Fondamentaux de l'analyse de risque

Regard fiabiliste sur la sécurité industrielle

Yves Mortureux

Edition coordonnée par Clotilde Gagey et Caroline Kamaté

n° 2016-02

Les Regards sur la sécurité industrielle

FONCSI
Fondation pour une culture de sécurité industrielle

La Fondation pour une culture de sécurité industrielle (Foncsi) est une Fondation de Recherche reconnue d'utilité publique par décret en date du 18 avril 2005. La Foncsi finance des projets de recherche autour des activités à risque et souhaite favoriser l'ouverture et le dialogue entre l'ensemble des acteurs (administrations, associations, collectivités, équipes de recherche, entreprises, organisations syndicales, *etc.*).

L'originalité de sa démarche repose sur l'interdisciplinarité de ses travaux, en France et à l'international, ainsi que sur sa volonté affirmée d'innover et d'anticiper les enjeux de demain.

La Foncsi s'est fixé quatre missions :

- Faire émerger les nouvelles idées et les pratiques innovantes
- Développer, soutenir et financer la recherche
- Contribuer à l'essor d'une communauté de recherche
- Rendre accessibles les connaissances à l'ensemble du public

La communauté autour de la sécurité industrielle est sur www.foncsi.org **!**

- Découvrez et téléchargez gratuitement l'ensemble des publications : Cahiers de la sécurité industrielle, Regards…
- Partagez des informations – appels à communications et propositions scientifiques, manifestations, offres d'emploi… – dans la rubrique Communauté/Rézotons
- Explorez la carte des laboratoires et chercheurs, de toutes disciplines, investis dans la sécurité industrielle et développez votre réseau. Vous n'êtes pas référencés ? C'est tout simple, cliquez ici !
- Enfin, faites connaître vos idées, entrez dans la communauté et commentez les articles, proposez une Tribune…

Ce document

Titre	Fondamentaux de l'analyse de risque, regard fiabiliste sur la sécurité industrielle
Mots-clés	sûreté de fonctionnement, analyse de risque, probabilisme, déterminisme
Auteur	Yves Mortureux
Date de publication	Juillet 2016

Clotilde Gagey et Caroline Kamaté ont coordonné l'édition de ce *Regard sur la sécurité industrielle*. Les opinions qui y sont exprimées sont celles de l'auteur, seul.

À propos de l'auteur

Ingénieur de l'École nationale des Ponts et Chaussées, Yves Mortureux a effectué sa carrière professionnelle au sein de la SNCF (les dernières années à l'Union internationale des chemins de fer) dans les domaines de l'exploitation, de la sécurité, du retour d'expérience et des FHOS. Reconnu comme expert en sûreté de fonctionnement, il s'est fortement impliqué à l'Institut de sûreté de fonctionnement, dont il a assuré la vice-présidence. Il préside à l'IMdR la commission « Groupe de travail et de réflexion », et est membre de la commission scientifique « Risques accidentels » de l'Ineris.

Pour citer ce document

Mortureux Y. (2016). *Fondamentaux de l'analyse de risque, regard fiabiliste sur la sécurité industrielle.* Numéro 2016-02 de la Collection *Les Regards sur la sécurité industrielle*, Fondation pour une culture de sécurité industrielle, Toulouse, France.

Gratuitement téléchargeable sur : http://www.foncsi.org/.

Table des matières

Introduction

Ce *Regard* se veut celui de la sûreté de fonctionnement sur le risque industriel. La sûreté de fonctionnement n'est pas une discipline scientifique clairement reconnue. Il n'y a en effet pas de nom pour le métier ou la compétence associé. Nous utiliserons le terme de « fiabiliste » pour désigner ces professionnels de la sécurité, de la maîtrise des risques qui mettent en œuvre les concepts, les démarches et les méthodes de la sûreté de fonctionnement. Ce n'est pas une discipline scientifique reconnue, mais de nombreuses sciences sont sollicitées et certains de ses outils sont utilisés par d'autres métiers. C'est une matière d'enseignement et de recherche qui se place soit transversalement en se reconnaissant pluridisciplinaire, soit en se nichant dans une spécialité bien identifiée (mécanique, mathématiques, statistiques, sciences de l'information). Dans les deux cas, les personnes qui s'y consacrent dans le cadre universitaire souffrent d'un manque de reconnaissance et d'un défaut d'identité.

Le métier de fiabiliste est, par contre, assez présent dans les industries dites « à risques », surtout dans les grandes entreprises. Il n'existe sans doute que peu d'emplois définis comme fiabiliste ou un terme équivalent, et ce n'est probablement pas une façon recommandable de se présenter pour un chercheur d'emploi. Toutefois, nombre d'équipes projet et de services hygiène sécurité, environnement (HSE) ou sécurité emploient des spécialistes pour leurs compétences en sûreté de fonctionnement ; et c'est de l'approche du risque de ces spécialistes qu'il sera question ici.

Ce *Regard* tente de présenter les éléments centraux (concepts, méthodes, démarches) et bien partagés qui caractérisent cette « discipline ». Ce n'est pas un cours, même de base, il s'en faut. Il s'en tient aux classiques qui forment le noyau de la culture des fiabilistes et ne s'aventure pas dans les développements récents.

Ce *Regard* ne couvre pas toute la sûreté de fonctionnement, ni toutes les activités des fiabilistes. Il est limité à leurs contributions à la maîtrise des risques d'accidents, donc à la composante « sécurité » de la sûreté de fonctionnement. La couverture de leurs apports aux composantes Fiabilité-Maintenabilité-Disponibilité (*dependability* en anglais) et associées nécessiterait d'importants compléments, un autre *Regard* peut-être.

1

Le mot-clé : risque

« Risque » est le mot-clé le plus central de l'approche du fiabiliste : le métier du fiabiliste est construit autour de la combinaison de deux dimensions, la fréquence et la gravité, pour caractériser ce qu'on appelle le risque. Mais fréquence et gravité de quoi ?

Risque

Définition

La définition de « risque » arrive en tête de nombre d'ouvrages didactiques ou de normes. La définition la plus classique est celle d'un couple « fréquence – gravité ». Comme il est très important de bien préciser fréquence et gravité de quoi, nous le définirons comme une triplette « événement – fréquence – gravité ».

Aujourd'hui, ont fleuri nombre d'autres définitions qui tendent à élargir le domaine traité[1]. Toutefois, l'approche fiabiliste fondamentale présentée dans ce *Regard* est basée sur cette idée simple de la combinaison des deux dimensions fréquence et gravité. Elle permet d'aborder efficacement la question de ces événements dont on sait qu'ils peuvent arriver, mais dont il est plus difficile de savoir si c'est souhaitable, acceptable ou excessif.

Divers secteurs, divers pays, diverses époques ont mis en valeur à côté de fréquence et gravité, d'autres dimensions dont la plus souvent citée est la détectabilité.

Détectabilité

Définition

La détectabilité concerne généralement des questions de forme, de façon de présenter les choses : on peut définir la détectabilité de l'événement E, ou évaluer fréquence et gravité des deux événements, « E détecté » et « E non détecté ».

1.1 En regardant dans le rétroviseur

Les démarches visant à construire, entretenir et exploiter avec le souci que cela fonctionne, longtemps et sans accident, sont aussi vieilles que l'humanité. En faire l'histoire serait riche et passionnant, mais hors sujet. Toutefois un tournant paraît devoir être mis en valeur pour bien comprendre le fiabiliste d'aujourd'hui : l'exploitation systématique et poussée de régularités statistiques.

Les démarches pour se prémunir des mauvaises surprises relèvent d'aussi loin qu'on puisse remonter :

- du déterminisme, quand les connaissances étaient suffisantes pour prédire[2] ;
- de la mise en œuvre de règles de l'art et des codes établis, surtout par l'expérience et l'exploitation des connaissances accessibles[3] ;
- d'un certain fatalisme à l'égard d'événements qu'on ne sait ni prédire ni prévenir.

1. Par exemple : « effet de l'incertitude sur les performances ».
2. Et c'est toujours aussi vrai.
3. Cette approche joue toujours un très grand rôle même si elle n'est guère valorisée.

Définition

Approche déterministe

Le déterminisme est une philosophie selon laquelle tout phénomène résulte d'une chaîne de causes, et les mêmes causes produisent toujours les mêmes effets. Dans ce contexte, il s'agit des approches qui consistent à prévoir les événements à venir à partir de l'identification des conditions et événements initiaux, en développant la suite des enchaînements causes-conséquences.

Définition

Approche probabiliste

Des approches non déterministes peuvent être probabilistes en attribuant à des événements à venir des probabilités de se produire à partir des conditions et événements initiaux.[4]

Il existe toujours des phénomènes vis-à-vis desquels, en l'état de nos connaissances, nous sommes totalement démunis[5]. D'autre part, il y a de nombreuses familles de phénomènes dont on est toujours incapable de prédire l'apparition (et les conséquences) mais dont on sait toutefois qu'elles présentent des régularités statistiques et peuvent donc être modélisées par des lois de probabilité.

L'arrivée de l'électronique dans l'industrie — avec des composants dont on ne savait prédire lequel durerait et lequel tomberait en panne alors qu'on constatait une régularité statistique dans la fraction d'un lot tombant en panne par unité de temps — puis l'avènement des moyens permettant d'établir et de traiter des séries statistiques (selon la « loi des grands nombres ») ont conduit au développement rapide (à partir de la deuxième guerre mondiale à peu près) des approches et des concepts qui font la base du métier de fiabiliste.

1.2 Les trois composantes du risque

Pour préciser la vision du fiabiliste de ce concept de risque, il paraît intéressant de faire quelques commentaires sur ses trois composantes.

1.2.1 L'événement redouté

« Événement redouté » est l'expression la plus consacrée en matière de sécurité pour désigner l'événement incertain qu'on va caractériser en fréquence et gravité. L'expression traduit bien l'état d'esprit a priori qui veut qu'on travaille sur les événements indésirables. Toutefois, les approches s'appliqueraient de même aux « coups de chance » qu'aux « coups de malchance ». Des voix s'élèvent régulièrement avec un succès d'estime pour rappeler aux acteurs de l'industrie qu'il peut y avoir gros à gagner en travaillant au risque « positif », aux « opportunités » et pas seulement aux malheurs[6].

