Contribution à la formalisation unifiée des connaissances fonctionnelles et organisationnelles d'un système industriel en vue d'une évaluation quantitative des risques et de l'impact des barrières envisagées

Aurélie Léger

UFR Sciences et Techniques Mathématiques, Informatique et Automatique
Ecole Doctorale IAEM Lorraine
Département de Formation Doctorale en Automatique

Thèse

présentée pour l'obtention du grade de

Docteur de l'Université Henri Poincaré - Nancy 1

Spécialité Automatique, Traitement du Signal et Génie informatique

par

Aurélie Léger

Contribution à la formalisation unifiée des connaissances fonctionnelles et organisationnelles d'un système industriel en vue d'une évaluation quantitative des risques et de l'impact des barrières envisagées

Soutenue publiquement le 28 mai 2009 à la Faculté des Sciences et Techniques devant la commission d'examen composée de :

Président du Jury et Rapporteur	Daniel NOYES	Professeur à l'École Nationale d'Ingénieurs de Tarbes
Rapporteur	Patrick MILLOT	Professeur à l'Université de Valenciennes
Examinateurs	Carole DUVAL	Chargée de Mission - EDF Recherche et Développement
		Ingénieur de l'ENSEM - INPL - Nancy
	Régis FARRET	Délégué Scientifique Adjoint - INERIS
		Direction des Risques Accidentels
	Benoît IUNG	Professeur à l'Université Henri Poincaré - Nancy 1
		Directeur de thèse
	Éric LEVRAT	Maître de Conférences à l'Université Henri Poincaré - Nancy 1
	Philippe WEBER	Maître de Conférences à l'Université Henri Poincaré - Nancy 1
	Enrico ZIO	Professeur à l'Université Polytechnique de Milan

Centre de Recherche en Automatique de Nancy - CNRS UMR 7039
Faculté des Sciences et Techniques - BP239 - 54506 Vandoeuvre-lès-Nancy

Puisqu'on ne peut être universel en sachant tout ce qui peut se savoir sur tout, il faut savoir (un) peu de tout. Car il est plus beau de savoir quelque chose de tout que de tout savoir d'une chose. Cette universalité est la plus belle. Si on pouvait avoir les deux, encore mieux, mais s'il faut choisir, il faut choisir celle-la, et le monde le sent et le fait, car le monde est un bon juge souvent.

Blaise Pascal, **Pensées** , 1670

« Commence par finir ce que tu commences. »

Proverbe japonais

Remerciements

Les lignes qui suivent sont les dernières que j'apporte à ce manuscrit mais les premières que va découvrir le lecteur. J'espère qu'elles l'aideront à s'imprégner du contexte dans lequel ces travaux de recherche se sont déroulés.

En premier lieu, je tiens à souligner qu'une thèse est une aventure humaine collective, quelquefois douloureuse, mais qui au final est forte d'enseignements. Aussi, je souhaite remercier toutes les personnes qui, de près ou de loin, ont contribuées à faire aboutir ces travaux et dont j'aurais omis de mentionner le nom dans ces pages.

Je remercie sincèrement mon directeur de thèse, monsieur Benoît Iung, pour ses conseils avisés et son soutien. Son encadrement m'a permis de prendre confiance en moi et d'assumer mes choix, et m'a également aidée dans mon apprentissage du métier de chercheur.
Je souhaite également remercier monsieur Eric Levrat, qui a été un très bon professeur de logique en premier cycle, qui a ensuite encadré mon stage de DEA et m'a encouragée à poursuivre en thèse en me co-encadrant.
Un merci particulier à monsieur Philippe Weber, pour son encadrement, pour les nombreux échanges que nous avons eu autour des réseaux bayésiens, et pour sa disponibilité et son aide dans mes moments de doute.
Un grand merci à madame Carole Duval pour son encadrement quotidien et sa capacité d'écoute durant ces années. Son implication, son soutien et la confiance qu'elle a su me donner m'ont souvent permis de faire avancer mes recherches.
Je tiens également à remercier monsieur Régis Farret pour les discussions que nous avons eu autour de la problématique du risque, et pour m'avoir permis, par son encadrement, de confronter mes travaux à un cas industriel réel.

Je remercie monsieur Daniel Noyes pour avoir accepté de présider mon jury de thèse, et pour ses remarques constructives en tant que rapporteur de ce manuscrit.
Je tiens à remercier monsieur Patrick Millot pour avoir accepté de rapporter mes travaux de recherche et pour ses remarques portant sur l'étude du facteur humain.
Merci également à monsieur Enrico Zio pour avoir accepté d'examiner mon travail et pour sa présence lors de ma soutenance.

Je remercie tous les doctorants, ATER, post-doctorants, maîtres de conférences et professeurs du CRAN avec qui j'ai pu converser au cours de ces années. Je remercie plus particulièrement Pierre, Maxime, Gabriela, Jean-Philippe, Esma, Nicolas, Edouard, David, Idriss, Maha, Cristian, Leila, Dragos, Simona, Pascale, Alexis, William, Carlos, Gilbert, Andres ... pour nos échanges animés (concernant, entre autres, les couleurs à adopter pour la BSR [1]) et pour leur soutien dans mes moments difficiles.

