cit.) considère d'autre part que le choix des méthodes dépend aussi du degré de connaissance du système étudié. Par exemple, au terme d'une comparaison entre méthodes déductives et inductives, il distingue certaines d'entre elles en fonction d'un critère d'expérience acquise sur les risques.

En somme, la distinction rationnelle entre outils inductifs et déductifs s'efface en partie au profit de considérations plus empiriques, même si elle reste par ailleurs consacrée par l'usage.

3. DESCRIPTION DES PRINCIPALES METHODES

La réalisation d'une étude de sécurité des systèmes fait appel à différents outils d'analyse, très diversifiés quant à leurs performances, leur domaine d'application et leur complexité. Seules, les caractéristiques essentielles des méthodes les plus utilisées ainsi que les critères qui permettent de les distinguer (critères techniques et d'usage) seront présentés ici ([15]).

Les quatre méthodes suivantes seront examinées : analyse préliminaire des risques (Preliminary hazard analysis), analyse des modes de défaillance et de leurs effets (Failure modes and effect analysis), analyse par arbre d'événements (Event tree analysis), analyse par arbre des défauts (Fault tree analysis).

3.1. L'analyse préliminaire des risques (APR)

3.1.1. Présentation

L'APR a pour objet d'identifier les risques présentés par un système et, par suite, « de définir des règles de conception et des procédures permettant d'éliminer ou de maîtriser les situations dangereuses et les accidents potentiels ainsi mis en évidence » (Lievens, op. cit., p. 124) ([16]).

C'est donc essentiellement au stade de la conception (et, d'après l'auteur, lorsque le système fait intervenir des technologies mal connues) que ce type d'analyse présente le plus d'intérêt. L'APR doit par conséquent être remise à jour périodiquement : durant la phase de conception et de développement puis, ultérieurement, au cours de l'exploitation industrielle.

La description des résultats obtenus s'effectue au moyen de divers modes de présentation :

- tableaux à colonnes,
- arbres logiques,
- éventuellement, sous forme de documents plus synthétiques (type « documents récapitulatifs »).

3.1.2. Tableaux à colonnes

Ils permettent d'ordonner les informations utiles en fonction de notions prédéfinies.

> La liste suivante d'intitulés pour chaque colonne peut être proposée (Lievens, op. cit.).
>
> 1) *Sous-système ou fonction :* identification de l'ensemble étudié, qu'il s'agisse d'un sous-système ou d'un ensemble fonctionnel.
>
> 2) *Phase :* identification des phases ou des modes d'utilisation du système pendant lesquels certains éléments de l'ensemble étudié peuvent générer un risque.
>
> 3) *Eléments dangereux :* identification des éléments du sous-système ou de l'ensemble fonctionnel auxquels on peut associer un danger intrinsèque.
>
> 4) *Evénement causant une situation dangereuse :* identification de conditions, événements indésirables, pannes ou erreurs qui peuvent transformer un élément dangereux en situation dangereuse.
>
> 5) *Situation dangereuse :* identification des situations dangereuses, résultant de l'interaction de l'élément dangereux et de l'ensemble du système, à la suite d'un événement décrit en 4).
>
> 6) *Evénement causant un accident potentiel :* identification des conditions, événements indésirables, pannes ou erreurs qui peuvent transformer une situation dangereuse en accident.
>
> 7) *Accident potentiel :* identification des possibilités d'accidents résultant des situations dangereuses à la suite d'un événement décrit en 6).
>
> 8) *Conséquences :* identification des conséquences attachées aux accidents potentiels, lorsque ceux-ci se produisent.
>
> 9) *Classification par gravité :* mesure qualitative de la gravité des conséquences précédentes, dans le cadre de la classification de la norme MIL. STD 882 : mineur, significatif, critique, catastrophique (cf. § 2.1).
>
> 10) *Mesures préventives :* recensement des mesures proposées pour éliminer ou maîtriser les risques ainsi identifiés (situations dangereuses ou accidents potentiels).
>
> 11) *Application de ces mesures :* recueil d'informations touchant :
>
> - l'efficacité des mesures précédentes,
> - leur introduction dans le système ou ses procédures d'utilisation.
>
> Ce tableau est rempli par un spécialiste possédant une bonne connaissance du système, en tenant compte des relations dynamiques existant entre les différentes étapes de l'analyse.

([15]) Pour une présentation détaillée (et technique) de l'ensemble des méthodes actuellement opérationnelles, cf. Villemeur (1988).

([16]) Différentes méthodes actuellement en usage ont un objectif comparable. Voir par exemple la méthode HAZOP, présentée dans la 1re partie de ce bilan sur les méthodes d'analyse prévisionnelle des risques (note documentaire ND 1768-138-90).

Ainsi, pour qu'un *élément dangereux* (col. 3), par exemple une machine tournante, entraîne une *situation dangereuse* (col. 5), certaines conditions doivent être remplies, par exemple apparition de vibrations intempestives (« l'événement » de la col. 4).

De même, une *situation dangereuse* ne conduit pas nécessairement à l'*accident potentiel* (col. 7). Un autre événement ou une condition supplémentaire (col. 6) devra se manifester, par exemple la proximité d'un opérateur. L'auteur précise à ce propos que l'*application conjointe des démarches inductive et déductive* s'impose naturellement lorsque l'analyste s'efforce d'identifier des situations dangereuses, c'est-à-dire lorsqu'il se demande de quelle façon les éléments dangereux peuvent conduire à un accident potentiel.

La distinction proposée entre « éléments dangereux », « situation dangereuse » et « accident potentiel » renvoie implicitement à une certaine conception de l'accident, qui peut être représentée de façon schématique (fig. 6).

Cette figuration du processus conduisant à l'accident (potentiel) présente une certaine valeur heuristique (aide à la conceptualisation). Elle constitue en effet un guide utile pour l'analyste dans sa tâche de décomposition du système, en vue de mettre en évidence les risques inhérents à celui-ci.

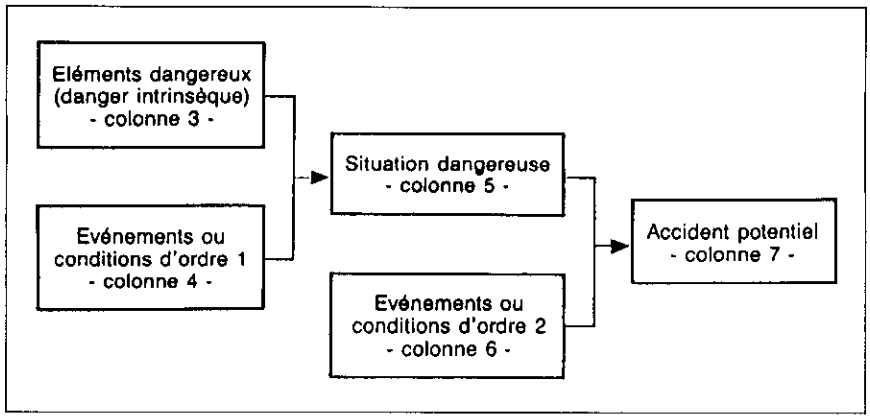


Fig. 6. Modèle de l'accident implicite à l'analyse préliminaire des risques – *Tacit accident model for the preliminary hazard analysis*

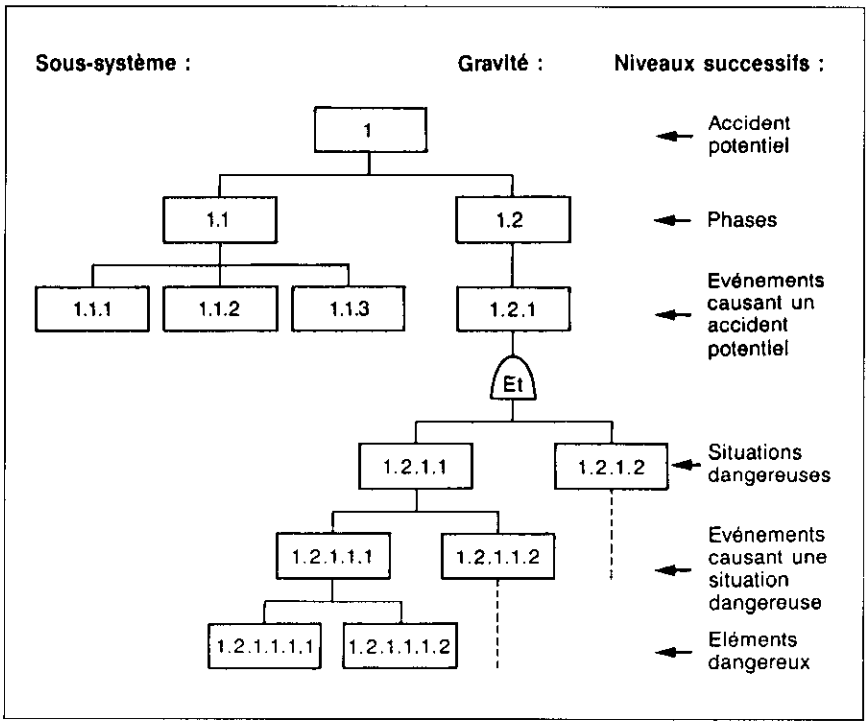


Fig. 7. Présentation sous forme d'arbre logique des données issues de l'analyse préliminaire des risques (Lievens, 1976) – *Logical tree shaped data from preliminary hazard analysis*

3.1.3. Arbres logiques

Une présentation différente des données issues de l'APR peut être obtenue en utilisant une structure de type arborescent (fig. 7).

Pour chaque sous-système étudié, comprenant mention de la gravité des conséquences en cas d'accident, cet arbre décompose l'enchaînement des circonstances qui conduisent à l'événement indésirable. Les notions utilisées restent inchangées par rapport à la présentation sous forme de tableaux. Seul diffère l'aspect, qui présente l'intérêt de mieux montrer l'enchaînement des causalités.

3.1.4. Autre mode de description

L'Union des industries chimiques (cahier n° 1, 1981) propose une utilisation de l'APR fondée sur la distinction entre les produits et les procédés (17).

Des « fiches produits » et des « fiches procédés » (tableau II) permettent à l'analyste de prendre en compte systématiquement et selon le contexte

(17) Distinction particulièrement adaptée à l'industrie chimique que l'UIC représente (concernant l'analyse des risques dans les procédés chimiques, cf. aussi Abribat et coll., 1988).

TABLEAU II

Fiche produit et fiche procédé préconisées par l'UIC (extrait des rubriques principales) – Products and processes sheets advocated by the Chemical Industries Union (extract of the main headings)

Fiche produit	
1	Propriétés
2	Solubilités
3	Chaleur spécifique
4	Combustion
5	Agents extincteurs
	etc.
Fiche procédé	
1	Équation de la réaction principale et des réactions secondaires
2	Conditions opératoires
3	Risques
4	Dispositifs
5	Moyens de prévention de la contamination
	etc.

l'ensemble des données concernant la sécurité. Au moyen d'un système d'indexation, ces fiches donnent accès à un dossier de sécurité qui regroupe l'ensemble des informations répondant à chaque rubrique.

3.2. L'analyse des modes de défaillance et de leurs effets (AMDE)

3.2.1. Présentation

L'AMDE est l'outil d'analyse le plus utilisé et l'un des plus efficaces parmi l'ensemble des techniques inductives disponibles. Lievens (op. cit., p. 130-131) précise qu'il s'agit « d'une procédure très utilisée en fiabilité pour :

– analyser les conséquences des défaillances qui peuvent affecter un équipement ou un système,

– identifier les pannes ayant des conséquences importantes quant à différents critères tels que : réussite des missions, disponibilité, charges de maintenance, sécurité, etc. ».

L'application de l'outil à des fins de sécurité résulte de travaux effectués par divers auteurs et firmes (Compagnie McDonnell-Douglas en particulier) ([18]).

3.2.2. Mission principale et mise en œuvre de l'AMDE

La mission et la mise en œuvre peuvent être décrites en sept points :

– définition du système à étudier,

– identification des modes de défaillance,

– recherche des causes d'apparition des modes de défaillance,

– analyse des effets des défaillances,

– examen des possibilités de compensation des effets des défaillances,

– évaluation du risque associé à chaque mode de défaillance,

– proposition d'actions correctrices et de mesures préventives.