L'important ici va être une définition assez précise et opérationnelle de l'événement redouté. En effet, la qualité de la définition de chaque événement redouté étudié est décisive pour la pertinence de la démarche quelle qu'elle soit.

Exemple

Qu'est-ce qu'un déraillement ?

On discute longuement dans le détail : « *un déraillement, c'est une roue à côté du rail, ou les deux d'un même essieu ou tout un véhicule ? Si la roue est entièrement montée sur le rail, est-ce un déraillement ou pas ? Et si l'essieu a perdu une roue, est-ce un déraillement ? Etc.* » ; mais on néglige, parce que ça paraît évident à chacun : « *un véhicule qui déraille consécutivement à un choc avec un obstacle, est-ce un déraillement ? Un déraillement provoqué volontairement pour protéger d'une dérive par exemple, est-ce un déraillement ? Et s'il résulte d'un sabotage ? Etc.* », en ignorant que chacun a une réponse différente à ces questions en raison de son métier par exemple (financier, statisticien, juriste, etc.).

Cette question est trop souvent mal traitée parce qu'on y répond comme si c'était un contrôle de connaissance, et que la réponse juste était celle du dictionnaire, de la norme ou de l'expert. Or, **la bonne réponse est celle qui correspond à l'objectif de l'étude de risque**.

4. On peut être encore plus limité et ne savoir qu'identifier des événements possibles sans pouvoir associer rigoureusement des lois de probabilité à leurs survenues…
5. C'est là que le principe de précaution intervient.
6. Voir une définition économique du risque dans le *Regard sur la sécurité industrielle* n° 2014-02.

Le périmètre du système étudié influence aussi la définition. Si on se préoccupe du scénario d'accident selon lequel une personne est blessée en recevant une charge suspendue qui se détacherait intempestivement, travailler sur l'événement « détachement intempestif de la charge du pont » donnera des résultats très différents de travailler sur l'événement « une personne est blessée en recevant une charge se détachant intempestivement du pont roulant ». L'étude du premier événement ne permet pas d'envisager des mesures empêchant de passer sous la charge par exemple. Pourtant, c'est une erreur qui entache nombre d'études de risque. Il est alors primordial de définir précisément les limites du système étudié, une fois de plus en fonction des objectifs, en se posant la question : « sur quoi peut-on agir ? »

Exemple

Définition du système étudié

Dans le cadre de l'achat d'un système « clé en main », on se limitera probablement à l'étude du système technique. Alors que dans le cas d'un système dont le comportement dépend fortement de son utilisation, on prendra également en compte l'humain (erreur humaine, voire mauvaise utilisation, vandalisme, terrorisme, etc.), d'où la nécessité de borner ce qui est considéré dans l'étude. La prise en compte de l'humain peut se faire en termes d'opérateur/utilisateur, de mainteneur, d'exploitant, etc.

La prise en compte du contexte est aussi couramment négligée. Pour réaliser une étude sur les risques d'accidents en tunnel ferroviaire, on veut connaître la fréquence d'un déraillement de train (par train, par kilomètre parcouru). Mais en ne précisant pas le contexte « tunnel » ni les différents scénarios conduisant au déraillement, on introduit un paramètre totalement faux, car la fréquence de cet événement en tunnel est très différente de sa moyenne toutes conditions confondues.

Et il est une erreur de raisonnement encore plus étonnante, mais assez répandue, qui consiste à ne pas être clair ou ne pas être constant sur la définition de la consistance du système auquel on applique une démarche de sûreté de fonctionnement. Cette erreur se manifeste couramment sous la forme suivante : le retour d'expérience (les statistiques) montre que tel type d'accident (rupture de garde-fou en hauteur, fuite de gaz…) n'est pas grave, donc on se permet d'alléger les mesures de sécurité… alors que c'est justement grâce à ces mesures que ces accidents ont des conséquences légères. On retient une information tronquée : « ce type d'événement cause en moyenne quelques dégâts matériels et, parfois, quelques blessures légères » ; et on oublie : « quand telle, telle et telle mesures sont prises et fonctionnent (harnais de sécurité, ventilation, etc.) ».

1.2.2 La fréquence

À première vue, cette notion est simple et claire.

Définition

Fréquence

La fréquence est le nombre d'événements — correspondant à la définition du système étudié —, divisé par le temps sur lequel ils ont été relevés.

En réalité, on constate beaucoup de confusion entre des notions de fréquence (inverse d'un temps), de probabilité (sans dimension) et de taux[7].

De plus, il est nécessaire d'expliciter le temps dont il s'agit : ce peut être le temps qui passe ou le temps sous tension ou le temps d'utilisation, etc. Ce temps peut s'exprimer dans des unités inattendues : nombre de manœuvres (d'un interrupteur), nombre de cycles (charge-décharge), tonnes (charges supportées par un rail par exemple), watts (transmis par un circuit électrique), octets d'informations, etc.

La variété de ces unités ne résulte pas de la fantaisie du fiabiliste qui la subit, mais découle des constats qui peuvent être faits de régularités statistiques. Selon les composants, équipements et systèmes pour lesquels on a la chance de constater des régularités statistiques exploitables, il se trouve que cette régularité apparaît avec telle ou telle unité de temps. À ce stade du constat des régularités et de leur modélisation en probabilités, une grande prudence s'impose.

7. Souvent inverse d'un temps mais pas toujours, et qui peut s'exprimer dans des unités inattendues.

Exemple

Erreur de modèle de probabilité

Imaginons un interrupteur manœuvré très régulièrement dans une pièce qui connaît un cycle chauffage-refroidissement journalier. On pourrait trouver une régularité entre les pannes des interrupteurs et le nombre de manœuvres ou le temps qui passe ou les cycles de température, puisque ces données « temporelles » sont corrélées entre elles (même proportionnelles). On pourrait imprudemment en déduire un modèle de probabilité de défaillance avec une grandeur inappropriée — comme la température alors qu'il y aurait une véritable régularité statistique entre les pannes et le nombre de manœuvres — de sorte que, dans un autre contexte, le modèle serait complètement faux.

La difficulté pratique qui découle de cette variété d'unité est que, durant une étude sur un système qui comporte diverses technologies, on va combiner des temps exprimés dans des unités différentes. Pour ce faire, on va convertir en faisant des hypothèses : le nombre de manœuvres se convertit en temps qui passe en supposant « tant de manœuvres par an », etc. Cependant, le résultat de l'étude n'est valide qu'avec toutes ces hypothèses qu'il a fallu faire pour intégrer les divers éléments du système. Il est trop courant, malheureusement, de perdre de vue ces réserves à l'énoncé des résultats ; il est bien sûr possible, mais souvent très difficile, de produire des conclusions sous forme de fonction des valeurs de ces conversions temporelles.

1.2. 3 La gravité

La gravité semble aussi à première vue une notion simple et familière. Elle pose cependant une colle majeure aux fiabilistes : elle est subjective dans le sens originel du terme, elle dépend de pour qui on l'évalue. Un événement (défini de façon claire et univoque) n'a pas du tout la même gravité pour Pierre ou pour Jacques, pour la société ou pour telle entreprise, etc. Et si choquant que ce soit pour certains, c'est tout à fait normal.

2

Les notions fondamentales

Dans l'activité du fiabiliste, gravite autour de cette notion centrale de risque un ensemble hétérogène de notions que nous effleurerons ici. Il va de soi que cette liste est critiquable, on pourrait en évoquer d'autres, en supprimer aussi.

2.1 Analyse fonctionnelle et notion de système

Le fiabiliste travaillant sur les potentiels échecs, pannes et défaillances se réfère nécessairement à l'expression de ce qu'on attend de l'objet, de la machine, du service… Autrement dit, de ce qu'on qualifie de « bon fonctionnement » et ce qu'on qualifie de « non-fonctionnement ». Aussi, l'analyse fonctionnelle (identification, caractérisation de ce qui est attendu) et la notion de système (des éléments en interaction pour une activité donnée dans des conditions données) sont des fondamentaux. Une présentation de la démarche d'analyse de risques commence très souvent par l'analyse fonctionnelle. Les avis peuvent diverger pour considérer l'analyse fonctionnelle comme faisant partie de la sûreté de fonctionnement et du métier du fiabiliste, ou la décrire comme une démarche autre sur laquelle le fiabiliste doit s'appuyer.

2.2 Risque *versus* danger

C'est un véritable pont aux ânes de la discipline que de s'insurger contre la confusion entre risque et danger. Si les définitions sont quasiment innombrables et l'objet d'âpres discussions, elles tournent autour de la progression : le danger est un potentiel de nuisance, d'accident, d'atteinte aux personnes ou aux biens… La rencontre du danger avec un système génère une situation dangereuse… Le risque associe une évaluation, une mesure à une possibilité d'accident.

2.3 Rappel de probabilité

Le métier de fiabiliste est tellement associé à l'exploitation de modèles probabilistes que les cours et les livres sur la sûreté de fonctionnement commencent souvent par un chapitre « Rappel de probabilité ». Outre des bases générales du calcul de probabilité, on y trouve habituellement un accent mis sur les lois les plus courantes en sûreté de fonctionnement : Gauss, Poisson, Weibull, normale, log-normale, exponentielle, théorème de Bayes…

2.4 Taux de défaillance, lambda, mu et MTBF

Les lettres λ et μ sont devenues symboliques de la sûreté de fonctionnement au point d'avoir donné son nom (le λμ) au congrès français de sûreté de fonctionnement[1].

Définition

Taux de défaillance - λ

λ est le symbole du taux de défaillance. Le taux de défaillance d'un système à un instant t est le rapport de la probabilité que ce système, non défaillant à l'instant t, ait cette défaillance entre t et t+dt à la durée dt.

1. Le plus important au monde, comparable au RAMS américain.

Définition

Taux de réparation - μ

μ est le symbole du taux de réparation : la probabilité que le système en panne à l'instant t soit réparé entre t et t+dt divisée par dt.

Le MTBF est un sigle très utilisé et très apprécié, mais qui prête à des interprétations divergentes et à des quiproquos.