1. BSR : Brain Storming Room

Je tiens à remercier l'ensemble des agents (statutaires ou non) du département MRI [2] d'EDF R&D pour les nombreuses discussions que nous avons pu avoir et qui m'ont permis de découvrir la diversité des disciplines nécessaires à la maîtrise des risques industriels.
Je tiens à remercier plus particulièrement monsieur Yves Dien pour son aide concernant la compréhension des spécificités des analyses organisationnelles, et pour son expertise dans ce domaine.

Merci à l'ensemble des agents du département EVAL [3] de la DRA [4] de l'INERIS pour les échanges que nous avons eu autour des analyses de risques.
Je remercie plus particulièrement madame Cécile Deust pour son aide concernant la modélisation des aspects techniques du cas d'application, et monsieur Jean-Christophe Le Coze pour son expertise concernant les aspects organisationnels de ce même cas.

Je n'en serais pas là sans le soutien de ma famille et de mes amis. Aussi, je souhaite remercier :
- Mes parents pour m'avoir accompagnée dans chacun de mes choix.
- Marithé pour avoir nourri ma curiosité durant mon enfance.
- Josette pour ses petits plats (qui sont souvent le remède à bien des maux ...).
- Amandine, Yann et Ambre pour avoir toujours été là quand j'avais besoin de vous.
- Françoise et Christian pour m'avoir supportée pendant mes nuits de rédaction.
- Mes oncles, tantes et cousins pour l'intérêt qu'ils ont porté à mes travaux.
- Mélina, Philippe, Julie, Sylvain, Julien, Ewen, Stéphanie, Gérald et Stéphane pour nos joyeuses soirées vandopériennes et strasbourgeoises.

Mon dernier remerciement, et sans doute le plus important, est pour Sébastien. Je te remercie d'avoir cru en moi il y a quelques années et de m'avoir aidée à me dépasser. Mes travaux n'auraient pu aboutir sans ton soutien indéfectible. Merci d'être à mes côtés à chaque instant.

2. MRI : Management des Risques Industriels
3. EVAL : Evaluation des risques
4. DRA : Direction des Risques Accidentels

Table des matières

Introduction générale

Depuis la révolution industrielle, l'Homme développe et utilise des systèmes industriels pour satisfaire ses exigences de production (de biens et de services). Mais l'exploitation de tels systèmes n'est pas sans risques pour leurs utilisateurs directs et leur environnement (humain, naturel, installations voisines ...).
Nous pouvons par ailleurs observer que l'étude, ou l'analyse, des risques s'est considérablement développée durant ces dernières décennies, du fait d'une part de la complexification des systèmes de production (comme les avancées technologiques, le développement des industries lourdes [5]), et d'autre part du développement de la réglementation, telle que la loi ICPE [6] élaborée suite à la catastrophe de Seveso en 1976.

En effet, si jusque dans les années 1970, les études étaient focalisées sur les défaillances technologiques des systèmes (réalisées par le biais d'études de fiabilité, d'AMDEC [7] ...), un certain nombre d'accidents majeurs (tel que l'accident nucléaire de Three Miles Island en 1979) ont mis en évidence l'importance du facteur humain dans l'occurrence de ces accidents. Ainsi, dans les années 1980, de nombreuses méthodes consacrées à une meilleure prise en compte de ce type de facteurs ont émergées. De plus, l'occurrence d'autres accidents (tels que la catastrophe de Bhopal en 1984, et l'accident nucléaire de Tchernobyl en 1986) ont permis d'identifier des causes sous-jacentes à ces défaillances techniques et humaines : les dysfonctionnements organisationnels.

L'intégration de différentes ressources technique, humaine et organisationnelle, dans les analyses de risques semble aujourd'hui incontournable pour les installations classées, pour lesquelles un haut niveau de maîtrise des risques doit être démontré aux autorités de contrôle (comme les DRIRE [8], ou l'Autorité de Sûreté pour les installations nucléaires). Ces études, impliquant des disciplines différentes (comme la sociologie, l'ergonomie, la fiabilité humaine, la sûreté technique), étaient jusqu'alors conçues et conduites indépendamment les unes des autres. Cet état de fait amène à une sectorisation des analyses et ne permet pas d'avoir une vision globale de la situation étudiée. Ce n'est que récemment qu'ont émergé des méthodologies proposant une intégration de ces différentes dimensions dans la démarche d'analyse de risques. Certains de ces développements se basent sur l'analyse de cas avérés [Paté-Cornell et Murphy, 1996], d'autres sur une utilisation qualitative de modèles graphiques [Svedung et Rasmussen, 2002], et d'autres encore sont réalisés pour