Définition du système à étudier

Cette démarche conduit à « décomposer le système en éléments ou composants, pour lesquels on dispose d'informations jugées suffisantes » (Barbet et Guyonnet, op. cit., p. 44).

L'étape est concrétisée le plus souvent au moyen d'un diagramme par blocs qui permet de mettre en évidence l'ensemble des fonctions devant être réalisées par le système.

Les auteurs précisent que le niveau de décomposition n'est pas définissable a priori : « il dépend du système à étudier, de l'ampleur de l'analyse à effectuer, des renseignements dont on dispose suivant la phase de la conception à laquelle on se situe » (op. cit., p. 44). Ce point est confirmé par Lievens (op. cit.), indiquant qu'il convient en pratique de choisir un niveau qui rende possible l'obtention de données suffisantes sur chaque mode de défaillance. Le choix du niveau de décomposition à partir duquel l'AMDE doit être effectuée est « affaire d'opportunité et non de principe » (p. 132).

Identification des modes de défaillance susceptibles de nuire au bon fonctionnement d'une installation

L'établissement des modes de défaillance revient à déterminer « l'effet par lequel une défaillance est observée » (Barbet et Guyonnet, op. cit., p. 44) ou, en d'autres termes, à se poser la question du « comment » : « comment les fonctions à exécuter peuvent-elles être affectées » (Lievens, op. cit., p. 132) ([19]).

L'UIC propose une autre définition de la notion de mode de défaillance (cahier nº 4, 1981) : « perturbation dans la fonction ou dans les performances d'un sous-système, assemblage, composant ». Cet organisme précise d'autre part qu'il est possible d'analyser le comportement d'un sous-système sous l'angle :

– des défaillances de fonction (ex. : fonctionnement prématuré, arrêt intempestif, etc.),

([18]) Cf. § 4.1 pour la distinction entre « fiabilité » et « sécurité ».

([19]) L'auteur (p. 133) propose de classer les modes de pannes en six catégories :

– *sortie bloquée à zéro (ou à un)* : c'est le cas de la rupture d'une connexion, de la panne d'un composant électronique en court-circuit (ou en circuit fermé) ;

– *sortie dégradée* : c'est le cas d'une perte de débit dans une canalisation hydraulique pouvant entraîner une moindre efficacité du refroidissement, un délai excessif de freinage, une lubrification insuffisante, etc. Les méthodes générales d'analyse des dérives peuvent être appliquées aux cas de sorties dégradées ;

– *pannes intermittentes* : on peut citer l'exemple d'un composant électronique de système logique dont la sortie oscille en permanence entre le niveau 0 et le niveau 1. Ces pannes sont parmi les plus difficiles à étudier, tant dans l'AMDE que dans toute analyse de sécurité ;

– *sortie excessive* : c'est le cas d'un liquide dont la température serait trop élevée à la suite d'une panne de thermostat ;

– *sortie intempestive* : c'est le cas d'une alarme qui retentit à un moment où elle n'aurait aucune raison de le faire ;

– *sortie indésirable* : on peut citer l'exemple d'un équipement électrique qui exécute les fonctions pour lesquelles il a été conçu, mais qui dégage une chaleur excessive et peut, de ce fait, compromettre le bon fonctionnement des équipements voisins.

– des défaillances de performance (ex. : pour un moteur d'entraînement, variations de vitesse, vibrations, étincelles, etc.).

Recherche des causes d'apparition des modes de défaillance

La recherche des causes possibles d'une défaillance s'effectue simultanément à l'identification des modes de défaillance (Damien, 1985, p. 50). Cet auteur, dont la démarche s'inspire de celle proposée par l'UIC, indique que les causes doivent être recherchées :

– sur le matériel (ex. : ruptures mécaniques et électriques, déformations, usure, grippage, etc.),

– sur les « entrées » (ex. : énergie, liaison depuis le composant précédent, lubrifiant, etc.).

Analyse des effets des défaillances

L'analyse des effets doit s'effectuer au cas par cas, après avoir énuméré les modes de défaillance (UIC). Cette étape distingue généralement :

• les effets locaux, par exemple :

– sous-système : entraînement par moteur,

– défaillance : déclenchement électrique,

– effet local : arrêt de l'entraînement ;

• les effets sur le système : « dans l'exemple précédent, si le moteur entraîne un agitateur, l'effet sur le système peut être une augmentation de température, voire un emballement de réaction. Si c'est une pompe, l'effet peut être une inversion de son sens de rotation » (exemples empruntés au cahier nº 4 de l'UIC).

Examen des possibilités de compensation des effets des défaillances

Damien (op. cit., p. 50) présente trois moyens de réduire l'effet des défaillances :

– réduction de la probabilité de défaillance (ex. : dispositifs de sécurité tels que clé de contact, procédures écrites, entretien préventif, etc.) ;

– réduction de la propagation de la défaillance (ex. : doublement des capteurs, alarmes, etc.) ;

– réduction de la gravité (ex. : trappe coupe-feu, écrans, etc.).

Evaluation du risque associé à chaque mode de défaillance

L'évaluation du risque s'effectue généralement à partir d'échelles de cotation de la gravité et de la probabilité ([20]) (échelle préalablement utilisée pour chaque mode de défaillance).

([20]) Sur la « mesure » du risque, cf. § 2.1.

A titre d'exemple, les échelles proposées par l'UIC sont les suivantes.

– Évaluation de la gravité. Les niveaux de gravité sont définis par les conséquences des défaillances ou défauts de fonctionnement d'un sous-système ou d'un composant, suivant l'échelle ci-dessous :

	Niveaux	
... n'entraînent ni accident de personne, ni dommage au système	1	Négligeable
... admettent des palliatifs ou des correctifs tels qu'il n'y ait ni accident de personne, ni dommage important occasionné au système	2	Marginal
... nécessitent la prise de mesures immédiates pour que la vie du personnel ne soit pas mise en danger et pour que le système ne subisse pas de dommage important	3	Sérieux
... entraînent des accidents graves dont les effets :		
- sont limités à l'atelier	4	Majeur
- sont limités à l'établissement	5	Idem
- dépassent les limites de l'établissement	6	Idem

– Évaluation de la probabilité : souvent il est difficile d'obtenir les probabilités des défaillances et on procède à une évaluation semi-quantitative. On classe les défaillances en 6 niveaux de probabilité :

	Niveaux	
Probabilité de défaillances extrêmement faible – éventualité d'apparition négligeable pendant l'intervalle de fonctionnement du système	1	Extrêmement rare
Probabilité de défaillance très faible	2	Très rare
Faible probabilité de défaillance	3	Rare
Possibilités de défaillance	4	Possible
Grande probabilité de défaillance	5	Fréquent
Très grande probabilité de défaillance	6	Très fréquent

L'évaluation du risque s'exprime au moyen d'un nombre de deux chiffres, par combinaison des niveaux de gravité et de probabilité préalablement définis (ex. : gravité 3, probabilité 2 → risque 32).

L'ensemble des résultats de l'analyse est ensuite reporté sur une « grille critique », construite en portant les gravités en abscisses et les probabilités en ordonnées.

TABLEAU III

Grille d'évaluation du risque (exemple UIC) (la zone hachurée représente les risques jugés inacceptables) – Hazard assessment chart (hachured area shows hazards considered as unacceptable)

Probabilité						
6	16	26	36	46	56	66
5	15	25	35	45	55	65
4	14	24	34	44	54	64
3	13	23	33	43	53	63
2	12	22	32	42	52	62
1	11	21	31	41	51	61
	1	2	3	4	5	6

Gravité

A chaque case est attribué un nombre caractérisant le risque, nombre qui varie par conséquent de 11 (risque minimum) à 66 (risque maximum).

Il est important de remarquer ici que ce mode de représentation (hachurage) donne la priorité à la gravité sur la probabilité. Cette priorité s'exprime par le mode de lecture du nombre dans le sens colonne-ligne. Le tableau III (exemple UIC) permet ainsi de constater que l'on donne la priorité à la case 63 (événement « majeur » et « rare ») par rapport à la case 36 (événement « sérieux » et « très fréquent »).

En fonction des besoins et des possibilités, l'évaluation des risques peut aussi être envisagée d'une façon plus strictement quantitative, en considérant la probabilité d'occurrence de chaque mode de défaillance. L'analyse prend alors le nom d'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC).

Propositions d'actions correctrices et de mesures préventives pour l'élimination et la maîtrise des risques détectés

L'identification de situations susceptibles de dégénérer en accidents doit permettre de décider de l'acceptabilité ou non des risques correspondants. Dans cette dernière éventualité (risque inacceptable), l'étude devra conduire à effectuer des actions correctrices ou à proposer des mesures preventives.

1) Les actions correctrices conduiront par exemple à préciser les points suivants (Lievens, op. cit.) :

– alarmes existantes,

– connaissance d'autres défaillances qui déclenchent les mêmes alarmes,

– possibilité d'identification de la défaillance par les personnels chargés de la conduite et de la maintenance du système,

– actions correctrices immédiates, à long terme,

– paramètre à surveiller,

– etc.

2) Les mesures préventives doivent être recensées et faire l'objet d'une remise à jour périodique afin de contrôler leur efficacité dans le temps. Les mesures préventives, qualifiées par Lievens (op. cit.) de sécurité primaire (la sécurité secondaire et tertiaire concernant la maîtrise des conséquences des accidents), mettent en œuvre différentes techniques. A titre d'exemple, l'auteur distingue les mesures suivantes :

– élimination du risque (ex. : utilisation de matériaux non inflammables),

– limitation des paramètres dangereux (ex. : utilisation de la basse tension - 12/24 V - pour outils électriques manuels, suivi en continu et contrôle automatique des paramètres de fonctionnement critiques),

– dispositifs d'isolation, de blocage et d'interdiction (ex. : inertage des liquides inflammables, verrouillage des équipements électriques, fonctionnement du démarreur d'une automobile conditionné par le bouclage des ceintures de sécurité),

– sécurité après défaillance (fail-safe) (ex. : emploi des fusibles et disjoncteur),

– réduction des probabilités de pannes ou d'erreur (ex. : surdimensionnement des éléments importants, utilisation de redondances),

– récupération (ex. : nettoyage soigneux du sol après épandage accidentel d'un liquide inflammable).

3.2.3. Présentation des résultats

Les résultats d'une AMDE sont présentés sous forme de tableaux à colonnes, dont la structure peut varier en fonction des contextes et des besoins (adjonction ou suppression de certaines informations). Tous respectent cependant dans l'ensemble les sept étapes décrites au paragraphe précédent.

TABLEAU IV

Analyse du mode de défaillance, des effets et des probabilités - sous-système C : protection incendie (extrait) (Damien, 1985) –
Failure mode, effects and probabilities - unit C : fire protection

Nom du composant	Mode de défaillance	Causes	Effet de défaillance		Compensation procédure et entretien	Gravité	Probabilité	Risque	Repère du risque	Recommandations et observations
			localement	sur le système						
1	2	3	4	5	6	7	8	9	10	11
C.1 Vanne d'arrêt de ligne	Fermée	Erreur humaine	Pas de passage de l'eau	Protection incendie non opérationnelle	Volant de manœuvre de la vanne retiré en possession de l'agent de maîtrise	3	2	32	1	
	Obturée	Gel	Idem	Idem	Vannes dans local hors gel	3	1	31	2	
		Entartrage	Idem	Idem	Essai mensuel	3	4	34	3	
		Corps étranger	Idem	Idem	Idem	3	3	33	4	
		Défaillance mécanique de la vanne	Idem	Idem	Idem	3	3	33	5	
C.2 Vanne de détection électrique	Pas d'ouverture à la commande	Défaillance mécanique ou électrique	Pas d'eau	Protection incendie électrique non opérationnelle	Essai mensuel doublage par la vanne mécanique (2e circuit)	2	3	23	11	

Un extrait des résultats d'une AMDE, conduite par le « Groupe technique sécurité » de la Société nationale des poudres et explosifs (SNPE) et concernant la sécurité d'une installation pyrotechnique, est reproduit dans le tableau IV ([21]).