Dans sa version anglaise, il signifie : *Mean Time Between Failures*. Il s'agit donc de la moyenne des temps séparant deux défaillances successives.

Dans sa version française, il signifie : moyenne des temps de bon fonctionnement.

La différence est que le temps entre défaillances (*Time Between Failures*) est la somme du temps de bon fonctionnement (*Up Time* en anglais) et du temps de réparation (*Down Time* en anglais). Donc, en sigles, dans la version anglaise :

MTBF = MUT + MDT (où le MUT anglais est le MTBF français)

Si les durées d'indisponibilité du système pour réparation sont très courtes, négligeables par rapport aux durées de fonctionnement continu sans panne, les valeurs des deux versions du MTBF sont assez proches pour que la confusion ne prête pas à conséquence, mais ce n'est pas toujours le cas.

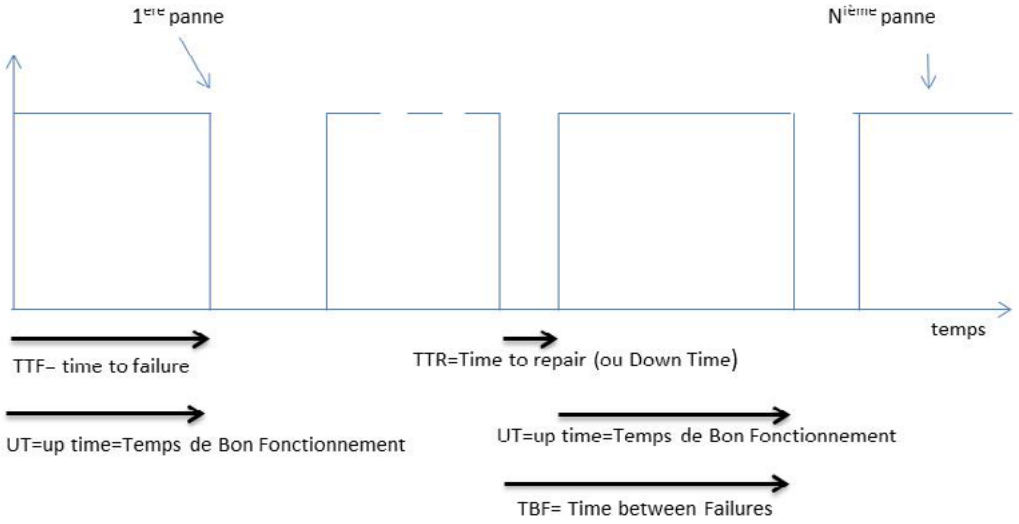

FIG. 2.1 — *Représentation des deux versions du MTBF*

Parmi les confusions très répandues, un client, un donneur d'ordre, exprimant son exigence sous forme de MTBF, pense qu'il exprime ainsi une durée pendant laquelle il peut légitimement espérer un fonctionnement exempt de pannes. Or, il en va assez différemment. Par exemple, dans le cas le plus simple mathématiquement où le taux de défaillance est constant dans le temps, la probabilité de ne pas avoir de panne pendant une durée égale à 1 MTBF (version anglaise) n'est que de 0,368 !

2.5 Diagramme de Farmer, criticité, modèles quasi-normalisés en boîte

Le diagramme fréquence-gravité, dit aussi diagramme de Farmer, représente de façon synthétique le risque et les plus importants concepts associés. Il se présente comme un cadran d'un espace à deux dimensions qui sont la fréquence (F) et la gravité (G) ; un point de cet espace représente un événement. Avec sa position, une fréquence et une gravité, il représente un risque.

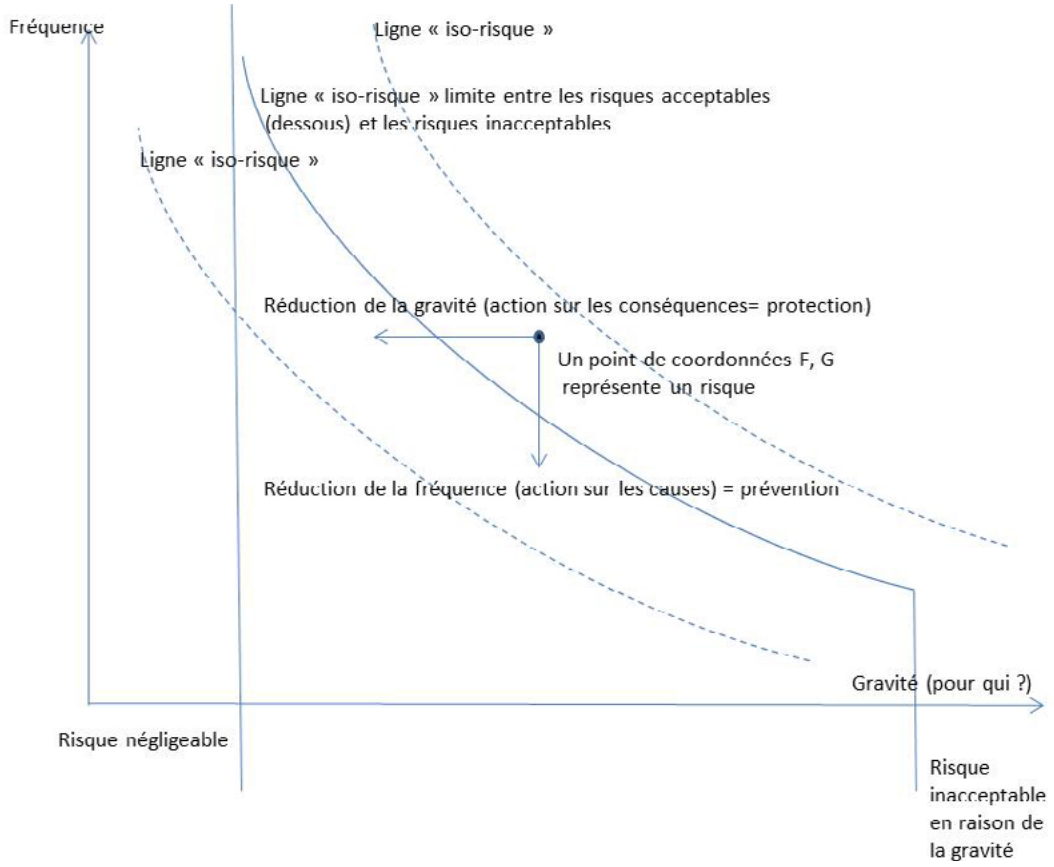

FIG. 2.2 — *Diagramme de Farmer*

L'essence même de la mesure du risque est bidimensionnelle, mais il n'est pas simple de manipuler (comparer, voire additionner ou soustraire) des grandeurs bidimensionnelles. Aussi est-il très tentant de réduire le couple (F, G) à une valeur unique qui serait le niveau de risque. Comme fréquence et gravité sont usuellement représentées par des chiffres, il est hélas très courant de croire que multiplier l'un par l'autre donne une représentation juste du niveau de risque. Ce n'est vrai en fait que sous des conditions assez strictes et pas si souvent réunies :

- les chiffres représentant fréquence et gravité doivent être des quantités et non des échelles (nombre d'événements par an et coût en euros par exemple, mais pas 1, 2, 3 et 4 correspondant à des classes de fréquence ou de gravité) ;
- les valeurs restent équivalentes d'un bout à l'autre de l'échelle.

Cette dernière condition est rarement réalisée pour la gravité. Par exemple, généralement, « une fois dix décès » n'est pas équivalent à « dix fois un décès ». Et, si on évalue le coût d'un décès à 1 million d'euros par exemple, il ne sera quand même pas équivalent à mille incidents coûtant 1 000 euros en moyenne, tant des aspects non pécuniaires pèsent lourd dans l'appréciation de la gravité d'un accident mortel. Il est usuel et pratique de compter en « équivalent-mort », mais la réalité est généralement significativement plus complexe et plus multidimensionnelle.

Définition

Criticité

Il est usuel d'appeler « criticité » le niveau de risque, mesure unidimensionnelle résultant de la combinaison de la fréquence et de la gravité.

Malheureusement, le terme « criticité » est aussi couramment utilisé dans un sens quasi-synonyme de gravité. Pour éviter les confusions dans ce *Regard,* nous l'éviterons et parlerons de niveau de risque.

Dans le diagramme de Farmer, les lignes définies par le fait que les points qui les constituent présentent des risques équivalents sont appelées lignes iso-risque. L'idée de bon sens est que fréquence et gravité

se compensent de sorte qu'on considère équivalents deux risques, l'un étant plus fréquent et moins grave que l'autre.

Cette représentation bidimensionnelle du risque prend souvent la forme d'une matrice : la fréquence et la gravité sont divisées en classes (généralement 3 à 5), et chaque case qui correspond à un couple (classe de fréquence/classe de gravité) reçoit une identification en niveau de risque (souvent appelée criticité dans ce contexte). Les cases sont généralement colorées en rouge (risque inacceptable), orange ou jaune (à réduire si raisonnablement possible) ou vert (acceptable) qui représentent trois « niveaux d'acceptabilité » (mais il peut y en avoir que deux ou plus de trois). Cette représentation, assortie de processus de construction et d'utilisation, est très répandue et très utilisée. Malheureusement, il est très fréquent que de très gros défauts entachent ces méthodes.

Gravité / Fréquence	mineur	significatif	grave	catastrophique
rare				
courant				
fréquent				

risque acceptable — risque à réduire — risque inacceptable

FIG. 2.3 — *Matrice de représentation du risque*

2.6 Prévention, protection, risque acceptable

Dans un diagramme de Farmer, parmi les lignes iso-risque, on peut en distinguer une qui représente la frontière entre les risques acceptables (en dessous) et les risques inacceptables, donc à réduire (au-dessus). Des mesures qui réduisent la fréquence d'un risque relèvent de la prévention, des mesures qui réduisent la gravité d'un risque relèvent de la protection.

2.7 Défense en profondeur, redondance, rattrapage

Pour atteindre des fréquences très basses (obligation en particulier vis-à-vis des événements graves), il est très rare qu'on puisse se contenter d'une mesure de fiabilité très élevée. On a donc recours à un empilement de mesures, de barrières de sécurité… Il s'agit de faire en sorte, par construction, qu'un accident ne puisse effectivement résulter que de la coïncidence de plusieurs erreurs et défaillances. On parle alors de défense en profondeur, de redondance et de possibilité de rattrapage.