5. Secteurs liés à la production ou la transformation de matières premières comme les mines, la métallurgie, la papeterie, la construction navale et la production électrique.
6. ICPE : Installations Classées pour la Protection de l'Environnement
7. AMDEC : Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité
8. DRIRE : Directions Régionales de l'Industrie, de la Recherche et de l'Environnement

des installations particulières (la SNCF [9] par [Delmotte, 2003], des process chimiques par [Papazoglou *et al.*, 2003], les installations nucléaires par [Galàn *et al.*, 2007] ...).
Cependant ces travaux sont pour la plupart partiels car ils ne considèrent que certaines ressources du système et/ou certaines particularités de la démarche d'analyse de risques, et sont principalement spécifiques à un domaine d'activité. Cette situation s'explique du fait :
- de la nouveauté de certaines approches pour les industriels (les analyses organisationnelles ne sont pas pratiquées aussi couramment que peuvent l'être les analyses ergonomiques du poste de travail ou les analyses d'activités),
- de ce qu'elles remettent en cause (l'observation de dysfonctionnements organisationnels est difficile à faire accepter par les équipes de direction car elles se retrouvent alors directement impliquées),
- de la différence des paradigmes (micro, méso et macro) nécessaires à l'étude de ces dimensions du système.

De ces différents points émergent un ensemble de verrous qui freinent encore actuellement le développement des analyses intégrées des risques, comme : la modélisation de systèmes complexes (systèmes de grande taille qui intégrent des dimensions appartenant à des sphères différentes), la caractérisation (qualification et/ou quantification) des aspects humains et organisationnels d'un système dans un objectif de hiérarchisation des risques (et non pas pour une analyse d'accident avéré), l'unification de ces connaissances pour leur intégration dans une démarche d'analyse de risque, et l'acceptation (par les équipes de direction) de l'influence de ces causes sous-jacentes dans l'occurrence de situations à risques.

Cette nécessité de faire évoluer les approches sectorielles d'analyse de risques vers des méthodologies intégrées et orientées système, constitue aujourd'hui une problématique, à la fois scientifique et industrielle, pour les exploitants de systèmes de production critiques (que sont les installations classées : centrales nucléaires, process chimiques ...). Ce constat, ayant initié des travaux préalables entre le département *Management des Risques Industriels* d'*Électricité De France - Recherche & Développement* (EDF R&D), et le département *Évaluation des risques* de l'*Institut National de l'Environnement Industriel et des Risques (INERIS)*, fonde le contexte initial de ces travaux de thèse, qui résultent d'une collaboration entre ces deux précédentes entités et le groupe thématique *Systèmes de Production Ambiants* (et plus particulièrement le groupe de travail *Systèmes Interopérants*) du *Centre de Recherche en Automatique de Nancy* (CRAN). Ils font suite à différents travaux réalisés dans plusieurs projets (ARAMIS [10], ATHOS [11], GLORIA [12] ...) et ont pour objet initial une rationalisation scientifique et une extension des résultats existants portant principalement sur l'évaluation des risques relatifs à l'exploitation d'un système industriel.

En ce sens, les développements proposés dans ces travaux de thèse se basent sur les connaissances d'experts issus de différentes disciplines. Les domaines d'activités impliqués dans ces travaux sont : les analyses de risques (EDF, INERIS), les études de systèmes complexes (CRAN), les analyses organisationnelles (EDF, INERIS), la modélisation et

9. SNCF : Société Nationale des Chemins de Fer Français
10. ARAMIS : Accidental Risk Assessment Methodology for Industries in the framework of SEVESO II directive (www.aramis.jrc.it)
11. ATHOS : Analyse Technique, Humaine et Organisationnelle de Sécurité (INERIS)
12. GLORIA : Global Risk Assessment (EDF)

la quantification de systèmes complexes (CRAN). Ce partenariat implique également un industriel pour la partie applicative de nos travaux.
Ces travaux sont, de plus, en lien avec des communautés nationales (comme l'*AFIS*[13] et le *GT S3* du *GdR MACS*), européennes (comme l'*ETPIS*[14], et sa déclinaison française la *FTPIS*[15]) et internationales (comme la SRA[16]).

Partant de ce besoin (à la fois scientifique et industriel), les développements proposés dans ces travaux de recherche ont été construits en suivant une approche abductive, comme le définit [Karim, 2008], *i.e.* en combinant des approches de recherche déductives[17] et des approches inductives[18] (cf. figure 1).

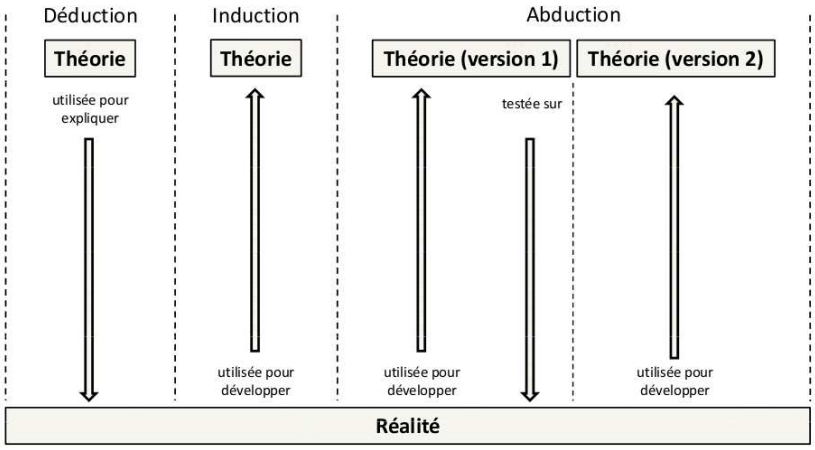

FIG. 1 – Relations entre Théorie et Réalité dans les différentes approches de recherche