3.3. L'analyse par arbre d'événements (illustration)

Cette procédure permet de représenter l'ensemble des éventualités résultant de différentes combinaisons d'événements.

Le développement de l'arbre s'effectue à partir d'un événement initiateur et progresse selon une logique binaire (oui/non) ([22]). Chaque événement conduisant à identifier deux états successifs possibles, un nombre n d'événements pris en considération entraînera 2^n chemins possibles et par conséquent autant d'éventualités finales.

Une illustration de cette démarche empruntera l'exemple proposé par Barbet et Guyonnet (op. cit.), qui concerne l'examen des risques dus aux combinaisons de défaillances possibles des fonctions principales d'un système de désenfumage en cas d'incendie (fig. 8 et 9).

Une 1re solution envisage une séquence de déclenchement des cinq fonctions suivantes :

Solution A

1. Soufflage escalier (SE).
2. Soufflage sas (SS).
3. Extraction sas (ES).
4. Soufflage circulation (SC).
5. Extraction circulation (EC).

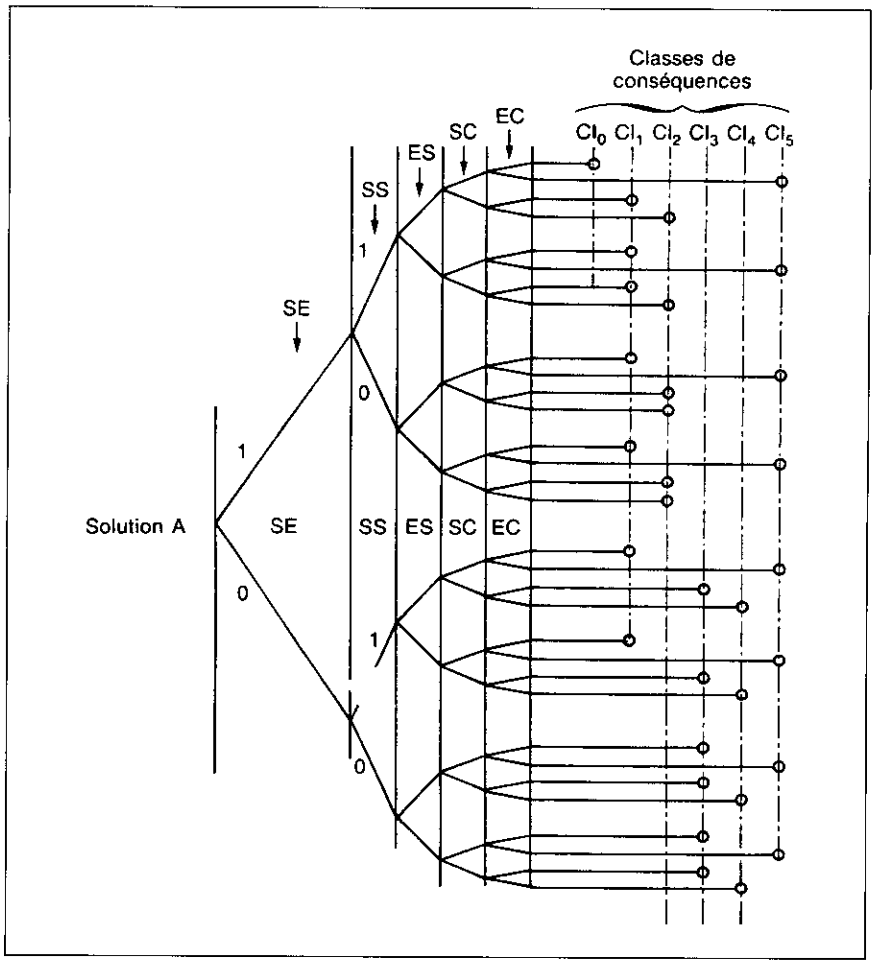
Une 2e solution retient la séquence suivante (suppression de deux fonctions ; ordre inchangé) :

Solution B

1. Soufflage escalier (SE).
2. Soufflage sas (SS).
3. Extraction circulation (EC).

([21]) Etude présentée par Damien (op. cit.).

([22]) Du point de vue du type de raisonnement impliqué, ce mode d'investigation permet de distinguer nettement cette méthode de celles présentées aux paragraphes précédents (APR et AMDE).



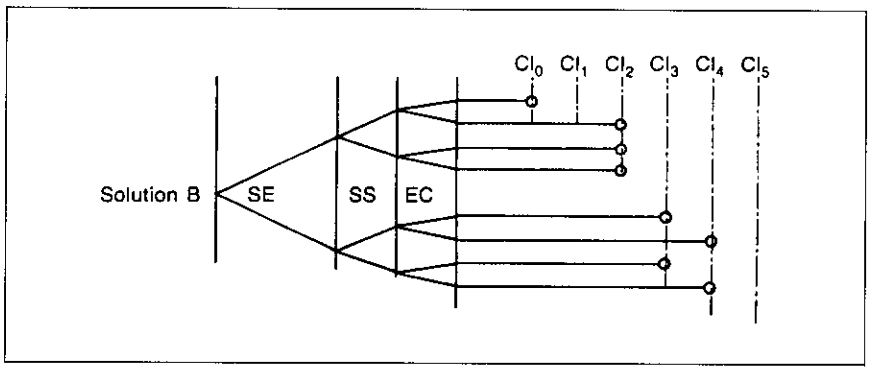
◄ ***Fig. 8. Arbre d'événements pour la solution A (Barbet et Guyonnet, 1984)*** – *Event tree for the solution A*

Légende

Fonction assurée (1)

Fonction non assurée (0)

SE : Soufflage escalier
SS : Soufflage sas
ES : Extraction sas
SC : Soufflage circulation
EC : Extraction circulation



◄ ***Fig. 9. Arbre d'événements pour la solution B (Barbet et Guyonnet, 1984)*** – *Event tree for the solution B*

Chacune de ces fonctions représente un événement. Les deux solutions conduisent à mettre en évidence l'ensemble des classes de conséquences indésirables possibles, présentées ci-dessous :

– classe 1 (cl 1) : cette classe regroupe les combinaisons de pannes n'altérant pas suffisamment le système de désenfumage afin que soient encore assurés la protection de l'escalier et le balayage satisfaisant de la circulation ;

– classe 2 (cl 2) : cette classe regroupe tous les cas de figure où est seulement assurée la protection de l'escalier. Le balayage de la circulation n'est plus réalisé correctement ;

– classe 3 (cl 3) : cette classe regroupe les cas de panne où est seulement assuré le balayage satisfaisant de la circulation sinistrée. La protection de l'escalier n'est plus réalisée ;

– classe 4 (cl 4) : cette classe regroupe les combinaisons de panne ne réalisant ni un balayage satisfaisant de la circulation, ni une protection de la cage d'escalier. Ceci est équivalent dans la pratique à une absence de désenfumage ;

– classe 5 (cl 5) : on regroupe dans cette classe les cas de pannes entraînant lors d'un incendie une configuration plus dangereuse qu'une situation où le désenfumage serait absent.

Une sixième classe, la classe 0 (cl 0), représente la situation de fonctionnement normal de l'installation.

La solution A conduit à l'arbre des événements présenté sur la figure 8. Cette solution présente huit cas conduisant à la classe de conséquence du type 5, qui caractérise la configuration la plus dangereuse.

La solution B conduit à examiner les situations données sur la figure 9. Aucune classe de conséquence du type 5 n'apparaît dans cette éventualité.

Cet exemple illustre une utilisation possible de la technique de l'arbre des événements. Par l'examen systématique des différents modes de dysfonctionnements d'un système, elle permet d'identifier la solution la plus sûre.

L'arbre d'événements se prête assez bien à l'analyse quantitative : attribution de probabilités de défaillance et/ou de bon fonctionnement (probabilités complémentaires) pour chaque événement et calcul des probabilités résultantes [23].

L'analyse par arbre d'événements s'inscrit dans le cadre plus général de la « méthode des arbres » (Lagadec, 1981), qui inclut aussi l'analyse par arbre des défauts. Les deux types d'analyses font appel à une démarche intellectuelle essentiellement déductive (identité des modes de raisonnement). Par contre, chacune d'entre elles considère différemment le système : un arbre d'événements est élaboré en partant d'événements élémentaires (dans l'exemple précédent, le « soufflage escalier » fonctionne ou ne fonctionne pas) ; un arbre des défauts part d'une situation (indésirable) qui peut être d'un ordre très général (destruction d'un dispositif technique par exemple).

3.4. L'analyse par arbre des défauts (ADD)

3.4.1. Présentation

Il s'agit essentiellement d'un diagramme logique représentant les combinaisons d'événements qui conduisent à la réalisation d'une sortie indésirable et définie a priori, ceci dans le cadre d'un système conçu pour assurer une mission déterminée [24]. Il est formé « de niveaux successifs tels que chaque événement soit généré à partir des événements du niveau inférieur par l'intermédiaire de divers opérateurs (ou portes) logiques » (Pages et Gondran, 1980, p. 49). Le processus déductif permet de développer l'arbre en partant de l'événement au sommet, ceci jusqu'à atteindre une série d'événements de base.

Les événements de base, ou événements élémentaires, sont caractérisés par les trois critères suivants :

- ils sont indépendants entre eux [25],
- leurs probabilités d'occurrence peuvent être calculées ou estimées,
- les spécialistes concernés n'éprouvent pas le besoin de les décomposer en événements plus simples.

La figure 10 illustre l'apparence prise par un arbre des défauts (cf. tableau V pour récapitulation des principaux symboles utilisés).

3.4.2. Principes d'application

Pour être conduite de façon efficace, une analyse par arbre des défauts doit respecter les étapes suivantes :

- connaissance du système,
- définition et choix de l'événement indésirable à étudier,
- élaboration de l'arbre,
- exploitation de l'arbre.

Connaissance du système

Les personnes chargées de l'étude doivent posséder une très bonne connaissance du système (conception, fabrication, utilisation) afin d'être en mesure d'analyser ses défaillances possibles. Par ailleurs, les objectifs nécessitent le plus souvent la mobilisation d'équipes pluridisciplinaires.

Définition et choix de l'événement indésirable à étudier

Il s'agit d'une étape essentielle, la définition de l'événement de tête conditionnant la pertinence et la portée de l'ensemble de l'analyse.

« L'événement de tête peut être défini a priori comme étant un événement potentiel connu caractéristique du système étudié et mis en évidence par l'expérience, en particulier par l'analyse des incidents qui se sont produits sur le système étudié ou sur des systèmes équivalents » (Barbet et Guyonnet, op. cit., p. 45).

Il est utile de compléter cette définition en rappelant que la connaissance de cet événement peut être obtenue à l'issue d'une phase d'identification générale des risques (en faisant appel le cas échéant à une méthode du type APR ou AMDE).

Une première estimation de ces risques – en fréquence et en gravité – facilitera le choix du ou des événements qui devront faire l'objet d'une analyse par ADD.

Elaboration de l'arbre

La construction de l'arbre s'effectue selon une logique déductive et sa mise en forme graphique fait appel aux divers symboles en usage.

Cette étape met généralement à contribution diverses compétences afin de permettre l'élaboration la plus complète possible. Lievens (op. cit.) précise à ce propos que l'ADD n'est pas d'un maniement facile, ce qui justifie à son point de vue le recours à des équipes pluridisciplinaires : « l'arbre doit être construit et exploité par des équipes pluridisciplinaires, rassemblant un grand nombre de généralistes et de spécialistes d'origines diverses. Chacun d'entre eux voit les événements de sa compétence dispersés entre plusieurs points de l'arbre, noyés au milieu d'autres événements qui le concernent moins » (p. 88).

---

[23] La méthodologie ASP (Accident sequence precursor) constitue une illustration de la démarche quantitative associée à la méthode des arbres d'événements (cf. Cooke et coll., 1987).

[24] Une certaine confusion est entretenue entre la technique de l'arbre des défauts (ou des « défaillances » ou des « fautes ») et celle de l'arbre des causes. La plupart des auteurs utilisent en effet indifféremment les deux expressions pour désigner la méthode d'analyse prévisionnelle présentée ici.