Le concept de défense en profondeur très souvent cité aujourd'hui est sans doute aussi vieux que l'humanité. Avant les exemples modernes (classiquement, les trois enceintes qui séparent le combustible nucléaire d'une centrale de l'environnement), on cite souvent les fortifications « à la Vauban ». En fait, les fortifications des camps romains décrites par César dans *De bello gallico* en sont déjà un magnifique exemple.

L'image la plus courante aujourd'hui dans l'industrie est celle popularisée par James Reason et accompagnée de l'expression « *Swiss cheese model* » c'est-à-dire le modèle du « fromage suisse ».

Dans tous les cas de figure, il s'agit de représenter l'idée que l'événement grave, dont la probabilité doit être réduite à une valeur très basse, ne peut se produire que par combinaison simultanée de plusieurs événements redoutés[2]. La prévention de cet accident, mesurée par la probabilité de cet événement grave, résultera donc de la combinaison des trois facteurs suivants :

- le nombre de barrières (nombre d'enveloppes autour du combustible nucléaire par rapport au risque de dispersion dans l'environnement de cette matière radioactive ; nombre

2. Ici, comme plus loin dans le texte, « simultané » ne signifie pas que les événements, les défaillances surviennent au même instant, mais qu'à un moment donné les deux ou trois sont présents simultanément.

d'obstacles, fossés, rempart, rangées de pieux… à franchir pour un assaillant du camp romain ou de la place forte ; nombre de tranches de fromage dans le « *Swiss cheese* model » ; etc.) ;

- ▹ la fiabilité de chacune des barrières (chaque enveloppe, chaque fortification, chaque tranche de fromage) ;
- ▹ l'indépendance des barrières.

Ce dernier point est le plus délicat et souvent le cheval de Troie de systèmes de défense. En effet, s'il existe une cause, un événement, qui peut à lui seul provoquer la défaillance de plusieurs des barrières, il n'y a plus la défense en profondeur qu'on croyait. Par exemple, si un événement mettait en défaut toutes les barrières, on ne pourrait plus dire qu'un accident ne peut résulter que de la coïncidence de plusieurs erreurs ou défaillance puisqu'un scénario à une seule cause peut aboutir à l'accident grave. Rechercher ces cas dits de cause commune de défaillance n'a rien d'évident. Un certain nombre d'accidents montre a posteriori l'existence de cas où une défaillance, une erreur ou un événement externe défavorable suffisait à provoquer un accident grave ou une catastrophe alors qu'on se croyait en situation de défense en profondeur où seule la coïncidence de trois (ou plus) événements défavorables indépendants pouvait provoquer l'accident. Le cas trivial, mais pas si rare que cela, est celui du défaut d'alimentation (électrique par exemple) qui met en panne toutes les barrières.

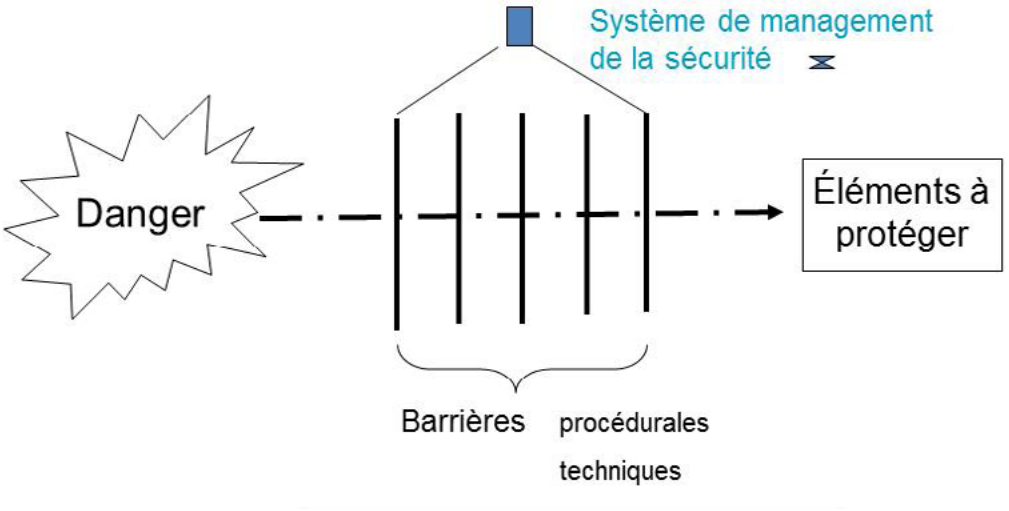

FIG. 2.4 — *Solidité, indépendance et nombre suffisant de barrières*

Un point faible assez répandu dans les systèmes de prévention d'accident conçus sur le modèle de la défense en profondeur est l'existence de défaillances dites « latentes ». Il s'agit de défaillances qui peuvent persister de longue date : en l'absence de conséquence visible tant que d'autres ne viennent pas se combiner avec elles, elles ne seraient pas détectées et le système ne serait pas réparé ou corrigé. En général, elles ne sont pas pour autant indétectables. Cependant si la surveillance, la veille, le retour d'expérience ne reposent que sur le signalement d'événements affectant la sécurité ou la performance et n'incluent pas une recherche volontariste d'éventuelles défaillances, on peut fonctionner longtemps avec un système n'ayant en réalité de fonctionnelles que deux barrières au lieu de trois (ou une au lieu de deux… voire une au lieu de trois).

2.8 Sûreté de fonctionnement et FMDS

Enfin, venons-en à l'expression spécifiquement française dont on ne connaît pas d'équivalent dans d'autres langues : « sûreté de fonctionnement ».

Définition

Sûreté de fonctionnement

Cette expression s'est peu à peu imposée pour décrire l'ensemble des démarches, des concepts, des méthodes convoqués pour traiter les risques d'un système conçu, réalisé, mis en œuvre, et maintenu par des hommes, qui ne rendrait pas les services prévus ou causerait des dommages inacceptables.

Le périmètre exact du concept évolue dans le temps, plutôt en élargissant son champ de pertinence (contributions aux démarches de maîtrise des risques naturels, sociaux, géopolitiques, financiers, etc.) et avec les personnes impliquées.[3]

Trois notions sont assez intéressantes pour cerner les débats qui entourent les définitions de la sûreté de fonctionnement : le maintien de la qualité dans le temps, la science des défaillances et la FMDS.

2.8.1 Le maintien de la qualité dans le temps

La proximité des objectifs de démarches qualité et de la sûreté de fonctionnement, ainsi que l'omniprésence pendant quelques années de la vague « Qualité » au sens norme ISO 9000, ont fait que pendant ces années les débats sur la définition de la sûreté de fonctionnement ont surtout tourné autour de sa position par rapport à la qualité. Les vigoureux débats sur « laquelle est une partie de l'autre ? » étaient beaucoup le reflet de rivalité sur « qui du fiabiliste ou du qualiticien serait le chef de l'autre ou le plus proche du président ou directeur général ? ». Toutefois, la définition suivante, « la sûreté de fonctionnement est le maintien de la qualité dans le temps », sans faire l'unanimité a été assez reconnue et a le mérite de souligner l'importance, l'essentialité de la durée dans l'approche du fiabiliste et, en même temps, une forte communauté d'objectifs avec la qualité.

2.8.2 La science des défaillances

On peut certes dénier à la sûreté de fonctionnement la qualité de science, le fait d'être une nouvelle science en soi. Cependant, cette définition – la sûreté de fonctionnement comme science des défaillances – a deux mérites. Elle souligne que la sûreté de fonctionnement, tout à fait typique du métier d'ingénieur et praticable par bien des personnes ayant reçu d'autres formations, s'appuie sur des connaissances scientifiques et utilise copieusement les mathématiques. D'autre part, cette définition souligne l'importance des connaissances sur les défaillances, les processus de leurs apparitions, leurs développements, etc. C'est important car on oublie parfois que, si merveilleuses que soient les méthodes mises en œuvre par le fiabiliste, la valeur de ses conclusions n'excédera pas la valeur et la justesse des connaissances et données exploitées par ces méthodes. La sûreté de fonctionnement ne nous apprendra rien sur un système dont on ne saurait rien, c'est une évidence qui demande parfois à être rappelée !

2.8.3 FMDS : fiabilité, maintenabilité, disponibilité et sécurité.

Ces quatre caractéristiques d'un système sont bien connues, avec les mêmes définitions dans de nombreuses langues.

Les définitions de fiabilité, maintenabilité et disponibilité sont très semblables et bien stabilisées ; les définitions de sécurité sont plus nombreuses et un peu plus diverses.

Définition

Fiabilité

Aptitude d'une entité à assurer des fonctions requises dans des conditions données pendant un temps donné. On ajoute souvent : elle se mesure par la probabilité R(t) que, le système assurant ces fonctions à l'instant 0, continue à les assurer jusqu'à l'instant t.

Définition

Maintenabilité

Aptitude d'un système à revenir en état d'assurer les fonctions requises dans les conditions données après une panne. On ajoute souvent : elle se mesure par la probabilité M(t) que le système, en panne à l'instant 0, soit réparé avant l'instant t.

3. Ce *Regard* étant spécifiquement orienté vers la sécurité est assez loin de couvrir toute la sûreté de fonctionnement, mais espère bien refléter les fondamentaux des approches « sûreté de fonctionnement ».

Définition

Disponibilité

Aptitude d'un système à être en état d'assurer les fonctions requises dans des conditions données. On ajoute souvent : elle se mesure par la probabilité A(t) que le système soit en état d'assurer les fonctions requises dans les conditions spécifiées à l'instant t.

Définition

Sécurité

Aptitude d'un système à ne pas causer de dommages inacceptables dans des conditions données. On ajoute souvent : elle se mesure par la probabilité S(t) qu'aucun accident n'ait été causé par le système de sa mise en service à l'instant 0 jusqu'à l'instant t.

La sûreté de fonctionnement est souvent définie comme l'ensemble de ces caractéristiques et comme l'ensemble des approches, méthodes permettant de les gérer ensemble.