Ainsi, en nous basant sur ces trois types d'approches de recherche, notre démarche de travail s'organise comme suit :

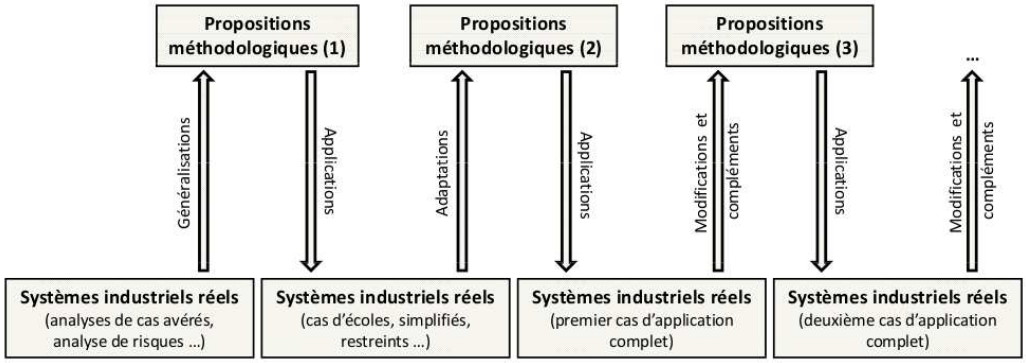

FIG. 2 – Démarche de travail support au développement de la méthodologie proposée

13. AFIS : Association Française d'Ingénierie Système
14. ETPIS : the European Technology Platform on Industrial Safety
15. FTPIS : the French Technology Platform on Industrial Safety
16. SRA : the Society for Risk Analysis
17. Une approche de recherche déductive se base sur le développement de méthodes et théories pour expliquer un cas particulier.
18. Une approche inductive part d'observations issues d'un grand nombre de cas particuliers pour en proposer une généralisation au travers de nouvelles méthodes et théories.

En ce sens, cette démarche se décompose en plusieurs phases successives (d'applications concrètes et de conceptualisations théoriques), que nous pouvons décrire par les points suivants :

- L'étude des caractéristiques d'événements avérés, et des spécificités des méthodes d'analyses mises en œuvre sur ces cas, permettent (par généralisation) de proposer les principes fondateurs de notre démarche méthodologique.
- Chacun de ces principes est ensuite appliqué à des cas simplifiés. Cette première mise en application permet de s'assurer de la cohérence des résultats obtenus face à des situations dont le comportement attendu est connu.
- L'observation de certaines limites, incohérences, et/ou manques, entraîne de nouveaux développements qui viennent compléter la démarche existante.
- Cette nouvelle version de la méthodologie est appliquée à un cas industriel réel et complet, afin d'en étudier la faisabilité et d'analyser la validité des méthodes et modèles proposés.
- Ces premiers résultats permettent d'identifier de nouvelles limites et de nouveaux manques, qui nécessiteront des travaux complémentaires, avant de pouvoir proposer une troisième version de la démarche.

À terme, l'intérêt d'une telle approche de travail est de pouvoir proposer une méthodologie d'analyse à la fois générique et opérationnelle, car elle est régulièrement confrontée à des situations industrielles réelles issues de divers domaines d'activités. Cette méthodologie, qui constitue notre contribution, a pour objet l'analyse de risques de systèmes socio-techniques [19] en exploitation. Ce type d'analyse multi-points de vues vise à probabiliser le risque étudié à des fins d'aide à la décision. C'est pourquoi, nous proposons une démarche de formalisation, d'intégration et de représentation des connaissances fonctionnelles, dysfonctionnelles, comportementales et organisationnelles du système, dans un même modèle de risque.
La démarche de modélisation s'appuie, quant à elle, sur le formalisme des réseaux bayésiens [Jensen, 2001] qui permet de combiner à la fois des données quantifiées et qualifiées dans un même modèle [20]. Il devient ainsi possible d'identifier, pour un scénario d'accident donné, l'ensemble des causes menant à son occurrence, et ce en considérant à la fois les données techniques du système (la probabilité de défaillance d'un composant, la probabilité d'occurrence d'un événement ...) mais également les données liées aux opérateurs (la probabilité de réussite d'une mission ...) et à l'organisation (présence ou absence de facteurs représentatifs d'un contexte organisationnel particulier).

L'originalité de notre approche réside principalement dans le fait d'intégrer dans un même modèle de risque, les aspects techniques, humains et organisationnels relatifs à un système industriel. Et plus spécifiquement, l'intérêt de notre contribution porte sur :

- L'appréhension du système industriel comme un tout (au sens systémique, à savoir comme « un ensemble d'éléments en interrelations entre eux et avec l'environnement » [21]). Cette spécificité nous permet de poser les principes fondateurs d'une approche structurée.