Il convient de rappeler que la méthode de l'arbre des causes développée par l'INRS vise à représenter l'ensemble des faits ayant provoqué un accident et non pas à effectuer une analyse a priori des risques d'accidents. D'autre part, cette méthode conduit à mettre en évidence des facteurs d'accidents à dominantes socio-technique et organisationnelle et non pas de nature essentiellement technique, ce dernier point caractérisant plutôt l'ADD (pour plus de précisions, cf. Leplat, 1985, pp. 55-59 et Guillermain et coll., 1989, p. 5).

[25] Ce qui signifie qu'un événement élémentaire ne résulte ni directement ni indirectement d'un autre événement de même niveau (la probabilité de défaillance d'un composant α ne doit pas inclure la probabilité de défaillance d'un composant β).

Fig. 10. Représentation générale de l'arbre des défauts – *Overall representation of the fault tree* ▶

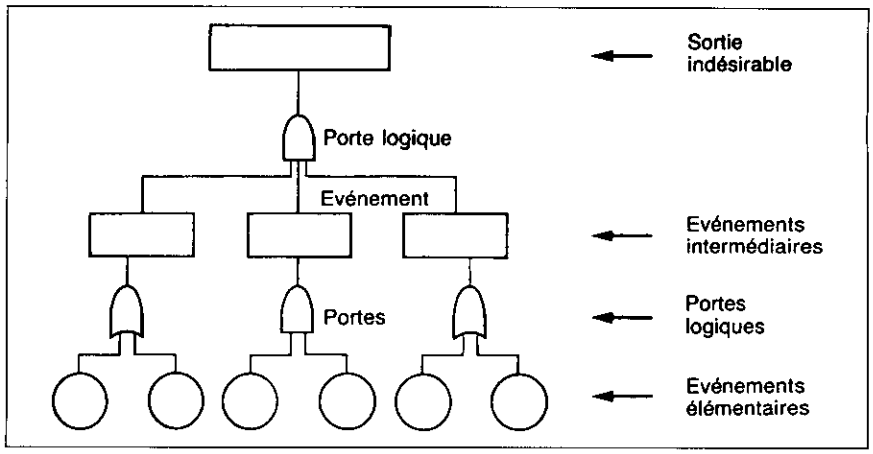
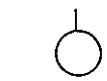
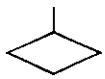
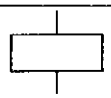
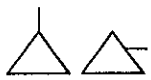
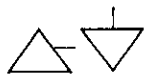
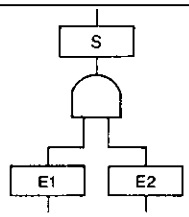
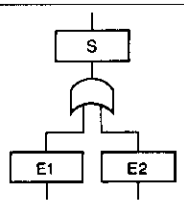
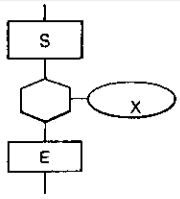


TABLEAU V

Représentation des événements et des portes logiques – Events and logical gates presentation

Symbole	Nom du symbole	Signalisation du symbole
	Cercle	Représentation d'un événement élémentaire
	Losange	Représentation d'un événement qui ne peut être considéré comme élémentaire, mais dont les causes ne sont pas développées faute de renseignements ou faute d'intérêt
	Rectangle	Représentation d'un événement intermédiaire résultant de la combinaison d'événements plus élémentaires par l'intermédiaire de portes logiques
	Maison	Représentation d'un événement qui correspond à un fonctionnement normal du système. Par définition, la probabilité de cet événement est 1
	Triangle	La partie de l'arbre qui suit le symbole △ est transférée à l'endroit indiqué par le symbole △
	Triangle inversé	Une partie sembable, mais non identique, à celle qui suit le symbole △ est transférée à l'endroit indiqué par le symbole ▽
	Porte ET	L'événement de sortie S est généré si les événements E_1 et E_2 sont présents simultanément
	Porte OU	L'événement de sortie S est généré si l'un au moins des événements E_1 ou E_2 est présent
	Porte SI	L'événement de sortie S est généré si l'événement E est présent et si la condition X est réalisée

Exploitation de l'arbre

L'exploitation d'un arbre des défauts peut rester qualitative ou être prolongée si nécessaire par une étape de quantification, lorsqu'il existe des sources de données concernant les taux de défaillance des différents composants.

Une solution intermédiaire consiste à effectuer une analyse semi-qualitative, en utilisant un procédé de classement des événements élémentaires en niveaux de risque (type UIC).

L'exploitation qualitative consiste à analyser l'arbre sur le plan de sa structure logique. Ainsi, l'examen des différents scénarios possibles conduit à identifier les événements ou les conjonctions d'événements de base reliés de la façon la plus directe à l'événement de tête (notion de « coupe minimale »). Par exemple, un événement de base lié à l'événement de tête par une succession de portes *ou* entraîne logiquement, de par l'inexistence de combinaisons intermédiaires, l'événement de tête.

D'autre part, la structure logique d'un arbre des défauts permet d'utiliser l'algèbre de Boole, c'est-à-dire permet d'exprimer cette structure au moyen d'équations logiques. Deux conséquences importantes en résultent :

– la possibilité de simplifier la structure logique de l'arbre, par la mise en évidence de fausses redondances. La réduction des fausses redondances (réduction booléenne) consiste à simplifier certaines expressions booléennes et par conséquent les éléments de structure qu'elles représentent ;

– la possibilité d'effectuer des simulations sur ordinateur. Il s'agira ici de simulations qualitatives, dont l'objet porte sur la structure de l'arbre et non pas sur d'éventuelles données quantifiées.

Ces simulations permettent notamment d'examiner les différentes combinaisons existantes et de résumer l'arbre à l'ensemble des coupes minimales. Tout arbre des défauts peut en effet être décrit au moyen d'un nombre fini de coupes minimales, reliant les événements élémentaires à la sortie indésirable. De telles simulations peuvent aussi servir, le cas échéant, à tester diverses propositions de modification du système (substitution de portes par exemple).

L'exploitation quantitative nécessite de disposer de données probabilistes sur les événements (fiabilité des composants notamment). Ces probabilités proviennent le plus souvent d'estimations statistiques effectuées à partir d'essais ou à partir de données recueillies au cours d'exploitations antérieures sur des systèmes comparables, ce qui revient à mettre en évidence l'articulation de fait entre les démarches « a priori » et « a posteriori » : « c'est à partir des probabilités d'occurrence des événements primaires, estimées statistiquement d'après les résultats d'exploitations passées, que l'on calculera, par la suite, la probabilité d'occurrence des événements redoutés (autrement dit (...) c'est à partir des données de fiabilité des composants de systèmes déjà existants que l'on évaluera le risque présenté par des systèmes nouveaux) » (Signoret et Leroy, op. cit., p. 1602).

La connaissance des densités de probabilités d'apparition de chaque événement de base (c'est-à-dire des lois de distribution des probabilités de défaillances) permet :

– de déterminer la probabilité globale d'apparition de l'événement de tête,

– de déterminer les chemins les plus critiques, autrement dit les plus probables parmi les combinaisons d'événements susceptibles d'entraîner l'événement de tête.

3.4.3. Illustration

Cette illustration reprend les éléments principaux d'une étude de sécurité présentée par Chereau et coll. (in : Lievens, op. cit., pp. 275-294). Elle porte sur un système technique relativement simple : un générateur de gaz pour coussin de sécurité automobile ([26]). Il s'agit d'un dispositif de protection pour conducteur ou passager en cas de collision frontale. Le système comprend :

– un détecteur de choc : accéléromètre,

– un dispositif pyrotechnique générant des gaz froids,

– un sac gonflable.

Le fonctionnement prévu pour ce système est le suivant :

– non fonctionnement en-dessous de 25 km/h de vitesse de choc (zone de choc faible ou d'absence de choc),

– fonctionnement au-dessus de cette vitesse de choc (zone de choc fort).

Une analyse des conséquences pour la sécurité des différents modes de dysfonctionnement a permis de constater qu'un fonctionnement inadéquat ou intempestif du système introduit un risque important dans les trois situations examinées par les auteurs (choc fort, choc faible, absence de choc).

Ces derniers ont retenu l'étude systématique de l'événement indésirable « éclatement du générateur de gaz », qui conduit à l'élaboration de l'arbre des défauts présenté à la figure 11.

Une étude par simulation des différentes combinaisons d'événements (probabilités connues) a permis de définir un premier chemin critique :

Eclatement du générateur

↓

Surpression dans la chambre :
P > 300 bars

↓

Non fonctionnement du système de sécurité et pression dans la chambre trop forte :
P > 120 bars

↓

Vitesse de combustion trop forte

↓

Géométrie du propergol défectueuse

↓

Tenue mécanique insuffisante

L'événement ayant la plus grande influence est le « non fonctionnement du système de sécurité » ([27]).

([26]) Ce système pyrotechnique était conçu pour fonctionner une seule fois par unité.

([27]) L'influence est définie comme le rapport de la « probabilité a posteriori » correspondante (probabilité pour que l'état i soit simulé et que simultanément l'événement indésirable ait lieu) à la probabilité de l'événement indésirable. Ici l'influence de l'événement « non fonctionnement du système de sécurité » est : p. a posteriori / p. événement indésirable = 0,776 (cf. Lievens, op. cit., p. 286).

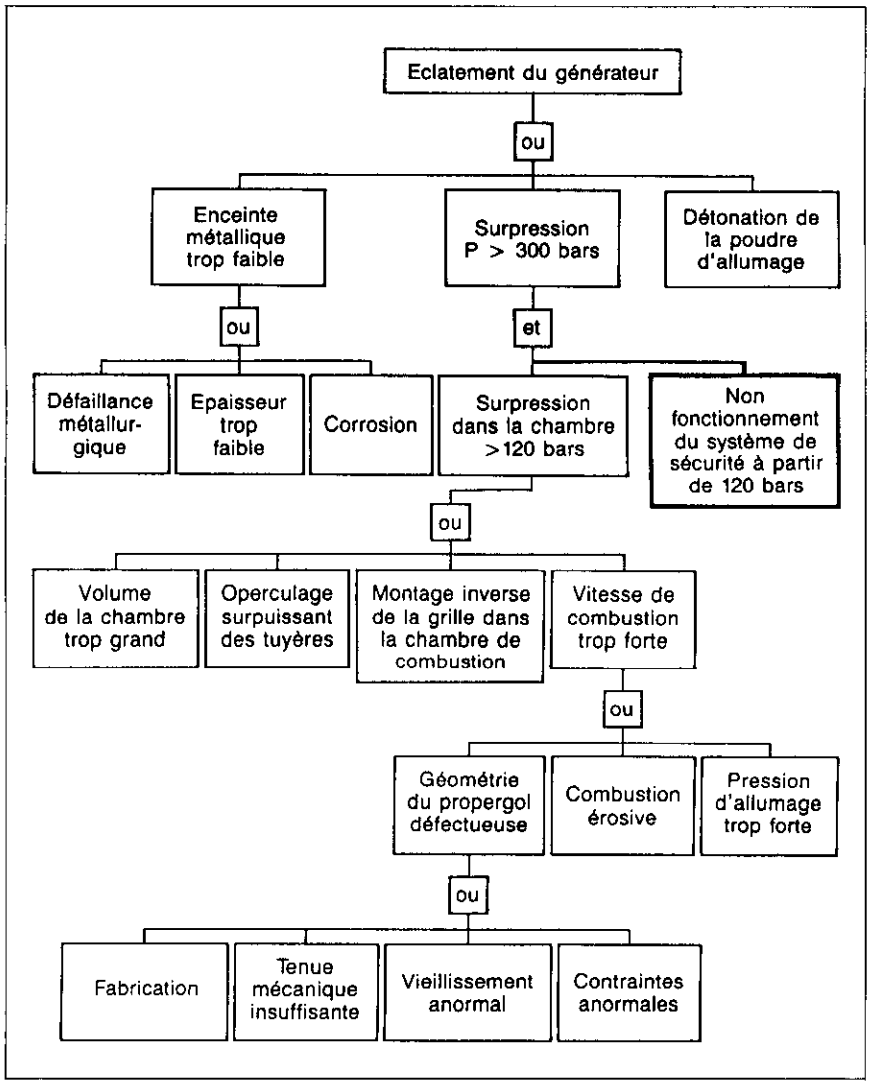


Fig. 11. Arbre des défauts : éclatement du générateur (Chereau et coll., in : Lievens, 1976) – *Fault tree : breaking-up of the generator*

Les modifications devront donc porter sur cette partie du système, afin de diminuer sa probabilité de défaillance initiale.