Cependant, la traduction en anglais de la sûreté de fonctionnement française est un sujet de polémique : l'acronyme FMDS, pour Fiabilité, Maintenabilité, Disponibilité et Sécurité, a son équivalent RAMS (pour des raisons de consonance, il correspond lettre par lettre à FDMS). L'anglais emploie volontiers le terme de « *dependability* », que de nombreuses normes et autres documents présentent comme l'équivalent anglais de « sûreté de fonctionnement ». Certes, si on doit citer le terme anglais le plus proche de « sûreté de fonctionnement », ce sera « *dependability* », mais l'approche « *dependability* » couvre les dimensions F, M et D mais pas la sécurité *(safety)*. Le fait que, dans certains cas, certaines questions de sécurité se résument à la disponibilité d'un dispositif de sécurité (« *dependability* » est alors correct) conduit certains auteurs à affirmer que « *dependability* » couvre la sécurité. Ces confusions (comme autour de MTBF ou de criticité) peuvent générer quelques débats peu productifs mais aussi quelques malentendus lourds de conséquences. De plus, elles amplifient le phénomène totalement contre-productif de séparation de la dimension de sécurité des autres dimensions, quand elles sont tant liées dans la réalité. Ainsi, un système « sûr » mais très peu fiable/disponible sera rendu inactif, et la sécurité globale sera dégradée ; de même, un système très fiable, mais dangereux, ne sera pas non plus utilisé. Ces confusions peuvent amener à de graves conséquences financières, puisque le système ne serait pas adapté au besoin et devrait donc être reconçu ou remplacé.

3

Les approches basiques

Le fiabiliste met souvent en œuvre des méthodes dont quelques-unes sont si courantes qu'elles sont emblématiques de la sûreté de fonctionnement. Elles ont fait l'objet de nombreuses publications et, généralement, de normes. Elles sont si répandues qu'il en existe diverses versions. Ce chapitre tente de décrire l'essence des plus emblématiques.

3.1 AMDE(C)

L'analyse des modes de défaillances, de leurs effets et de leurs criticités est plus connue sous les acronymes AMDE et AMDEC.

Le résultat d'une AMDE est présenté dans un tableau. Dans la première colonne, le système étudié est séparé en composants. Dans la deuxième, chaque mode de défaillance du composant (c'est-à-dire la façon dont les défaillances se manifestent et affectent les fonctions du composant) est décrit. Dans la troisième, les effets de chaque mode de défaillance sur le système sont décrits. Dans une quatrième figure éventuellement une évaluation de la criticité.

Ceci constitue le noyau dur qui exprime le principe de l'AMDE. En pratique, les normes et les innombrables documents consacrés à l'AMDE(C) proposent tous des tableaux un peu ou beaucoup plus détaillés. Il en existe d'innombrables variantes selon les contextes. Toutefois, on peut mentionner les développements supplémentaires suivants comme très largement répandus :

- La décomposition du système en composants se présente souvent sur deux colonnes (ou trois ou plus) pour une présentation arborescente plus lisible (système, sous-systèmes, équipements, composants par exemple).
- Chaque composant est associé à l'identification de la fonction (voire des fonctions) à laquelle il contribue en référence à une analyse fonctionnelle préalable.
- La/les cause(s) possible(s) de chaque mode de défaillance est/sont mentionnée(s) dans une colonne, avant ou après la colonne « mode de défaillance ».
- Trois paramètres (répartis dans autant de colonnes) sont évalués pour chaque mode de défaillance et leur combinaison forme la criticité : la fréquence, la gravité et la non-détection (probabilité de). Cette évaluation de la criticité connaît d'importantes variantes, avec seulement fréquence et gravité ou au contraire plus de paramètres. On multiplie généralement « naturellement » fréquence, gravité et non-détection pour obtenir la criticité, mais il serait sain de s'interroger sur la pertinence de l'opération (Cf. § 2.5 dans « Notions fondamentales »).
- Une colonne action est souvent ajoutée en fin de tableau. On dépasse donc le stade de l'analyse pour déterminer les mesures à prendre en fonction des motivations pour lesquelles l'analyse a été menée.

L'AMDE(C) est qualifiée de méthode inductive. Elle a la réputation d'être exhaustive. En fait, cette exhaustivité résulte de son caractère systématique mais ne vaut que pour les conséquences des défaillances des composants du système avec une capacité très limitée à prendre en charge les combinaisons de causes, les effets du temps et dans la limite, bien entendu, de l'exhaustivité des connaissances réunies sur les éléments composant le système.

L'AMDE/AMDEC est une méthode extrêmement connue — ou que l'on croit connaître — au point d'être trop souvent assimilée à la méthode de maîtrise des risques. Outre les limitations mentionnées ci-dessus, il faut aussi noter que l'AMDEC permet d'attribuer des criticités aux modes de défaillance.

Pour traiter de l'acceptabilité des risques, il faut encore à partir de là évaluer la criticité (fréquence/gravité) des événements redoutés, car c'est à ce niveau-là que les critères d'acceptation du risque ont un sens et non au niveau des modes de défaillance des composants.

Fonction	Performances	Matériels	Caractéristiques	Modes de défaillance	Causes possibles de la défaillance	Effets possibles de la défaillance	G	P	Moyens de détection	Dispositions AQ pour le développement et la production	N°
Fonction étudiée	Performances caractérisant la fonction et contraintes	Matériel associé	Caractéristiques du matériel influente au regard des modes de défaillance	Modes de défaillance : -pas de fonction, - perte de la fonction, - fonction dégradée, - fonction intempestive	Causes de défaillance induites par : - l'environnement, les contraintes, - une défaillance du matériel ou un défaut caractéristique	Effets des défaillances sur : - l'environnement, - les fonctions du niveau supérieur, - la mission	Gravité des effets (par ex. classes de 0 à 4)	Probabilité d'occurrence des causes (par ex. classes de 0 à 3)	Moyen de détection des causes et/ou des effets	Disposition permettant la réduction : - de l'occurrence de la défaillance et/ou - la gravité des effets	

FIG. 3.1 — *Format fiche AMDEC*
(exemple tiré du guide pédagogique ISdF-Institut de Sûreté de Fonctionnement ; aujourd'hui IMdR-Institut de Maîtrise des Risques)

Cette fiche illustre très bien l'esprit d'une démarche fondée sur l'AMDEC, mais il existe une grande variété de tableaux. Il est hautement recommandé de choisir un tableau adapté à son cas et de ne pas prendre comme modèle le premier tableau venu, fût-ce celui-ci ou un tableau issu d'une norme.

3.2 Arbre de défaillance

L'arbre de défaillance est la méthode déductive type. Un arbre de défaillance se construit à partir d'un événement dit « événement-sommet » et représente sous forme arborescente les combinaisons d'événements (défaillances, erreurs) ou circonstances qui peuvent le causer. Il s'agit, en partant de l'événement-sommet, de répondre à la question « que faut-il pour qu'il se produise ? ». La réponse doit être constituée de plusieurs événements liés par « OU » ou « ET » (on parle de « portes OU » et de « portes ET »). En recommençant la même opération sur chacun des événements apportés par les réponses précédentes, l'arbre se constitue. Traditionnellement, l'événement-sommet est en haut et on descend en s'étalant.

En principe, un arbre de défaillance se construit avec les deux seuls opérateurs logiques « OU » et « ET », mais on peut gagner de la place en utilisant d'autres opérateurs logiques comme « OU exclusif », « NON » ou des fractions « p/n » comme 2/3, 3/4, 3/5, etc.

On peut exploiter un arbre de défaillances fondamentalement de deux façons. La première consiste à calculer les probabilités de tous les événements à partir de celles des événements de base, dits « feuilles ». Une fois que l'arbre de défaillances a été développé jusqu'à des événements élémentaires dont on connaît la probabilité, on remonte de proche en proche. Dans le cas d'une porte « ET », on attribue à l'événement supérieur le produit des probabilités des événements qui le composent ; dans le cas d'une porte « OU », la somme moins le produit. Ces calculs permettent non seulement d'évaluer la probabilité de l'événement-sommet, mais aussi le poids de chaque scénario dans cette probabilité globale. Ces calculs sont très simples quand les événements sont indépendants ; ils deviennent plus compliqués et vite inextricables quand les événements ne sont pas indépendants et qu'il faut évaluer les probabilités conditionnelles (c'est-à-dire la probabilité que l'un se produise sachant que l'autre est vrai).

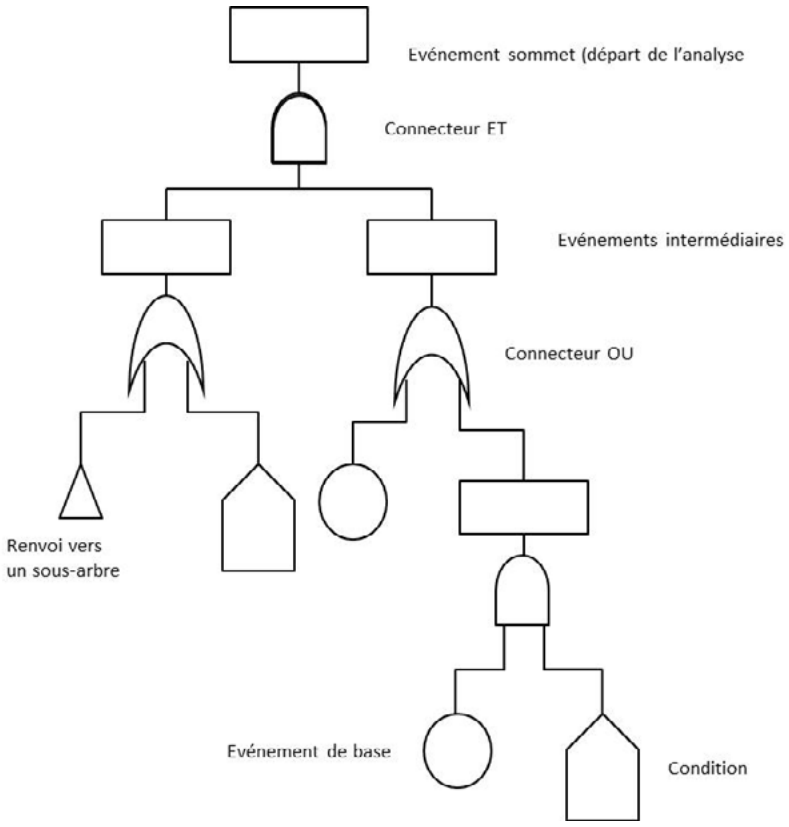

FIG. 3.2 — *Schéma d'arbre de défaillance avec les symboles usuels*

L'autre approche consiste à faire la liste de ce qu'on appelle les coupes, et à s'intéresser surtout aux coupes minimales.