19. Systèmes intégrant les dimensions technique, humaine et organisationnelle et pouvant être influencés par des contraintes sociétales et/ou environnementales.

20. « Bayesian probability theory is the most mature methodology which employs qualitative and quantitative modelling constructs to represent a problem. » [Gregoriades et Sutcliffe, 2008]

21. « A system may be defined as a set of elements standing in interrelation among themselves and with environment. » [Von Bertalanffy, 1968]

– La proposition d'un ensemble de concepts, méthodes et modèles génériques [22] permettant d'une part, l'extraction des connaissances présentes dans les différentes dimensions du système, et d'autre part, l'unification de ces connaissances dans un même modèle.
– L'utilisation de l'outil de modélisation comme moyen de propagation des connaissances ; pour aboutir à une évaluation probabiliste du risque étudié et pour pouvoir analyser les impacts que peuvent avoir certains éléments critiques du système.

Cette contribution méthodologique se développe dans le mémoire de thèse en quatre chapitres :

Chapitre 1 - Dans ce premier chapitre, nous positionnons l'ensemble des développements existants dans le domaine des analyses de risques. Dans cette optique, nous proposons tout d'abord d'identifier et de définir le type de risque considéré (le risque incidentel/accidentel) puis de présenter la démarche d'analyse de risques à partir des définitions données dans les normes [ISO, 1999] et [ISO-CEI, 2002]. Nous pouvons alors aborder plus spécifiquement les caractéristiques [23] des analyses sectorielles (centrées sur la technique, l'opérateur humain ou l'organisation), puis celles portant sur des méthodologies traitant de la problématique des analyses intégrées. Ce dernier point nous permet d'identifier les finalités de ce type de démarche [24] afin d'en identifier les manques et de pouvoir positionner notre démarche méthodologique.

Chapitre 2 - Ce deuxième chapitre permet d'aborder les trois premières étapes de notre approche, à savoir : la définition des limites du système, l'extraction des connaissances et leur unification. Dans un premier temps, nous présentons pour chacune des dimensions du système étudié : les objectifs liés à l'étude et la représentation de la dimension considérée, et la méthode utilisée pour recueillir et représenter les connaissances spécifiques à ce niveau d'abstraction. Dans un second temps, nous formalisons les mécanismes de structuration et d'intégration de ces connaissances en présentant les concepts valables pour l'ensemble du système, puis les mécanismes d'intégration développés pour lier les dimensions technique et humaine d'une part, et les dimensions humaine et organisationnelle d'autre part.

Chapitre 3 - Ayant défini la manière de recueillir, représenter et lier ces dimensions, nous pouvons à présent décrire les étapes de construction et de représentation du modèle de risque. Ainsi, ce troisième chapitre développe un ensemble de méthodes permettant de traduire ces différentes connaissances dans un même modèle de risque, et ce en exploitant le formalisme des réseaux bayésiens. Dans un premier temps, nous justifions le choix des réseaux bayésiens comme outil support à la modélisation. Puis, nous proposons pour chacune des dimensions du système, un ensemble de modèles génériques et de méthodes permettant une estimation probabiliste de leurs variables caractéristiques.

Chapitre 4 - Dans le dernier chapitre de ce mémoire de thèse, nous proposons une application de cette méthodologie à un cas industriel réel (proposé par l'INERIS), et visant

22. En effet, les développements méthodologiques se veulent applicables aussi bien à une installation nucléaire qu'à un process chimique. Ceci nous amène à proposer des principes génériques, qui pourront alors être instanciés pour une situation particulière et dans un domaine d'activité particulier.
23. Positionnement chronologique, théories sous-jacentes, principales méthodes ...
24. Dimensions du système considérées, objectifs recherchés, domaines d'applications, outils utilisés ...

à aider un exploitant particulier à identifier les faiblesses de son système de stockage de produit fini. Ainsi, le scénario analysé porte sur d'explosion dans un silo de stockage de produits finis (susceptible de libérer une substance dangereuse) d'une installation classée. Cette mise en application vise à démontrer la faisabilité de la démarche proposée sur un scénario industriel réel, et à étudier les apports et limites de l'approche proposée.

Chapitre 1

La démarche d'analyse de risques et ses évolutions

Ce premier chapitre vise à définir le cadre général de nos travaux : l'analyse de risques. En effet, cette démarche diffère selon le risque considéré, les acteurs impliqués et les systèmes étudiés. Afin de positionner notre contexte de thèse et nos objectifs de travail, il est nécessaire de préciser les différentes caractéristiques relatives au concept de risque.
Ainsi, nous proposons d'aborder ces différents points à partir d'aspects généraux puis de nous focaliser sur des notions plus spécifiques à notre problématique.

La première partie permet tout d'abord de proposer différentes définitions de la notion de risque et de présenter les étapes générales du processus d'analyse de risques. Partant d'une définition générale du risque, nous nous focalisons sur le risque incidentel/accidentel pour ensuite définir la démarche d'analyse de risques.