Une nouvelle simulation effectuée après introduction d'une probabilité cinq fois plus faible de l'événement considéré (de $0{,}5.10^{-3}$ à 10^{-4}) fait apparaître un nouveau chemin critique, qui présente l'intérêt d'être plus simple :

Eclatement du générateur
↓
Enceinte métallique trop faible
↓
Défaillance métallurgique

Cette simulation permet de mettre en évidence la nécessité d'améliorer le système de sécurité du générateur.

Une telle illustration de mise en œuvre de l'ADD sur un système technique fermé simple permet déjà de prendre acte de la complexité de la démarche (elle est représentative de l'usage décrit au § 2.4 concernant la « nature du système étudié »).

Le lecteur imaginera sans peine le degré de complexité pouvant être atteint lorsqu'un tel outil s'applique à des systèmes ou sous-systèmes très complexes et ramifiés (technologies de pointe, conduites de processus, etc.).

4. DIFFICULTES ET QUESTIONS SOULEVEES

4.1. La fiabilité et la sécurité

Les nombreuses analogies existant entre ces deux approches contribuent à entretenir une certaine confusion qui concerne en particulier les objectifs respectivement poursuivis. Cette situation a une origine historique, dans la mesure où le développement des études de sécurité des systèmes a fait largement appel aux techniques progressivement mises au point par les fiabilistes.

La théorie de la fiabilité date des années 1930. Elle s'est constituée comme discipline à part entière par suite de l'évolution de la notion primitive de « taux de défaillance » qui, d'instrument de mesure pour la comparaison entre eux d'événements passés (c'est-à-dire travaillant sur des fréquences), s'est transformée en instrument capable de fournir des résultats prévisionnels (introduction des probabilités).

A partir des années 1960, l'extension des principes de la théorie de la fiabilité de l'étude des systèmes électroniques vers celle de systèmes composés d'équipements mécaniques, hydrauliques ou électriques conduira au développement ou à l'adaptation des méthodes d'analyse systématique des risques que sont l'arbre des défauts, l'arbre d'événements, etc.

L'identité des outils utilisés par la fiabilité et la sécurité, à laquelle il convient d'ajouter l'usage commun de techniques de calculs statistiques et de calculs des probabilités, renforce

le sentiment d'être en présence d'une seule et même discipline que viendraient désigner deux appellations distinctes.

Le tableau VI rappelle les différences essentielles entre la fiabilité et la sécurité. Il permet notamment de constater que les deux disciplines ne se situent pas sur un même plan, aussi bien à l'égard des objectifs poursuivis qu'en ce qui concerne les moyens mis en œuvre pour les atteindre.

A tel point que ces objectifs peuvent entrer en conflit, en particulier lorsque l'analyste se trouve en présence de systèmes pour lesquels la probabilité de succès de la mission (la fiabilité) doit passer après la nécessité de ne pas encourir d'événement catastrophique avant ou au cours de celle-ci (la sécurité).

Il faut cependant ne pas perdre de vue que les résultats des études de fiabilité fournissent nombre de données (taux de défaillance des composants élémentaires en particulier) indispensables pour conduire les études de quantification des scénarios de dysfonctionnements développées dans les études de sécurité des systèmes.

TABLEAU VI

Comparaison entre fiabilité et sécurité (d'après Lievens, 1976) – Comparison between reliability and safety

Fiabilité	Sécurité
– Étudie les seuls risques de dysfonctionnements (non fonctionnement ou fonctionnement intempestif) susceptibles de survenir dans des conditions d'emploi conformes aux spécifications	– Envisage l'ensemble des circonstances, normales ou non, pouvant entraîner une situation dangereuse (pertes de vies humaines, blessures, destructions d'équipements...)
– Ne prend pas en compte les facteurs humains (défaillances, erreurs...)	– Considère l'homme comme un élément de l'ensemble étudié
– Considère des événements pouvant généralement être appréhendés par l'expérience et le traitement statistique	– Considère de très nombreuses combinaisons d'événements, dont chacune, peu probable, échappe à une exploitation statistique simple
– Peut entrer en conflit avec la sécurité et exiger parfois des solutions techniques différentes	– Peut être améliorée par de multiples moyens, l'augmentation de la fiabilité de certains éléments n'étant qu'un de ces moyens

4.2. L'origine et la fiabilité des sources de données

Deux sources d'information permettent d'alimenter les modèles d'analyse quantitatives des risques.

4.2.1. Banques de données

Elles fournissent à l'utilisateur « les valeurs les plus probables des taux de défaillance en fonction d'un certain nombre de contraintes appliquées au composant : contraintes climatiques et mécaniques (humidité, vibrations, pression, rayonnements), contraintes thermiques, contraintes électriques (tension, courant, puissance) » (Chapouille, 1972, pp. 52-53).

4.2.2. Données d'exploitation

Elles présentent l'avantage d'un certain réalisme à l'égard des facteurs de contexte (caractéristiques de l'environnement, utilisations hors spécifications, imperfections concernant la maintenance, etc.). En outre, les dysfonctionnements observés restent accessibles à l'exploitation statistique. Toutefois, certaines réserves doivent être émises en ce qui concerne la fiabilité de ces données.

4.2.3. Limites des données issues de la littérature technique

Basées sur des résultats d'essais menés en laboratoire, ces données risquent de minimiser l'importance des contraintes réellement rencontrées dans la réalité.

Lievens (op. cit., p. 54) signale par exemple que « la fréquence et la conséquence des erreurs de maintenance, qui contribuent largement au taux de panne global, ne peuvent y être appréciées ». Cette remarque est reconduite par Cooke et coll. (op. cit.). Les auteurs expriment, de façon générale, leur réserve concernant la confiance que l'on doit accorder à des données qui restent muettes sur l'origine exacte des taux de défaillance indiqués et, en particulier, lorsque les caractéristiques de la maintenance doivent être considérées « comme une cause significative de défaillance ».

D'autre part, les coefficients de pondération utilisés dans les calculs de taux de défaillance varient dans une très large proportion, ce qui conduit à « donner des valeurs assez différentes suivant les paramètres choisis » (Laplace, 1987, p. 40). L'utilisateur dispose-t-il toujours des critères adéquats lui permettant de décider en toute certitude du coefficient à appliquer ? ([28]).

([28]) En guise d'illustration, Laplace (op. cit., p. 40) indique le mode de calcul utilisé pour la détermination du taux de défaillance λ d'un circuit intégré. Soit :

$$\lambda = \pi e.\pi q.\pi l.\lambda b$$

avec

πe = 0,04 à 22 (plage de variation : 1 à 550) : dépend de l'environnement où est utilisé le composant (environnement sans contrainte particulière : 0,04 ; environnement de lancement de missile : 22),

πq = 1 à 300 : représente la qualité du composant,

πl = 1 à 10 : représente le facteur d'apprentissage pour le fabricant (un composant fabriqué depuis longtemps est plus fiable qu'un nouveau composant),

$$\lambda b = c1.\pi t.\pi v.\pi e\ (c2 + c3)$$

avec ici :
c1 : dépend du nombre de circuits logiques,
πt : dépend de la température de fonctionnement du composant,
πv : dépend de la tension d'alimentation du composant,
c2 : dépend de la complexité du composant (de même nature que c1),
c3 : dépend du nombre d'interconnexions vers l'extérieur, du type de boîtier.

4.2.4. Limites des données d'exploitation

Ces données sont entachées d'incertitudes qui résultent principalement de l'usage largement répandu des deux hypothèses simplificatrices suivantes :

– l'hypothèse de constance des taux de défaillance,

– l'hypothèse d'indépendance des défaillances.

1) L'hypothèse de constance des taux de défaillance revient à ne prendre en considération que la seule période correspondant à la durée de fonctionnement « normal » d'un produit, autrement dit à exclure les périodes de jeunesse (la période de « déverminage » des mécaniciens) et d'usure. Si l'hypothèse est justifiée pour les composants électroniques (durée de vie utile très longue, jusqu'à plus de 100 000 heures), elle l'est beaucoup moins pour les composants mécaniques.

Selon Lievens (op. cit., p. 54) ce taux est susceptible de varier en fonction des contraintes d'environnement et de fonctionnement. Il rappelle surtout que l'hypothèse de constance « est presque valable si les éléments concernés sont retirés du service avant l'apparition notable de phénomènes d'usure et de dégradation » (p. 157).

2) L'hypothèse d'indépendance des défaillances revient à considérer qu'à tout instant t, le taux de défaillance d'un élément quelconque est indépendant des défaillances qui se manifestent ou qui se sont manifestées sur d'autres éléments.

En réalité, cette hypothèse se heurte à trois difficultés (Lievens, op. cit., p. 255) :

« – il est extrêmement difficile de concevoir des ensembles parfaitement redondants, sans aucun élément commun dont la panne entraînerait la défaillance de l'ensemble,

« – la défaillance d'un élément entraîne souvent, soit au moment où elle se produit, soit d'une manière durable, des contraintes plus élevées au niveau d'autres éléments (...),

« – les contraintes générées par l'environnement du système induisent, au niveau des divers éléments, des contraintes qui ne sont pas indépendantes les unes des autres. Ainsi, au moment où un élément a la plus forte probabilité de panne, il en sera de même, selon toute vraisemblance, des éléments voisins. »

4.3. L'interprétation des probabilités

4.3.1. Notion d'événement rare

L'utilisation de la notion mathématique de probabilité pour estimer la survenue d'événements indésirables à l'échelle d'un complexe industriel est d'interprétation délicate. Que signifie par exemple une probabilité d'observer dans le domaine nucléaire un accident grave dont l'expression est de 10^{-7} (un dix millionième) par réacteur et par an ?

Un tel accident est-il susceptible de se produire en moyenne une fois tous les dix millions d'années (interprétation « en durée ») ou convient-il plutôt, considération faite d'un nombre théorique de dix millions de réacteurs en service, d'envisager en moyenne un accident par an (interprétation « en quantité ») ?

Aucune de ces deux interprétations n'est légitime. Elles sont néanmoins assez spontanées, car il est naturel pour l'esprit de tendre vers une représentation imagée d'un nombre aussi petit que 0,000 000 1 !

En réalité, la mesure de la probabilité d'occurrence d'un événement ne fournit aucune information concernant la distribution de celui-ci sur l'axe du temps ([29]).

Un événement aléatoire, aussi improbable soit-il, peut parfaitement se produire dans la seconde, dans le millénaire ou jamais.

4.3.2. Deux principaux modes d'interprétation d'une probabilité

Afin de lever de telles ambiguïtés d'interprétation, il est nécessaire de distinguer le concept mathématique de probabilité de l'utilisation qui est susceptible d'en être faite. Morlat (1983) rappelle que les objets du monde réel, dont la probabilité conceptuellement définie peut être un modèle, sont (outre la « mesure comptable » qui n'intéresse pas directement le propos) :

1) La fréquence

Elle s'observe en particulier dans le domaine de la statistique inférentielle, c'est-à-dire lorsqu'il y a confrontation entre la modélisation probabiliste d'un phénomène naturel et les résultats d'observations ou d'expériences ([30]). Cependant, en matière d'événements très rares et pouvant faire référence à des accidents jamais observés, l'utilisateur devra s'interroger sur la signification pratique de ce type d'interprétation.

2) La probabilité subjective

Elle fait moins référence à une définition technique de la notion d'événement aléatoire qu'à la mesure du degré de conviction d'un individu à l'égard d'une certaine situation ([31]). Pour l'auteur, la probabilité subjective « est une mesure de la confiance que peut accorder un sujet à une proposition incertaine ».