Coupe et coupe minimale

Définition

Dans un arbre de défaillance, une coupe est un ensemble d'événements intermédiaires ou élémentaires suffisant pour provoquer l'événement-sommet. Une coupe minimale est une coupe qui n'en serait plus une si on lui retirait un élément quel qu'il soit. Autrement dit, les coupes minimales sont les conditions nécessaires et suffisantes pour que l'événement-sommet se produise.

On peut aussi se servir des coupes pour combiner les probabilités d'événements élémentaires afin d'évaluer la probabilité de l'événement-sommet et des intermédiaires. Cependant, les coupes permettent de rendre évidentes d'autres informations : le nombre minimal d'événements dans les coupes minimales est le nombre minimal d'événements simultanés nécessaires à la survenue de l'événement-sommet (le nombre d'événements formant une coupe minimale correspond au nombre de barrières évoqué au § 2.7 des « Notions de base »).

3.3 Arbre d'événement

L'arbre d'événement est une méthode très simple, mais beaucoup moins utilisée. Il s'agit de représenter sous forme d'arborescence la suite d'alternatives qui déterminent les conséquences d'un événement initial. Traditionnellement, l'événement initial est à gauche, puis on rencontre une première alternative, comme « le détecteur détecte OUI/NON ». Sur chaque branche de l'alternative, on va rencontrer l'alternative suivante, qui n'est donc généralement pas la même. Il est courant qu'une branche ne rencontre plus d'alternative alors que parallèlement l'autre branche en rencontre plusieurs successives. Les terminaisons des différentes branches constituent donc les conséquences ultimes, au niveau d'analyse choisi. En plaçant à chaque alternative la probabilité de chaque branche, on peut calculer la probabilité de chaque terminaison.

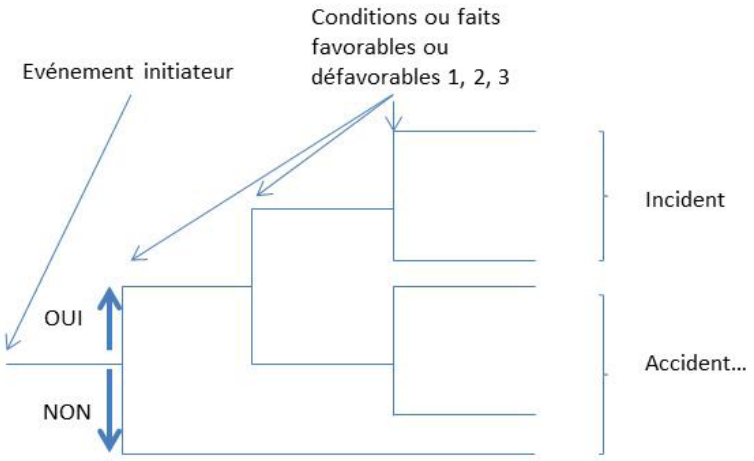

FIG. 3.3 — *Principe de l'arbre d'événement*

3.4 Arbre des causes

L'arbre des causes est une approche très répandue, très utilisée. Il se différencie fortement des méthodes précédentes en ce qu'il s'applique à l'analyse *a posteriori* d'un événement, souvent un accident, et non à l'analyse a priori de différentes possibilités. Il part de l'événement étudié, traditionnellement à droite de la feuille et il se développe vers la gauche. Il représente les faits, les liens logiques et chronologiques qui ont causé l'événement. Il se construit en répondant itérativement aux questions : « qu'a-t-il fallu pour que le fait apparaisse ? » et « était-ce suffisant pour que le fait apparaisse ? »

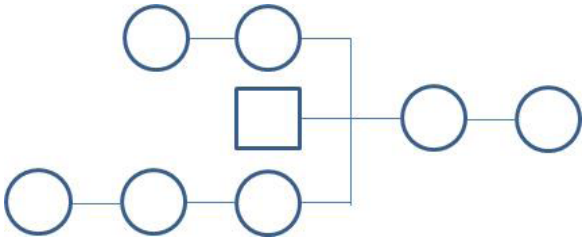

FIG. 3.4 — *Allure schématique d'un arbre des causes*

L'événement étudié, le « fait ultime » est tout à droite ; les cercles représentent les faits anormaux ou inhabituels et les rectangles les faits normaux. Étant très usitée, cette représentation connaît d'innombrables variantes.

3.5 Nœud-papillon

La représentation en nœud-papillon est très utilisée, en particulier dans les industries de procédé.

Comme son nom le suggère, le nœud-papillon est une représentation sous formes arborescentes, dont le centre est occupé par un événement dont les causes sont développées à gauche et les conséquences à droite. Cette généralité un peu vague recouvre des interprétations assez divergentes.

En matière d'analyse de risques, a priori **le nœud-papillon est la représentation sur un même document d'un arbre de défaillance et d'un arbre d'événement construit sur le même événement**. Cette représentation a le mérite de contenir beaucoup d'informations sous une forme très synthétique, et de permettre à la fois une vue d'ensemble ou de focaliser sur telle ou telle branche, ainsi que de conduire des calculs de probabilités ou de dégager l'architecture. Sur les branches de cette représentation, on peut placer des barrières : sur la partie gauche, des barrières de prévention qui peuvent prévenir la survenue de l'événement central, et sur la partie droite des barrières de protection (parfois de mitigation par anglicisme) qui peuvent en limiter les conséquences.

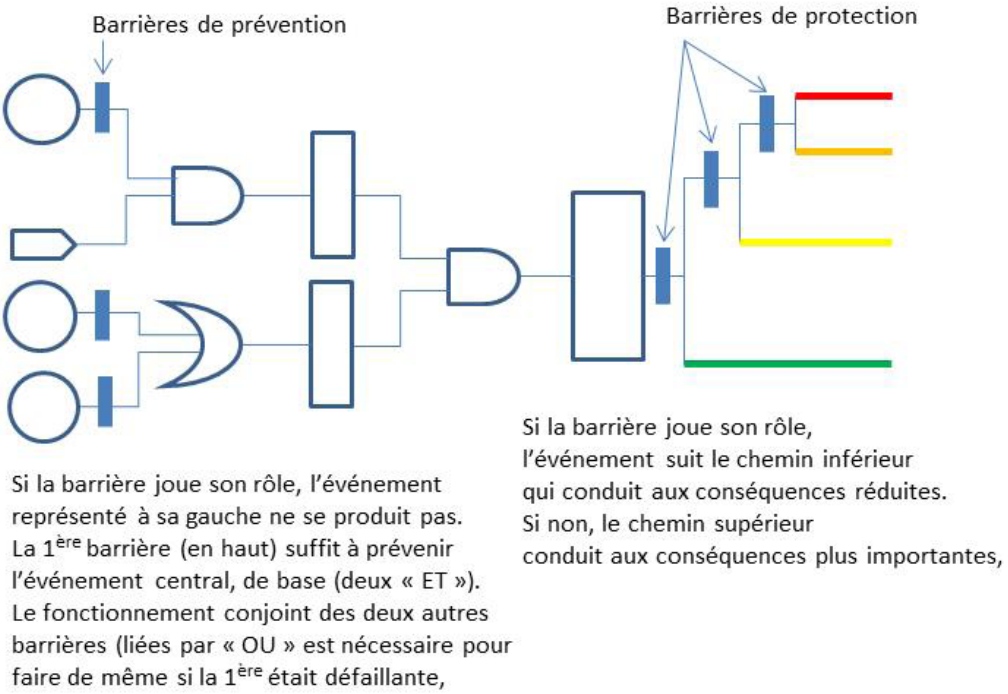

FIG. 3.5 — *Schéma de principe d'un nœud-papillon*

Mais le revers de la médaille est que cette représentation piège facilement les utilisateurs et que nombre de nœuds-papillons sont biaisés.

En effet, il est fréquent que les deux arbres ne décrivent pas vraiment le même événement. Même si l'intitulé de l'événement central est bien respecté, on constate souvent des sous-entendus différents dans les deux arbres quant au périmètre de ce qui est analysé. L'autre piège tient au fait qu'il est courant que l'arbre d'événement ne soit pas indépendant de l'arbre des défaillances. Selon le scénario qui a conduit à l'événement central, les possibilités de conséquences sont différentes et les probabilités de succès ou d'échecs aux différentes alternatives sont aussi différentes.

Il est aussi assez courant de parler d'un nœud-papillon à propos d'un arbre de causes sur un accident complété par un inventaire des conséquences de l'accident.

Enfin, la représentation en nœud-papillon et le même terme « nœud-papillon » ou « méthode du nœud-papillon » se retrouvent souvent dans une construction mixte : côté gauche, on développe un arbre de défaillances ; et côté droit, une représentation arborescente des conséquences possibles qui ne repose pas sur les scénarios possibles et sur une logique, mais sur la revue des différentes catégories de conséquences (humaines, matérielles, pertes de production, dégradation d'image, etc. ou au personnel, aux riverains, aux clients, aux biens de l'entreprise, à l'environnement, etc.).