Ayant défini ce processus de manière globale, nous pouvons l'aborder au regard des différents acteurs classiquement étudiés dans le domaine des analyses sectorielles : le système technique, l'opérateur humain et l'organisation. Pour ce faire, nous abordons tout d'abord ces évolutions de manière temporelle puis nous nous focalisons sur les spécificités de l'étude de chacune des ressources susmentionnées.

La troisième partie propose un panorama de méthodes développées dans un domaine récent des analyses de risques, celui des analyses globales (ou intégrées). Sans prétendre à l'exhaustivité, nous étudions et positionnons un ensemble de méthodologies au regard de critères utiles pour le développement de notre approche (comme par exemple : les ressources considérées dans l'analyse, les domaines d'applications ...).

Enfin, l'identification de certaines limites dans ces démarches, nous permet de définir notre approche de travail dans la dernière partie de ce chapitre.

1.1 La notion (d'analyse) de risques

Le risque est un concept aujourd'hui largement étudié, et pour lequel il existe de nombreuses définitions et méthodes d'analyses. Son caractère polysémique s'explique par la diversité des domaines d'application et des problématiques associées [1] (comme la finance, l'industrie, l'environnement ...).
Cette partie nous permet ainsi de positionner le type de risque considéré et de justifier la définition utilisée dans notre problématique. Ce positionnement amène à la présentation du processus d'analyse de risques classiquement utilisé dans le domaine industriel et à une adaptation de ce dernier à notre problématique.

1.1.1 De la naissance du concept ...

Selon [Pradier, 2004], « si l'on cherche dans des ouvrages savants une histoire du concept de risque, on trouvera en particulier deux éléments récurrents : une thèse moderniste et un roman nautique pour expliquer l'origine du mot ».
La thèse moderniste justifie l'avénement de la notion de risque comme une conséquence du développement du capitalisme. Alors que le roman nautique trouve sa justification plus en amont dans l'étymologie du terme.
Ainsi pour la première des écoles, selon [Lannoy, 2008], « l'apparition du risque remonte au début de la Réforme religieuse et de l'apparition du capitalisme, au développement du commerce et des assurances ».
Alors que pour la deuxième école, le risque est défini par ses « origines étymologiques latines ..., qui existe depuis la fin de l'antiquité » et par « l'implication et l'usage maritime de ce mot ». De plus, pour cette école, une autre justification est avancée : « les problèmes de risque ont bien été entrevus par les Romains et aussi au Moyen-Âge ; enfin, selon certains économistes, l'esprit du capitalisme était déjà bien présent dans l'Italie du treizième siècle ».
Mais au delà de ces écoles, qui permettent de positionner dans le temps la naissance de ce concept, ce sont les faits déclencheurs de l'approche scientifique du risque qui nous intéressent plus particulièrement.

Historiquement, l'approche scientifique du risque apparaît au dix-huitième siècle après le tremblement de terre de Lisbonne (en 1755) [Dufour, 2008]. Ce tremblement de terre engendra un tsunami et des incendies qui ravagèrent la ville et causèrent la mort de dizaines de milliers de personnes. Cet événement naturel majeur (considéré comme l'un des séismes les plus destructeurs et les plus meurtriers de l'histoire) fit évoluer les consciences vers une responsabilisation de l'Homme, alors qu'elles s'en remettaient jusque-là systématiquement à la Providence (ou responsabilité des dieux) [2].

1. « Chaque activité comporte des risques qui sont propres à son exercice. » [Desroches *et al.*, 2007]

2. Comme l'écrivit Rousseau, dans sa « Lettre sur la Providence » (18 août 1756), en réponse au poème de Voltaire sur le désastre de Lisbonne : « Je ne vois pas qu'on puisse chercher la source du mal moral ailleurs que dans l'homme libre, perfectionné, partant corrompu ; et, quant aux maux physiques, ils sont inévitables dans tout système dont l'homme fait partie ; la plupart de nos maux physiques sont encore notre ouvrage. Sans quitter votre sujet de Lisbonne, convenez, par exemple, que la nature n'avait point rassemblé là vingt mille maisons de six à sept étages, et que si les habitants de cette grande ville eussent été dispersés plus également, et plus légèrement logés, le dégât eût été beaucoup moindre, et peut-être nul. Combien de malheureux ont péri dans ce désastre, pour vouloir prendre l'un ses habits, l'autre ses papiers, l'autre son argent ? ». Ecrits qu'il justifia plus tard dans ses Confessions (volume IX) : « et je lui prouvai que de tous

C'est à partir de cette époque que l'on commence à se soucier des risques liés à l'activité humaine, en évaluant leurs effets potentiels et en proposant des solutions pour que ces effets soient les plus faibles possibles [Lannoy, 2008].