4.3.3. Probabilité et prise de décision

L'estimation de la probabilité d'occurrence de dysfonctionnements et, en particulier, d'accidents graves ne peut guère avoir d'autre objectif que celui d'assistance à la décision en matière de sécurité. C'est la raison pour laquelle il est raisonnable de considérer que les probabilités calculées doivent être interprétées au sens de probabilités subjectives, « même si le langage utilisé est souvent celui des fréquences » (Morlat, op. cit.). Une probabilité de défaillance de 10^{-5} n'a pas de signification absolue. Comparée à une probabilité de 10^{-4}, elle signifiera par contre une meilleure sécurité, ou une moins bonne confrontée à une valeur de 10^{-6}.

([29]) Sinon une information elle-même de nature probabiliste, ce qui nécessite de faire des hypothèses sur le comportement du phénomène étudié (notions de densité et de loi de probabilité théoriques) et/ou de disposer d'observations empiriques.

([30]) L'interprétation en fréquence de la mesure de probabilité caractérise par exemple la notion de taux de défaillance, évaluée le plus souvent à partir d'estimations statistiques (cf. § 2.1.2).

([31]) La probabilité de l'événement élémentaire au jet de dé est de 1/6. Il s'agit d'une probabilité pour laquelle le degré de conviction se fonde sur la notion d'équiprobabilité (P(1) = P(2) = ... = P(6)) et sur celle de fréquence limite (sur un grand nombre de jets, la probabilité de l'événement élémentaire tend vers 1/6). En revanche, deux géologues n'auront pas le même degré de conviction quant à l'existence d'une nappe de pétrole sous un terrain déterminé. Il s'agira ici d'une situation dans laquelle le même événement suscite des degrés de conviction différents d'un individu à l'autre (cf. Tricot et Picard, 1969).

4.3.4. Probabilité subjective et jugements d'expert

La mise en œuvre des probabilités subjectives est réalisée à l'occasion des jugements d'expert, ce qu'illustrent les quatre exemples ci-après.

1) Signoret et Leroy (op. cit., pp. 1606-1607) rappellent que « lorsqu'on ne dispose pas de résultats d'exploitation antérieurs, on peut utiliser le jugement d'expert, dont l'application systématisée est connue sous le nom de méthode « Delphi », pour estimer des ordres de grandeur des probabilités recherchées. Cette méthode consiste principalement à interroger les spécialistes des domaines techniques concernés sur la fréquence d'occurrence des événements primaires mis en évidence et à effectuer un calcul statistique sur l'ensemble de leurs réponses. Pour que les résultats soient statistiquement significatifs, il est nécessaire que le nombre d'experts interrogés soit suffisant (environ une vingtaine) et que leurs réponses soient indépendantes ».

La méthode Delphi a aussi été utilisée pour établir les données de défaillance des matériels électriques et électroniques recensées dans un document de l'IEEE (Institute of Electrical and Electronics Engineers) (IEEE Std-500, 1977).

2) Wanner, cité par Lievens (op. cit., pp. 201-202), utilise une procédure d'évaluation de la charge de travail qui consiste à associer des probabilités d'accident à diverses classes de notes, elles-mêmes attribuées de façon conventionnelle à partir des réponses fournies par les pilotes ou les équipages d'avions aux questions qui leur sont posées (tableau VII).

3) Sarrat et N'Kaoua (1986, p. 33) précisent à propos d'une étude consacrée à la sécurité des systèmes d'une paroi « qu'en l'absence de recueil de données probabilistes comparables aux recueils de fiabilité, les renseignements ont été obtenus en s'appuyant sur la connaissance et l'expérience acquise dans ces domaines. (...) Ces données ont été établies dans l'esprit suivant :

– événement courant : probabilité d'occurrence = 1.10^{-3},

– événement rare : probabilité d'occurrence = 1.10^{-6},

– événement extrêmement rare : probabilité d'occurrence = 1.10^{-9} ».

TABLEAU VII

Probabilité d'accidents associée aux réponses fournies pour l'évaluation de la charge mentale (d'après Wanner, in : Lievens, 1976) – Accident probabilities connected with answers given for mental load assessment

La sécurité immédiate et la sécurité à court terme ont-elles été assurées?		La charge de travail était-elle inférieure ou égale au maximum quotidien admissible pour cette sous-phase?		Classe	Probabilité conditionnelle d'accident
Non	Sans hésitation			7	10^{-1}
Non	Avec hésitation			6	10^{-3}
Oui		Non	Sans hésitation	5	10^{-5}
Oui		Non	Avec hésitation	4	10^{-7}
Oui		Oui	Avec hésitation	3	10^{-9}
Oui		Oui	Sans hésitation	2	10^{-11}

TABLEAU VIII

Estimations d'expert concernant la probabilité de défaillance (par heure et par tronçon) d'un conduit en acier de haute qualité (diamètre ⩾ 3 pouces) (d'après Cooke et coll., 1987) – Expert estimates for failure (per section and hour) of high quality steel pipe of diameter ⩾ 3 inches

Source	Valeurs estimées
1. LMEC (nuc)	5E-6 (⇔ 5.10^{-6})
2. Holmes (nuc)	1E-6
3. GE (nuc)	7E-8
4. Shopsky (nuc)	1E-8
5. IEEE Trans. a (nuc)	1E-8
6. IEEE Trans. b (nuc)	1E-8
7. NRTS Idaho (nuc)	1E-8
8. Otway (nuc)	6E-9
9. Davies (nuc)	3E-9
10. SRS	2E-9
11. IKWS. Germ. (nuc)	2E-10
12. Collins (nuc)	1E-10
13. React. incid. file (nuc)	1E-10

Estimations formulées dans le rapport WASH-1400 : 1E-10, intervalles de confiance à 90 % : 3E-9 à 3E-12
nuc = données concernant les réacteurs nucléaires

4) Une dernière illustration empruntée à Cooke et coll. (op. cit., p. 17) concerne le recensement de données fournies par 14 sources différentes d'expertises en vue d'estimer la probabilité de défaillance d'une conduite en acier. L'amplitude des réponses varie de 5.10^{-6} à 10^{-10} (tableau VIII). Les illustrations proposées font apparaître l'extrême variabilité des jugements d'expert. Compte tenu de l'utilisation particulière qui peut être faite des résultats obtenus, ces méthodes soulèvent la question de leur légitimité. La confiance que l'on peut accorder à l'estimation d'un risque par

un individu reconnu compétent est une chose, la conversion de cette estimation en mesure quantifiée de probabilité de défaillance en est une autre.

En effet, dans cette dernière éventualité, rien n'interdit plus d'effectuer des opérations arithmétiques et logiques sur de telles données, aussi sûrement qu'à partir d'une mesure de défaillance effectuée sur un composant au moyen d'essais en laboratoire ou d'observations statistiques établies aussi rigoureusement que possible. Une telle démarche incite à la prudence, ce qui fait dire par exemple à Villemeur (op. cit.), à propos de la quantification des erreurs et de leur introduction dans les arbres, « qu'il est généralement conseillé d'évaluer la sensibilité des résultats à une modification des probabilités des erreurs humaines qui ont le plus de poids. En effet, l'incertitude élevée des probabilités données par les modèles actuels rend peu significatif un résultat final non accompagné d'une étude de sensibilité ou d'un facteur d'erreur » (p. 431).

4.4. L'introduction de la fiabilité humaine

4.4.1. La fiabilité technique et la fiabilité humaine

Le problème soulevé par l'utilisation des jugements d'expert n'est que l'expression particulière des difficultés qui accompagnent les tentatives de quantification non fondées sur l'observation de phénomènes strictement techniques. La traduction d'un jugement d'expert en mesure de probabilité revient ainsi à effectuer une mesure d'attribution de l'importance que le spécialiste associe à un risque donné (probabilité subjective).

Une telle démarche suppose d'adhérer à l'hypothèse suivant laquelle la représentation du risque que l'expert s'est construite s'ajuste raisonnablement au risque réel. Dans la mesure où ce dernier n'est pas techniquement évaluable (du moins avec des garanties suffisantes), l'hypothèse demeure invérifiable, sinon a posteriori, autrement dit et d'un point de vue théorique, en cas d'accidents (suffisamment nombreux). En bref, le jugement d'expert repose sur la confiance, ce qui, faute de mieux, permet de disposer d'estimations chiffrées ou chiffrables.

D'une façon analogue, l'intérêt porté aux risques susceptibles d'être engendrés par l'activité des opérateurs s'est concrétisé par la mise en œuvre de techniques inspirées directement des méthodes d'analyses de la fiabilité technique.

Le caractère mesurable de la défaillance technique résulte pour l'essentiel de la possibilité de décomposer un système en unités élémentaires ou fonctionnelles. De même, les techniques de fiabilité humaine se proposent de décrire d'un point de vue analytique l'ensemble des activités des individus, afin de mettre en évidence des classes d'erreurs susceptibles d'engendrer des risques pour le système.

La fiabilité globale d'un système est alors conçue comme la résultante de deux sous-ensembles : la fiabilité des composants techniques et celle des composants humains.

4.4.2. Les méthodes de la fiabilité humaine

Elles sont généralement distinguées, en fonction du type d'analyse pratiquée sur le système, en approches qualitatives et quantitatives. Pour chacune d'elles, les plus connues sont respectivement le modèle de « l'arche de Rasmussen » (Rasmussen, 1986) et la méthode THERP (Technique for human error rate prediction = technique pour la prédiction du taux d'erreur humaine) (Swain et Guttmann, 1983).

Le modèle d'analyse du comportement de l'opérateur développé par Rasmussen permet de distinguer différentes phases au cours desquelles des erreurs peuvent se produire. Il pourra s'agir par exemple d'un défaut d'attention au cours de la première phase « d'activation » ou encore de l'omission d'une étape au cours de la phase de « choix de la procédure ». Ce modèle distingue plus généralement trois niveaux de comportement de l'opérateur : comportement fondé sur les connaissances (ou comportement « cognitif »), sur les règles (comportement « procédural »), sur l'habileté (comportement « machinal ») (cf. aussi Villemeur, 1988, p. 416).

De nombreuses autres classifications à dominante qualitative, généralement plus simples, sont utilisées par certains analystes. Par exemple Lievens (op. cit., pp. 133-134) distingue, parallèlement aux modes de défaillances techniques, des « modes d'erreurs », tels que l'oubli, la fausse manœuvre, l'action imprécise ou l'action intempestive.

La méthode THERP peut être considérée comme « une extension des méthodes de fiabilité technique à la composante humaine dans le système » (Fadier et Guillermain, 1987). Le principe de sa mise en œuvre est le suivant :

« a) définition de la défaillance du système que l'on doit étudier,

« b) identification de toutes les opérations humaines effectives,

« c) prédiction des taux d'erreurs pour chaque opération,

« d) détermination de l'effet de l'erreur sur le taux de défaillance du système,

« e) recommandations de modifications du système pour ramener celui-ci à un taux de défaillance acceptable.

« Deux valeurs de base sont utilisées par THERP :

« – la probabilité (Pi) pour qu'une opération conduise à une erreur de classe i ;

« – la probabilité (Fi) pour qu'une erreur de classe i entraîne une défaillance du système.

« – Le produit Fi × Pi est la probabilité pour qu'une erreur se produisant dans une opération entraîne une défaillance du système » (Fadier, 1985).

D'autres méthodes orientées vers la quantification des tâches et des dysfonctionnements de l'opérateur ont été développées ([32]). Par exemple, Carnino (1987) cite le modèle OAT (Operator action tree), qui concerne plus particulièrement la détection et la quantification des erreurs de type décisions et actions : « le modèle d'action est un arbre d'événements lié à la détection, à l'interprétation, au diagnostic et aux réactions requises. La courbe de probabilité de défaillance des opérateurs en fonction du temps mis pour réfléchir et diagnostiquer donne alors la probabilité cherchée » (Carnino, op. cit., p. 74).

([32]) Hannaman et coll. (1984) passent 16 modèles en revue.