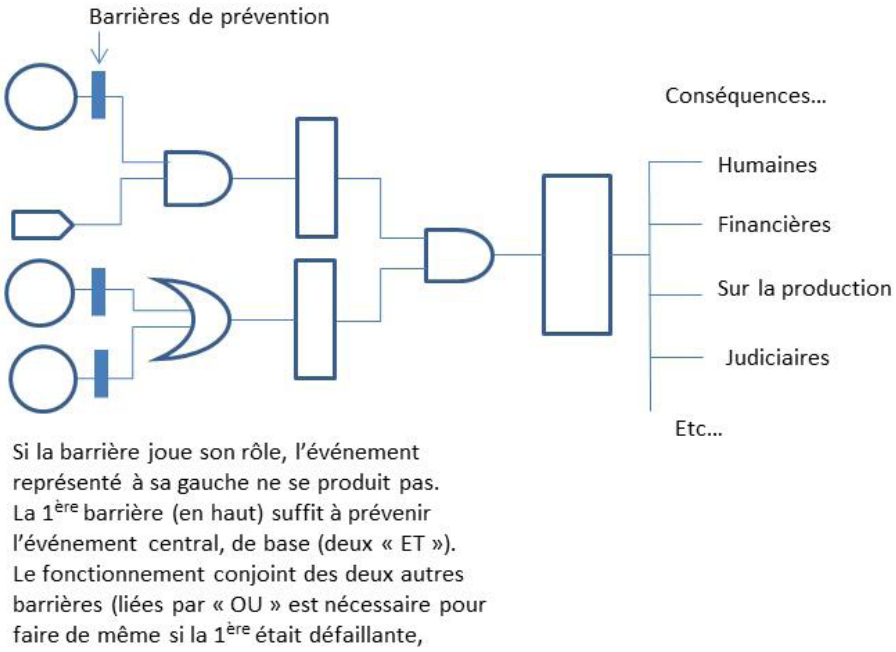

FIG. 3.6 — *Version en forme de nœud-papillon, mais ne comprenant qu'un arbre de défaillances et une représentation arborescente des conséquences possibles*

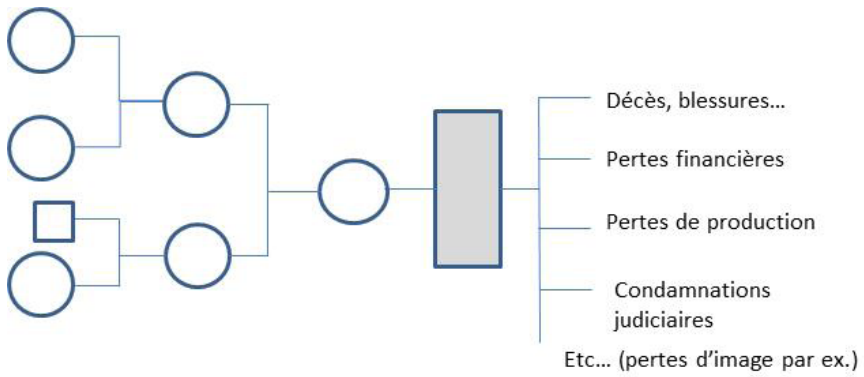

FIG. 3.7 — *Version en forme de nœud-papillon, mais ne comprenant qu'un arbre de causes et une représentation arborescente des conséquences de l'accident*

3.6 Graphes de Markov

Ces méthodes très puissantes sont particulièrement appropriées à la représentation des phénomènes stochastiques[1]. Elles fournissent une représentation graphique et reposent sur un modèle mathématique sous-jacent qui, au-delà des cas pédagogiques très simples, nécessitent très vite des moyens informatiques considérables et des compétences assez pointues.

Un graphe de Markov est constitué d'états et de transitions. Par exemple, un système constitué de deux composants A et B a quatre états :

- [A et B fonctionnent],
- [A fonctionne, B en panne],
- [A en panne, B fonctionne]
- et [A et B en panne].

La transition « A tombe en panne » conduit du 1er au 3e et du 2e au 4e. Si ces composants sont réparables, la transition « B est réparé » conduit du 2e au 1er et du 4e au 3e. La connaissance des taux de transition (probabilités de panne et de réparations) permet de calculer fiabilité et disponibilité.

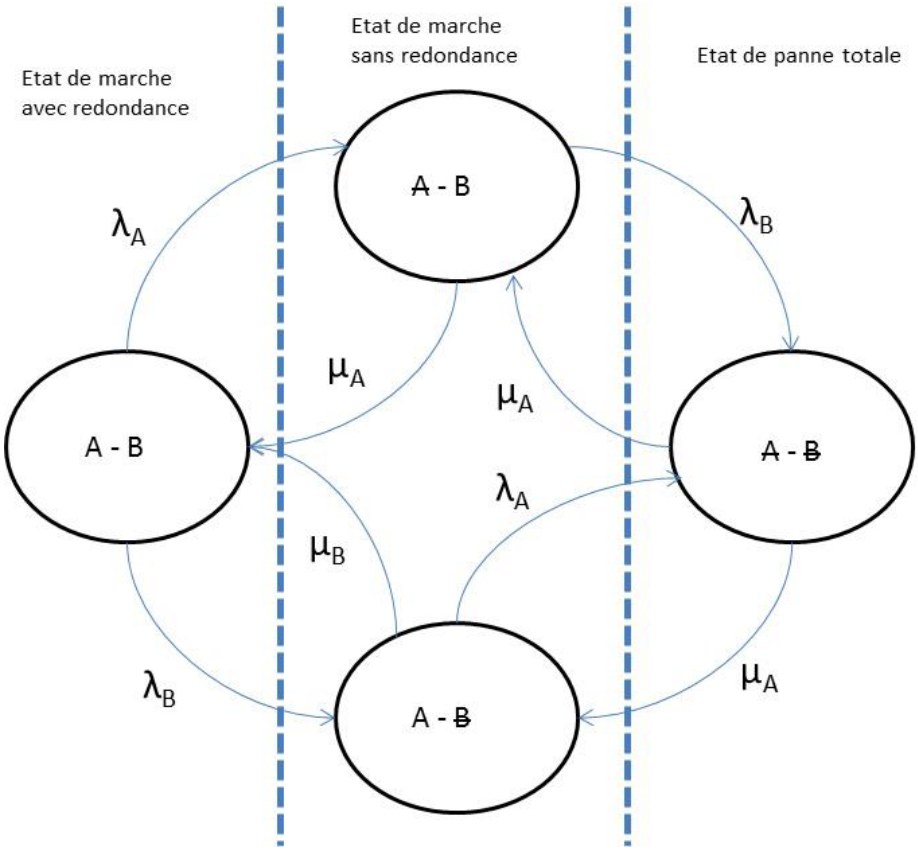

FIG. 3.6 — *Graphe de Markov basique*
2 équipements en parallèle peuvent assurer la fonction
(inspiré de *Le risque technologique* de A. Leroy et J-P Signoret PUF Collection « *Que sais-je ?* »)

1. Il s'agit des phénomènes dont nous représentons la survenue par l'objet mathématique « probabilité ».

3.7 Analyse préliminaire des risques

L'analyse préliminaire de risques (APR)[2] est une démarche essentielle en matière de sécurité. Contrairement à d'autres méthodes évoquées ici, elle est particulièrement dédiée aux approches de la sécurité.

Le terme recouvre un ensemble un peu nébuleux qu'on peut toutefois caractériser en se plaçant à deux niveaux :

- d'une part, à un niveau presque philosophique, une démarche qui se caractérise par ses objectifs et peut mettre en œuvre des moyens assez divers ;
- d'autre part, une méthode qui concourt spécifiquement à la démarche.

L'APR est d'abord une démarche visant à identifier les risques qu'il faudra traiter avec des ordres de grandeur de leurs importances et un principe des mesures qui devraient permettre de les maîtriser à un niveau acceptable. À vouloir décrire de façon précise et rigoureuse cette approche, on est vite conduit à spécifier une démarche exhaustive d'identification, d'évaluation, de réduction et de maîtrise des risques. La frontière entre analyse préliminaire et analyse est forcément floue. Cependant, dans un projet, il est intéressant de construire une démarche qui donne confiance dans ses conclusions et que l'on peut partager : les sujets risques importants sont repérés, les pistes de traitement sont assez crédibles pour éviter de graves remises en cause du projet et pouvoir anticiper les tâches et le planning relatifs à la maîtrise des risques, sans pour autant mener une analyse exhaustive et détaillée à chaque étape. Toutes les méthodes évoquées plus haut et d'autres peuvent être mises à contribution pour réaliser une analyse préliminaire des risques.

L'APR va chercher à repérer tous les risques qui devront être traités au cours du développement du projet, que ce soit la conception d'un nouveau système ou l'évolution d'un existant. Elle exploitera les analyses fonctionnelles/dysfonctionnelles qui recensent les attentes et les écarts possibles aux attentes[3]. Elle devra aussi anticiper les risques liés aux éléments (technologies, tâches confiées aux humains, impacts de l'environnement sur celles-ci). Un moteur électrique, par exemple, présente d'autres risques qu'un moteur thermique, à fonctions égales.

Une méthode spécifique à cet aspect de l'analyse préliminaire est très pratiquée pour identifier au mieux ces risques qui ne découlent pas nécessairement de l'expression fonctionnelle de besoins, mais des solutions qui vont être mises en œuvre pour les satisfaire. Cette méthode est souvent également appelée APR, d'où des possibilités de confusion. Elle consiste à balayer des documents qui recensent pour chaque technologie, produit… les risques associés compte tenu des connaissances et de l'expérience disponibles. Cette démarche s'impose en particulier en présence de produits chimiques pour lesquels des documents précis, généralement normés, informent explicitement sur les dangers qu'ils peuvent présenter (seuls ou en présence d'autres produits ou bien dans d'autres conditions : température, pression, etc.). Elle fournit généralement ses conclusions sous forme de tableaux associant à chaque produit ou composant, aux conditions qui influent sur sa dangerosité, la nature des phénomènes dangereux et les précautions efficaces connues. L'expression « analyse préliminaire de risques » s'applique selon les locuteurs à cette méthode ou à la démarche plus générale à laquelle elle peut contribuer au côté d'autres méthodes.

3.8 Le retour d'expérience, la « fiabilité logicielle », les FOH

Pour en terminer avec ce *Regard* du « fiabiliste », mentionnons trois domaines qui concernent directement le fiabiliste, mais dont chacun fait l'objet d'une abondante littérature.

3.8.1 Le retour d'expérience

Le fiabiliste travaille très souvent sur des systèmes complexes et toujours sur des systèmes sur lesquels le savoir est lacunaire. Aussi, l'exploitation des connaissances issues de l'expérience est-elle centrale dans l'activité de maîtrise des risques.