Mais la Révolution Industrielle (19^{ieme} siècle), caractérisée par une profonde transformation des sociétés sous l'effet des progrès techniques et du développement de l'industrie, va révéler l'importance de ce concept. En effet, l'industrialisation engendre une main d'œuvre très importante (hommes, femmes et enfants sont mobilisés) qui travaille souvent dans de mauvaises conditions et où les accidents sont fréquents.
Et ces accidents seront à l'origine (à la fin du 19^{ieme} siècle) de la première réglementation en terme de risque en France, au travers de la loi du 9 avril 1898 qui définit la notion de risque professionnel.

Ce sont principalement les évolutions de cette réglementation qui vont permettre la formalisation et l'utilisation d'outils d'analyse et de prédiction de ces risques. En effet, cette dynamique de normalisation sera à l'origine, durant le 20^{ieme} siècle (et surtout après la seconde guerre mondiale et pendant la guerre froide), du développement des approches fiabilistes (ou probabilistes) par des auteurs comme A. Markov (pour l'approche par chaînes de Markov), R. von Mises (pour l'approche fréquentielle), B. de Finetti (pour l'approche bayésienne, à partir du théorême formulé par T. Bayes en 1763), W. Weibull (pour l'étude de la fatigue des matériaux à partir de la distribution qui porte son nom), E. Murphy (pour l'énoncé de sa loi [3] qui est à l'origine du concept d'ingénierie de sûreté) ...

Ainsi, l'avènement de la notion de risque et des méthodes d'analyse est un processus qui s'inscrit dans le temps et qui suit l'évolution des mentalités et les avancées technologiques. Ces caractéristiques sont la source de la multitude de définitions et de méthodes existantes à l'heure actuelle.

1.1.2 ... à ses caractéristiques actuelles

Avant de définir le risque tel qu'il est considéré dans cette problématique, il convient de préciser quelles sont ses spécificités générales (au delà du type de risque considéré et de la manière de le mesurer). Au regard de ce positionnement, il est alors possible d'identifier les étapes usuellement suivies dans le processus d'analyse des risques d'un système. Enfin, et pour répondre aux besoins de notre problématique, nous terminons cette partie par la proposition d'une extension de ces étapes à d'autres dimensions des systèmes.

1.1.2.1 Le risque

De manière générale, selon [Robert, 2008], le risque se définit comme « un danger [4] éventuel, plus ou moins prévisible ».
Cette définition orientée sur les aspects négatifs du risque est largement utilisée dans

ces maux, il n'y en avait pas un dont la Providence ne fût disculpée, et qui n'eût sa source dans l'abus que l'homme a fait de ses facultés plus que dans la nature elle-même ».

3. « S'il y a plus d'une façon de faire quelque chose, et que l'une d'elles conduit à un désastre, alors il y aura quelqu'un pour le faire de cette façon ».

4. Danger : « Potentiel de dommage ou de préjudice portant atteinte aux personnes, aux biens ou à l'environnement. » [Desroches *et al.*, 2006]

les domaines de la santé, des transports, de l'industrie, de l'environnement ... En effet, lorsque l'on s'intéresse à des événements pouvant impacter l'homme (sa vie ou sa santé), l'environnement (préservation de la faune et de la flore) ou les structures (préservation de l'outil de production), il est difficile de considérer le risque autrement que comme une menace.
À contrario, dans certains domaines (comme le management ou la finance), le risque possède également une dimension positive, définie sous le terme d'opportunité (au sens où il peut être non plus la source d'une perte, mais celle d'un gain potentiel).
Par conséquent certains travaux [5] proposent, pour des problématiques de management des risques [6], de considérer à la fois les aspects négatifs du risque mais également ses aspects positifs.

D'un point de vue plus spécifique, les risques qui nous intéressent dans cette problématique, sont les risques industriels liés à l'occurrence d'incidents ou d'accidents majeurs pouvant impacter les hommes, l'environnement et/ou les structures ; autrement dit les risques liés à l'exploitation d'un système de production :
- Le risque technique, qui est le risque associé à un événement redouté résultant de l'incertitude sur le savoir-faire technologique et technique de l'activité ou de l'entreprise ou sur sa capacité à répondre au besoin [7].
- Le risque opérationnel, qui est le risque lié au déroulement d'une activité ou au fonctionnement d'une entreprise.
- Le risque technologique, qui est le risque pour l'activité ou l'entreprise ayant pour origine son environnement technologique.
- Le risque naturel, qui est le risque associé à un événement redouté naturel dont l'apparition est indépendante de la volonté de l'homme.

Ce positionnement permet de restreindre le champ des définitions possibles. En effet, nous ne considérerons pas, dans nos travaux, les risques liés aux secteurs routier, hospitalier, juridique, économique, financier ...

Ainsi, dans le domaine industriel, il existe de nombreuses définitions qui présentent le risque (ou plutôt sa mesure) comme une entité à deux dimensions : probabilité d'occurrence d'une part et conséquence(s) d'autre part [Leroy et Signoret, 1992].