4.4.3. Les deux modes d'approche de l'erreur humaine

La notion d'erreur humaine tient une place centrale dans l'approche « fiabilité humaine ». Bien qu'il s'agisse d'une préoccupation ancienne ayant donné lieu à de nombreux travaux, en particulier dans les domaines de la psychologie du travail et de la psychologie ergonomique, l'erreur humaine n'a pas toujours été associée au risque d'accident, comme en témoigne par exemple le passage suivant, extrait de l'introduction de l'étude documentaire « Les facteurs humains et la sécurité » (CECA, 1967) : « Allant plus loin encore, certains ont imaginé qu'il pouvait y avoir quelque parallélisme entre le mécanisme des erreurs et celui des accidents ; s'il était admis comme valable pour atteindre ces mécanismes d'étudier la production d'erreurs en laboratoire dans des conditions contrôlées, on disposerait d'une méthode puissante pour analyser les facteurs divers influençant la production d'accidents ; mais les « si » impliqués par cette technique pèsent trop lourdement pour qu'il ait paru souhaitable de transposer dans ce rapport les recherches sur les erreurs » (p. 18).

En fait, il est important de remarquer que les objectifs poursuivis par la sécurité des systèmes et, en particulier, par la fiabilité humaine concernent en priorité le risque d'accident technologique. En d'autres termes, la sécurité des personnes est considérée comme un sous-produit de la sécurité globale du système. Dans ce contexte, la place des études de fiabilité humaine ne peut pas être définie de façon univoque.

Sa contribution la plus manifeste, mais aussi la plus discutable, concerne la détection des erreurs humaines susceptibles de détériorer le niveau de sécurité globale du système. L'erreur humaine est considérée comme un équivalent fonctionnel des diverses classes de défaillances (mécaniques, électriques, électroniques...) qui affectent le système. Autrement dit, son statut méthodologique y est celui d'une variable d'entrée.

Un autre courant de la fiabilité humaine reste plus apparenté à la démarche de l'ergonomie des systèmes. Il confère alors à l'erreur le statut de variable de sortie, c'est-à-dire d'indicateur de dysfonctionnement du « système homme × tâche » dont il conviendra le cas échéant d'améliorer la performance, en particulier au moyen d'aménagements ergonomiques. Ici, erreur humaine et accident peuvent faire l'objet d'un rapprochement original.

L'une et l'autre seront en effet considérés comme autant de symptômes d'un dysfonctionnement qui n'est pas attribué exclusivement à l'opérateur (aptitudes, vigilance, etc.) mais aussi aux caractéristiques de son poste ou plus généralement de son environnement de travail ([33]).

4.4.4. Les limites de la fiabilité humaine

Les études ergonomiques consacrées à la sécurité ont démontré la nécessité de se dégager d'une approche trop exclusivement centrée sur l'opérateur. Les approches de type sociotechnique se sont ainsi progressivement substituées aux études unicausales, dominées par la notion de prédisposition aux accidents.

En d'autres termes, la nécessité d'élargir le champ des investigations s'est progressivement affirmée, en particulier avec la mise en évidence de phénomènes accidentogènes tels que les interférences entre tâches (coactivité, intersection, succession, zones frontières) ou les activités de récupération, phénomènes qui résultent en premier lieu de dysfonctionnements organisationnels ([34]).

Dans la perspective d'analyse de l'activité de l'opérateur humain, il conviendrait alors de faire référence au système sociotechnique et non plus seulement au système technique. Toutefois, il apparaît clairement que, dans le contexte de la sécurité des systèmes, les conceptions qui influencent le plus les recherches consacrées à l'évaluation des erreurs humaines n'ont jusqu'alors guère tenu compte des facteurs précités.

De nombreuses critiques ont par conséquent été adressées aux méthodes de quantification de l'erreur humaine.

1) La plus sérieuse et la plus profonde a trait au réductionnisme excessif, et par conséquent éloigné de la réalité, d'une approche qui n'est pas sans évoquer la position du mécanicisme qui « méconnaît les particularités spécifiques du fonctionnement de l'organisme vivant, et de l'homme en particulier, et manifeste une tendance à considérer l'opérateur dans les systèmes de direction comme un mécanisme inanimé » (Léontiev et coll., 1961).

Ainsi, Leplat (1985, p. 98) rappelle que le transfert des méthodes de la fiabilité technique vers la fiabilité humaine est délicat dans la mesure où, à la différence d'un dispositif technique, l'homme s'adapte et apprend, poursuit des buts multiples, traite souvent l'information de façon globale et dispose de la « capacité de se contrôler et de corriger ses erreurs ».

2) Une revue critique, plus directement centrée sur l'intérêt pratique des études de quantification de l'erreur humaine, a été effectuée par la « Human Factors Society of America » ([35]). Les aspects principaux sur lesquels portent cette revue sont rappelés par Cooke et coll. (op. cit., p. 28) :

– les données fournies par le rapport Swain et Guttman (op. cit.) ([36]) sont insuffisantes ;

– de telles données, qui n'ont jamais été validées, peuvent faire l'objet d'une utilisation trop confiante de la part d'utilisateurs peu avertis ;

– elles n'ont quasiment aucun impact sur la conception des centrales nucléaires ;

– une série d'aménagements ergonomiques bien conduits entraînerait à elle seule une amélioration notable de la situation dans le domaine du nucléaire.

3) Une dernière revue critique sera empruntée à Fadier et Guillermain (op. cit.). Les auteurs mettent l'accent sur une trop forte dépendance à l'égard

([33]) Pour une présentation plus détaillée de cette approche, cf. Guillermain et coll. (op. cit.).

([34]) Phénomènes que Faverge (1970) qualifiait précisément de « points noirs de la fiabilité ». Cf. aussi Monteau et Pham (1987) et la 1re partie de ce bilan (ND 1768-138-90), en particulier le dernier chapitre.

([35]) A l'occasion d'un rapport commandité par le Nuclear Regulatory Commission (NRC) suite à l'accident survenu à la centrale nucléaire de Three Mile Island (Snyder et coll., 1982).

([36]) Il s'agit du « Handbook of human reliability » (manuel de la fiabilité humaine) rédigé par Swain et Guttman pour le compte de la « U.S. Nuclear Regulatory Commission ». Ce document fournit en particulier des estimations probabilistes d'erreurs pour diverses tâches, estimations accompagnées d'intervalles de confiance. Par exemple, la probabilité d'erreur associée à la lecture d'un affichage digital serait de $p = 10^{-3}$ avec un intervalle de confiance compris entre 5.10^{-4} et 5.10^{-3}.

de « l'intuition de l'analyste », associée à une carence d'analyses ergonomiques sérieuses du travail en vue d'effectuer des évaluations. Ils rappellent en outre que « ces méthodes quantitatives sont difficilement transposables à des entreprises plus traditionnelles compte tenu de la durée et du coût de leur utilisation. En effet, les enjeux dans une entreprise à hauts risques sont financièrement sans commune mesure avec des industries à « bas risques ». De plus, la part de l'homme dans la mission des systèmes traditionnels est moins circonscrite et soumise à de fortes variations (dans le temps, la répartition des tâches...). Il est donc nécessaire de remanier ces méthodes, si l'on veut les généraliser à des systèmes plus traditionnels » ([37]).

Le « remaniement » dont il est question fait référence à la démarche « fiabilité du système homme/tâche », démarche moins ambitieuse mais sans doute plus réaliste, qui intègre la prise en compte ergonomique de l'activité (analyse de la tâche en particulier).

([37]) L'utilisation des méthodes de la fiabilité humaine (quantitatives et qualitatives) dans un contexte industriel traditionnel et à bas risques (système de production agro-alimentaire) a été proposée par l'un des auteurs (Fadier, op. cit.).

CONCLUSION

Le tableau IX donne une vue d'ensemble des méthodes, des objectifs et des niveaux d'application privilégiés de la sécurité des systèmes. Un examen rapide confirmera si nécessaire qu'il s'agit d'une approche essentiellement centrée sur les aspects techniques de la sécurité.

Resituée dans le contexte général des différentes méthodes d'analyse prévisionnelle des risques (cf. ND 1768-138-90), la sécurité des systèmes représente en fait une option qui tend à circonscrire délibérément le champ de ses investigations à un système, défini avec précision, dans lequel on

TABLEAU IX

Méthodes, objectifs et niveaux d'application privilégiés de la sécurité des systèmes –
Methods, aims and main application standards of the systems safety

Méthodes	Objectifs	Supports/outils	Mise en œuvre	Niveaux d'application privilégiés	Commentaires
	– Évaluer le niveau de risque d'un système technique – Identifier des combinaisons d'événements indésirables		– Par équipes d'experts et d'ingénieurs	– Système technique dangereux et/ou complexe	– Efficacité maximum au stade de la conception – Coût généralement élevé – Mise en œuvre de compétences élevées
Méthodes inductives (causes → effets) et Méthodes déductives (effets → causes)		– APR (Analyse préliminaire des risques)	– Système de fiches d'analyse (ex. Union des industries chimiques) (tableau II) – Arbres logiques (fig. 7) – Tableaux à colonnes	– Applicable pour les systèmes techniques les moins complexes (prise en compte malaisée des combinaisons de défaillances)	– Première étape d'une analyse type « sécurité des systèmes »
		– AMDE (Analyse des modes de défaillance et de leurs effets)	– Diagrammes par blocs – tableaux à colonnes (tableau IV)	– Systèmes techniques, avec possibilité de prise en compte de l'activité des opérateurs (erreurs humaines) si activité suffisamment formalisée	– Possibilité de quantification du risque (AMDEC)
		– AE (Analyse par arbre d'événements)	– Arbres logiques (logique binaire oui/non) (fig. 8 et 9)	– Systèmes techniques	– Peu efficace pour la détection des fonctionnements dégradés (dérives, etc.)
		– ADD (Analyse par arbre des défauts)	– Arbres logiques (logique booléenne et/ou) (fig. 10 et 11)	– Idem	– Exploitation délicate pour les systèmes complexes. Ne rend pas bien compte des configurations changeantes – Possibilités de quantification

recherche les défaillances qui conduisent à, ou sont à l'origine, des événements redoutés.

Appliquées à des dispositifs techniques limités, comme un circuit de commande de presse, par exemple, ces méthodes sont capables de supprimer les défauts de conception qui pourraient provoquer la répétition du cycle, le fonctionnement de la presse sans écran protecteur, la possibilité de démarrage avec une seule commande, etc. Les analyses de sûreté « systémiques » présentent donc l'indéniable mérite de réduire ou de supprimer certains risques avant d'en observer les effets.

Rappelons toutefois que leur usage s'est étendu en priorité aux systèmes qui pourraient connaître des événements dont les conséquences seraient très graves, voire catastrophiques. Les applications à de tels systèmes complexes (avions, centrales nucléaires, raffineries...) démontrent, si besoin est, que la sécurité absolue d'une activité est bien un mythe. Ainsi, « la sécurité est toujours relative et toute affirmation contraire n'est qu'une incantation sans valeur opérationnelle » (Goliger et Lievens, 1976). Le concept de maîtrise raisonnée des risques prévaut désormais et, en conséquence, celui d'insécurité assumée (en connaissance de cause).

Il nous semble important, pour conclure cette présentation générale des méthodes de la sécurité des systèmes, d'évoquer deux questions qui ne sont pas prioritairement de nature technique ou méthodologique.

1) Le seuil d'inacceptabilité du risque

En théorie, la représentation formelle du risque qui fait habituellement référence (cf. § 2.1) veut qu'un événement assez fréquent et de gravité mineure soit rejeté (risque non accepté) au même titre qu'un événement très improbable mais aux conséquences fâcheuses (risque = probabilité × gravité). En fait, l'hyperbole du risque masque une réalité d'évidence : la sécurité des systèmes n'a pas été conçue et développée dans la perspective de réduire les risques de faible gravité. Les méthodes qu'elle préconise s'imposent d'autant plus qu'elles concernent des systèmes à hauts risques, c'est-à-dire pour lesquels l'expérience de l'accident, du fait de sa gravité potentielle, n'est pas envisageable. « En bref, la question de la possibilité éclipse celle de la probabilité » (Lagadec, op. cit., p. 1148) (38).

2) Le rapport coût/efficacité

Le développement des méthodes d'analyse des risques développées dans le cadre de la sécurité des systèmes soulève aussi la question de leur transfert en direction d'activités « traditionnelles », c'est-à-dire en particulier d'activités à bas risques. Sous réserve qu'une telle évolution puisse être observée, la question du coût prendrait un caractère de première importance, notamment dans la phase de décision de mise en œuvre d'une étude.