2. Certains parlent plus volontiers d'analyse préliminaire des dangers (APD) avec des petites différences d'approche.
3. Une « AMDE fonctionnelle » sera souvent une méthode adaptée.

Sans prétendre couvrir le vaste champ du retour d'expérience, citons :

- L'enregistrement systématique des défaillances de composants pour valider les lois de probabilités de défaillance[4], pour identifier les conditions qui influent et calculer les paramètres des lois. Des essais peuvent être organisés pour recueillir ces données sans attendre des années d'exploitation. Des méthodes existent pour simuler des années d'expérience en quelques semaines.
- Le recensement des événements pour constituer des indicateurs statistiques.
- La description et les analyses des événements complexes pour affiner, compléter ou corriger la compréhension des phénomènes à l'œuvre.

3.8.2 La sûreté de fonctionnement logicielle

Comme déjà évoqué, le fiabiliste ne peut créer à partir de rien, il exploite des informations. Les connaissances sur les comportements possibles des éléments qui composent un système sont fondamentales. Deux domaines posent des problèmes particulièrement ardus, d'autant que la représentation des connaissances par des probabilités est largement impropre : la sûreté de fonctionnement logicielle et les facteurs humains, organisationnels (FHO) et sociaux. Penchons-nous tout d'abord sur le premier.

Malgré l'impression que peut avoir un utilisateur, un ensemble logiciel sur un support matériel donné a un comportement absolument déterministe.

Toutefois, le nombre de paramètres à prendre en compte, le nombre d'états qu'ils peuvent prendre et la complexité des systèmes programmés actuels sont tels que la prédiction déterministe est hors de portée. Aussi, de nombreuses approches et des méthodes spécifiques ont été développées[5] pour la maîtrise des risques des systèmes programmés. Il faut ensuite intégrer ce que ces nouvelles approches produisent avec celles adaptées aux autres éléments d'un système pour maîtriser l'ensemble, et c'est un artisanat complexe.

En général, on se concentre sur des règles de codage, de spécification, d'organisation… afin de limiter ce problème, sans toutefois le supprimer complètement. Sans doute, la seule solution est-elle le découpage en sous-fonctions/programmes plus simples et donc maîtrisables, mais alors se pose le problème des interfaces entre ceux-ci, trop souvent oubliées…

3.8.3 Les facteurs humains, organisationnels et sociaux

Le domaine de l'humain, où les sciences humaines et sociales apportent énormément de connaissances, ne se traduit pas non plus par une loi de probabilité.

L'expression même de « facteur humain », qui ne serait sans doute pas choisie s'il fallait aujourd'hui baptiser ce domaine de connaissances mais qui est assez établie pour se maintenir, en dit long sur le point de vue initial du fiabiliste sur le « composant » humain. Alors que la technologie fournirait un certain niveau de performance, il faut le pondérer — sous-entendu le réduire — d'un certain facteur à évaluer, à cause des erreurs humaines. « *L'homme est un facteur de fiabilité faillible* » (Mazeau, 1993) est une expression sans doute plus proche des approches actuelles. Toutefois la conviction, assez profondément ancrée pour ne pas être interrogée que toute réduction du rôle de l'humain au profit d'une machine, toute automatisation, toute limitation de l'action humaine par une machine réduit les risques, rassure encore et dicte bien des décisions.

La différence la plus fondamentale entre le domaine de l'humain et tous les domaines techniques est qu'ici on ne spécifie pas, on ne construit pas le « composant ». On bénéficie d'un « composant » extraordinaire, l'être humain, aux facultés presque infiniment riches et on souffre d'être dépassé par cette immense richesse.

Les connaissances apportées par les sciences humaines et sociales sont très vastes, mais ne permettent pas, de loin, de maîtriser ce qui tient à l'humain dans nos systèmes. La démarche du fiabiliste consiste à exploiter au mieux ces connaissances, comme pour les technologies. La sûreté de fonctionnement

4. Trouver et valider les régularités statistiques mentionnées au début de ce *Regard*.
5. Et le sont toujours, car nous ne sommes pas au bout de nos peines.

ayant connu un développement remarquable par l'exploitation des régularités statistiques dans les défaillances, le fiabiliste est particulièrement friand de contributions des spécialistes de l'homme au travail sous forme de probabilité (de fréquence ou de taux) d'erreurs humaines. Certes, mais les cas où des régularités statistiques de ce type sont avérées sont plutôt rares, et de plus relèvent surtout de tâches simples et répétitives qui de nos jours sont rarement confiées à des humains. Les connaissances issues des sciences humaines et sociales permettent plus souvent, plus directement, de construire, d'améliorer un système du point de vue des risques que de calculer ceux-ci. Et les choix, les actions portent non sur le « composant » humain mais surtout sur son environnement (outils, interfaces, documents, formations et l'ensemble très vaste et divers appelé « management »).

La difficulté majeure est donc d'intégrer des connaissances de nature et de forme très diverses pour approcher la sûreté de fonctionnement d'un système dans lequel interviennent des humains et des technologies variées.

Conclusion

J'aimerais conclure avec l'image du dolmen : la table est la sûreté de fonctionnement, avec un ensemble de notions, d'approches, de méthodes et d'outils et les spécialistes pour s'en servir. Elle offre une protection contre le ciel qui nous tomberait sur la tête, les catastrophes. Mais pour cela, elle doit être posée sur de solides piliers qui sont les sciences relatives aux composants de nos systèmes et de leurs environnements : mécanique et hydraulique, thermodynamique, électricité et électronique, psychologie, sociologie, anthropologie, etc.

Le fiabiliste est peut-être, comme je l'ai souvent entendu, quelqu'un de tordu puisqu'il ne s'intéresse qu'à ce qui ne marche pas et ne pense qu'à comment ça peut mal tourner. Mais le fiabiliste a aussi un regard de constructeur, un regard de conducteur qui veille à ce que ça se passe bien en vrai et mal sur le papier. Il se sait souvent perçu comme un enquiquineur et a besoin de la chaleur d'une équipe, même si, dans celle-ci, il est souvent la voix discordante qui répète « ça ne peut pas arriver, certes, mais si ça arrive quand même ? ».

Bibliographie

Techniques de l'ingénieur

CHARAVEL Bernard, *Système de management de la sécurité : mise en place sur site,* AG 4650

DALPONT Jean-Pierre, *Sécurité et gestion des risques*, SE 12

GAYON Alain, *Importance de la sécurité dans les entreprises,* AG 4600

IDDIR Olivier, *Le nœud-papillon : une méthode de quantification du risque majeur*, SE 4055

IDDIR Olivier, *Principes d'évaluation de la probabilité de défaillance des mesures de maîtrise des risques (MMR),* SE 4057

IDDIR Olivier, *Évaluation de la probabilité de défaillance d'un système instrumenté de sécurité (SIS)*, SE 4058

MORTUREUX Yves, *Analyse préliminaire de risques,* SE 4010

MORTUREUX Yves, *AMDE(C)*, SE 4040

MORTUREUX Yves, *Arbres de défaillance, des causes et d'événement*, SE 4050

MORTUREUX Yves, *La sûreté de fonctionnement : méthodes pour maîtriser les risques,* AG 4670

MORTUREUX Yves, *La sûreté de fonctionnement : démarches pour maîtriser les risques,* SE 1020

SIGNORET Jean-Pierre, *Analyse des risques des systèmes dynamiques : préliminaires*, SE 4070

SIGNORET Jean-Pierre, *Analyse des risques des systèmes dynamiques : approche markovienne,* SE 4071

SIGNORET Jean-Pierre, *Analyse des risques des systèmes dynamiques : réseaux de Petri. Principes,* SE 4072

SIGNORET Jean-Pierre, *Analyse des risques des systèmes dynamiques : réseaux de Petri. Exemples de modélisation*, SE 4073

VEROT Yvan, *Démarche générale de maîtrise du risque dans les industries de procédé,* AG4605.

Publications IMdR (Institut de Maîtrise des Risques)

Fiches méthodes du groupe de travail « Management, Méthodes, Outils, Standards » M2OS accessibles à l'adresse : http://www.imdr.eu/upload/client/document_site/Fiches_pedago_8_20140615_FR.pdf (version anglaise également disponible sur le site ; mises à jour au fur et à mesure des travaux du groupe).

« Guide de sélection des modèles de fiabilité prévisionnelle pour les composants électroniques » d'octobre 2009 accessible à l'adresse http://www.imdr.eu/upload/client/document_site/Projets/Guide_de_selection_oct09_159.pdf

Condensé pédagogique n°2 : « La sûreté de fonctionnement »

Condensé pédagogique n°3 : « Fiabilité prévisionnelle, principes de base »

Condensé pédagogique n°6 : « Conception de base de données de sûreté de fonctionnement »

Livres

DESROCHES Alain, LEROY Alain et VALLEE Frédérique, *La gestion des risques*, Hermès-Lavoisier, février 2003

DESROCHES Alain, *Concepts & méthodes probabilistes de base de la sécurité*, Lavoisier, mai 1995

LEROY Alain et SIGNORET Jean-Pierre, *Le risque technologique* PUF, Que sais-je ? n°2669, octobre 1992

MAZEAU Michel, « L'homme agent de fiabilité faillible », *Performances Humaines et Techniques*, 66, 24-29, septembre-octobre 1993

SUTTON Ian S. , *Process Reliability and Risk Management*, Van Nostrand Reinhold, 1992

VILLEMEUR Alain, *Sûreté de fonctionnement des systèmes industriels*, Eyrolles, 1988

Reproduction de ce document

FONCSI
Fondation pour une culture de sécurité industrielle

Fondation pour une culture de sécurité industrielle
Fondation de recherche reconnue d'utilité publique

http://www.foncsi.org/

6 allée Emile Monso – BP 34038
31029 Toulouse Cedex 4
France

Téléphone : +33 (0) 534 32 32 00
Twitter : @LaFonCSI
Courriel : contact@foncsi.org

ISSN 2100-3874

FONCSI

Fondation pour une culture
de sécurité industrielle

6 allée Émile Monso
ZAC du Palays - BP 34038
31029 Toulouse cedex 4 - France

www.foncsi.org