Or, l'adhésion au principe en vertu duquel « qui peut le plus, peut le moins », autrement dit faire l'hypothèse qu'il existe une relation linéaire entre les coûts engagés (coûts financiers mais pouvant aussi être exprimés en termes de mobilisation de personnel, de compétences requises...) et l'efficacité attendue (plus les coûts sont importants, meilleure serait l'efficacité) ne semble pas devoir être très raisonnable. Le niveau des techniques et des compétences engagées, le temps investi pour de telles études conduisent en effet à penser qu'une intervention menée avec toute la rigueur et le sérieux souhaités s'accorderait mal de contraintes économiques trop importantes.

A l'inverse, il conviendrait sans doute de s'interroger sur les limites pratiques d'une complexification grandissante de ces techniques ou d'une extension toujours plus grande du domaine de validité supposé de la sécurité des systèmes.

La prise en compte de paramètres de plus en plus sophistiqués et parfois fragiles sur le plan scientifique (en particulier dans le domaine des jugements d'expert et d'un certain courant de la fiabilité humaine), la mise en œuvre de programmes complexes de modélisation des dysfonctionnements (39) ou encore l'exploitation d'arbres des défauts « incohérents » (40) ou « augmentés » (41) sont-elles des voies d'approches susceptibles de déboucher rapidement sur des applications concrètes ailleurs que dans des secteurs de pointe ? (42).

Par ailleurs, des contributions apparaissent qui proposent des versions simplifiées des techniques usuelles de la sécurité des systèmes (cf. Capps, 1984 ; Agostini, 1986). Elles répondent à l'évidence à un besoin d'accessibilité financière et technique pour ces outils.

Au-delà d'un certain coût (envisageable dans le domaine de la recherche), le risque n'existe-t-il pas d'atteindre en pratique le seuil des « rendements décroissants » familiers aux économistes ?

(38) L'étude de la gravité potentielle des accidents représente une activité scientifique à part entière. Voir par exemple Escande et Lannoy (1989) pour une présentation des phénomènes de dispersion de produits inflammables.

(39) Cf. par exemple la technique des réseaux de Petri (illustrations dans Signoret et Leroy, op. cit., et Barbet et coll., 1987).

(40) Introduction de portes logiques complexes. Voir par exemple Kumamoto et Henley (1978) pour proposition d'un algorithme de traitement des arbres et Locks (1980) pour discussion critique.

(41) Introduction des techniques de modélisation de la propagation des défaillances inspirées des méthodes de l'intelligence artificielle (formalisation de règles de production des connaissances en particulier). Voir Narayanan et Wiswanadham, 1987.

(42) Nombre de catastrophes industrielles (Seveso, Bhopal, Flixborough, etc.) mettent en évidence des dysfonctionnements grossiers aux niveaux organisationnels les plus généraux. Que valent les explications formulées en termes d'erreurs humaines ou d'enchaînements sophistiqués de défaillances face à des constats semblables à celui-ci : « Ainsi, pour l'accident de Flixborough : changement de processus de production, triplement de la capacité de l'usine sans redéfinition du système de sécurité ; poste d'ingénieur d'entretien vacant ; place incertaine de l'ingénieur de sécurité ; décision de placer un tuyau provisoire sans étude préalable, sans test ; inattention aux fuites, certaines se « résorbant d'elles-mêmes », etc. » (Lagadec, 1987, p. 35).

Bibliographie

- ABRIBAT J.C. et coll. – Introduction à l'analyse du risque technologique dans les procédés chimiques. *Cahiers de Notes documentaires,* 1988, 131, pp. 265-276, ND 1675.
- AGOSTINI J. – Exploitation rapide d'arbres de défaillances. Actes du 5e Colloque international de fiabilité et de maintenance. Biarritz, ADERA, 1986, pp. 300-303.

- BARBET J.F., GUYONNET J.F. – Les méthodes d'analyse de la sécurité des systèmes. *Revue Générale de Prévention*, 1984, 30, pp. 42-50.
- BARBET J.F., JOUBERTON D., HOGNON B., MATHEZ J. – Approche probabiliste de la sécurité incendie dans les E.R.P. *Revue Générale de Sécurité*, 1987, 63 pp. 45-50.
- CAPPS J.H. – System safety for plant safety specialists. *Professional Safety*, 1984, 29, 6, pp. 22-26.
- CARNINO A. – La fiabilité humaine. *Enjeux*, 1987, 81, pp. 73-76.
- CECA - Les facteurs humains et la sécurité. Luxembourg, Etudes de physiologie et de psychologie, 1, 1967.
- CHAPOUILLE P. – La fiabilité. Paris, PUF, 1972.
- CHARBONNEAU S. – L'étude de danger des installations classées. Actes du Colloque AITASA. Bordeaux, IUT, 1987.
- CNPP-AFNOR - Les accidents technologiques. Paris, 1988.
- COOKE R.M., GOSSENS L.H.J., HALE A.R., HORST (VAN DER) J. – Accident sequence precursor methodology. Delft, Technische Universiteit, 1987.
- DAMIEN M. – Analyse des modes de défaillance des installations pyrotechniques. *Revue Générale de Sécurité*, 48, 1985, pp. 46-52.
- DESCHANELS J.L., LAVEDRINE P. – Maîtrise des risques techniques. *Revue Générale de Sécurité*, 1984, 35, pp. 31-35.
- ESCANDE J., LANNOY A. – Les risques chimiques industriels. *La Recherche*, 1989, 207, pp. 280-290.
- FADIER (FADDOUL) E. – Contribution à l'étude de l'influence de la fiabilité humaine sur la fiabilité d'un système de production agro-alimentaire. Bordeaux, thèse de 3e cycle (non publiée), 1985.
- FADIER E., GUILLERMAIN H. – Fiabilité humaine. Aspects qualitatifs et/ou quantitatifs. *Préventique*, 1987, 14, pp. 44-48 et 70.
- FAVERGE J.M. – L'homme agent d'infiabilité et de fiabilité du processus industriel. *Ergonomics*, 1970, 13, 3, pp. 301-327.
- FERAUGE C. – Rapport au Ministère de l'environnement du groupe de travail sur la prévention des risques industriels. Paris, Conseil supérieur des installations classées, 1984.
- GOLIGER J., LIEVENS C. – La sécurité des systèmes. *Le Monde*, 14 juillet 1976, p. 10.
- GUILLERMAIN H., FADIER E., NEBOIT M. – Ergonomie cognitive et fiabilité humaine : proposition d'une méthodologie commune appliquée à une situation de contrôle de processus discontinu. In : DE KEYSER V., VAN DAELE A. – L'ergonomie de conception. Bruxelles, De Boeck Wesmael, 1989, pp. 205-210.
- HANNAMAN G.W., SPURGIN A.J., LUKIC Y.D. – Human cognitive reliability model for PRA analysis. Palo Alto, document NUS-4531, 1984.
- HO M.T. – Réflexions sur l'analyse de la sécurité des systèmes, ses méthodes et ses problèmes. *Cahiers de Notes Documentaires*, 1976, 85, pp. 571-580, ND 1037.
- IEEE - Guide to the collection and presentation of electrical, electronic and sensing component reliability data of nuclear power generation stations, IEEE Std-500, 1977.
- KUMAMOTO H., HENLEY J.E. – Top-down algorithm for obtaining prime implicants sets of non-coherent fault trees. *IEEE Transactions on Reliability*, 1978, R-27, 4, pp. 242-249.
- LAGADEC P. – Le risque technologique majeur. Paris, Pergamon, 1981.
- LAGADEC P. – Défaillances technologiques majeures et grandes situations d'urgence. 1re partie. *Travail et Méthodes*, 1987, 450, pp. 33-37.
- LAPLACE R. – Critère de fiabilité des systèmes électroniques. *Electronique Applications*, 1987, 54, pp. 37-41.
- LEPLAT J. – Erreur humaine, fiabilité humaine dans le travail. Paris, Armand Colin, 1985.
- LEONTIEV K., LERNER A., OCHANINE D. – Sur quelques tâches dans l'investigation du système « homme-machine automatique ». *Voprosy Psikhologii*, 1961, 1, pp. 13-21.
- LEWIS H.W. et coll. – Risk assessment review group. Springfield, U.S Nuclear Regulatory Commission, National Technical Information Serie, NUREG/CR-0400, 1978.
- LIEVENS C. – Sécurité des systèmes. Toulouse, CEPADUES, 1976.
- LOCKS M.O. – Fault trees, prime implicants and noncoherence. *IEEE Transactions on Reliability*, 1980, R-29, 2, pp. 130-135.
- LOUET M., BARRAULT P. – La sécurité des systèmes, un exemple d'application. *Revue Générale de Sécurité*, 1986, 54, pp. 27-34.
- MONTEAU M., PHAM D. – L'accident du travail : évolution des conceptions. In : LEVY-LEBOYER C., SPERANDIO J.C. – Traité de psychologie du travail. Paris, PUF, 1987, pp. 703-727.
- MORLAT G. – Grands risques et probabilités. *Culture Technique*, 1983, 11, pp. 103-107.
- NARAYANAN H.N., WISWANADHAM N. – A methodology for knowledge acquisition and reasoning in failure analysis of systems. *IEEE Systems, Man and Cybernetics*, 1987, SMC-17, 2, pp. 274-288.
- PAGES A., GONDRAN M. – Fiabilité des systèmes. Paris, Eyrolles, 1980.
- RASMUSSEN J. – Information processing and human-machine interaction. New-York, Amsterdam, Londres, North-Holland, 1986.
- RASMUSSEN N. et coll. – Reactor safety study. Springfield, US Nuclear Regulatory Commission, WASH-1400, NUREG -75 10 14, 1975.
- SARRAT P., N'KAOUA M. – La sécurité des systèmes appliquée en conception : l'étude d'une paroi. *Revue générale de Sécurité*, 1986, 54, pp. 31-34.
- SCHWEITZER A., GERARDIN J.P. – Méthodes permettant d'améliorer le niveau de sécurité des systèmes à logique programmée. *Electronique, Techniques et Industries*, 1984, 12-13, pp. 51-56 et pp. 39-49.
- SIGNORET J.P., LEROY A. – La prévision du risque technologique. *La Recherche*, 1986, 183, pp. 1596-1607.
- SNYDER H.L. et coll. – Critical human factors issues in nuclear power regulation and recommended comprehensive human factors long-range plan. Springfield, US Nuclear Regulatory Commission, NUREG/CR-2833, 1982.
- STARR C. – Social benefit versus technological risk. *Science*, 1969, 165, 3899, pp. 1232-1238
- SUTTER A., TRÖXLER R. – Modèle d'analyse de la sécurité des systèmes à la conception et en fonctionnement. Actes du Colloque AITASA. Bordeaux, IUT, 1987.
- SWAIN A.D., GUTTMAN H.E. – Handbook of human reliability analysis with emphasis on nuclear power plant applications. Albuquerque, Sandia National Laboratory, NUREG/CR-1278, SAND 80-0200, 1983.
- TRICOT C., PICARD J.M. – Ensembles et statistique. Montréal, Mc Graw Hill, 1969.
- UNION DES INDUSTRIES CHIMIQUES (UIC) – Cahier de sécurité n° 1 – L'analyse préliminaire des risques. Cahier de sécurité n° 4 – L'analyse des modes de défaillance des effets et des probabilités. Paris, UIC, 1981 a et b.
- VILLEMEUR A. – Sureté de fonctionnement des systèmes industriels. Paris, Eyrolles, 1988.
- WANNER J.C. – Etude de la sécurité des aéronefs en utilisation (ESAU). Service technique aéronautique, 1969.

Reçu en février 1989, accepté en juin 1989 ■

INSTITUT NATIONAL DE RECHERCHE ET DE SÉCURITÉ
30, rue Olivier-Noyer, 75680 Paris cedex 14

Tiré à part des Cahiers de notes documentaires, 2e trimestre 1990, n° 139 - ND 1779 - Réimpression octobre 1996 - 1 000 ex.
N° CPPAP 804 AD/PC/DC du 14-03-85 - Directeur de la publication : J.L. MARIE
ISSN 0007-9952 - ISBN 2-85599-934-0