Citons notamment les définitions de :
- [Villemeur, 1992], pour qui le risque est « une mesure d'un danger associant une mesure de l'occurrence d'un événement indésirable et une mesure de ses effets ou conséquences ».
- [European Council, 1997], qui définit le risque comme la probabilité pour qu'un effet spécifique se produise dans une période donnée ou dans des circonstances déterminées.
- [OHSAS, 1999], qui le caractérise comme la « combinaison de la probabilité et de la (des) conséquence(s) de la survenue d'un événement dangereux spécifié ».

5. Citons les travaux de [Barthélemy, 2000], [Project Management Institute, 1992] et [Project Management Institute, 1996].

6. Selon [Courtot, 2002], « le management des risques est un ensemble de concepts, démarches et outils qui se concrétise par un processus continu et itératif visant successivement à identifier et analyser les risques, à les évaluer et les hiérarchiser, à envisager les moyens de les maîtriser, à les suivre et les contrôler et, enfin, à capitaliser le savoir-faire et l'expérience acquis dans ce domaine ». En ce sens le management des risques englobe notre problématique, car nous nous focalisons uniquement sur la démarche d'analyse de risques.

7. Cette définition et les suivantes sont issues de [Desroches *et al.*, 2006].

– [ISO, 2003] et [ISO, 2007], pour lesquelles il est présenté comme la combinaison de la probabilité d'occurrence d'un dommage et de la gravité de ce dommage (cf. figure 1.1).

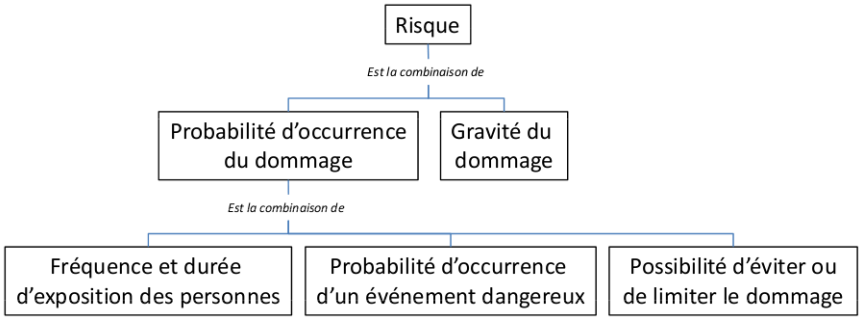

FIG. 1.1 – Définition du risque selon les normes ISO 12100-1 et 14121-1

– [Desroches *et al.*, 2006], qui le décrivent comme la caractéristique d'un événement, définie conjointement par sa vraisemblance d'occurrence et la gravité de ses conséquences.
– [Lannoy, 2008], qui voit le risque comme un ensemble de scénarios, chacun ayant une probabilité d'occurrence et une conséquence, généralement négative.

Ces définitions peuvent être source d'erreur car elles amènent « à penser que les composantes du risque sont de même nature et peuvent être combinées selon une loi de composition interne » [Desroches *et al.*, 2006], et « il est inexact de considérer que le risque est lié à l'occurrence d'un événement unique. En effet, la réalisation d'un ensemble d'événements, isolément sans impact, peut s'avérer également catastrophique » [Gouriveau, 2003].

C'est pourquoi, nous proposons d'adopter pour nos travaux, une définition du risque plus générale, au sens où ce concept se positionne au centre d'un processus dynamique initié par un ensemble de causes, et aboutissant à un ensemble de conséquences :

– Pour [Gouriveau, 2003], le risque « peut être défini par l'association de caractéristiques d'événements causes et conséquences (ou effets) d'une situation donnée », que l'on peut représenter sur la figure 1.2.

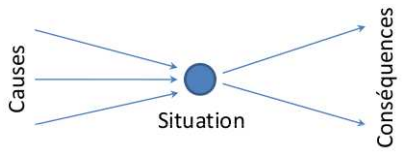

FIG. 1.2 – Composantes d'un risque reformulé par [Gouriveau, 2003]

– Selon [Desroches *et al.*, 2007], le risque est « la mesure de l'instabilité de la situation dangereuse ou menaçante et de la potentialité d'accident ... Plus précisément le risque est défini comme la mesure d'un ensemble d'éléments de la situation dangereuse qui, combinés à des conditions particulières d'environnement, redoutées ou non, connues ou non, peuvent entraîner des conséquences préjudiciables ou accidentelles ».

Enfin, le risque industriel peut être qualifié de « majeur » pour certains événements et certains domaines d'activités (comme le nucléaire, ou les Installations Classées). Ce risque, selon [European Council, 1997], est un « événement tel qu'une émission, un incendie, une

explosion d'importance majeure résultant de développements incontrôlés survenus au cours de l'exploitation, entraînant pour la santé humaine ou pour l'environnement, à l'intérieur ou à l'extérieur de l'établissement, un danger grave immédiat ou différé, en faisant intervenir une ou plusieurs substances ou des préparations dangereuses ».

Dans les définitions abordées précédemment, le risque est présenté comme une mesure. Cette notion se définit comme la représentation de la propriété d'un objet par un nombre ou un symbole, et des relations existantes entre les objets étudiés [Voisin, 1999]. Cette définition laisse entrevoir que pour mesurer un risque, il est nécessaire de suivre une méthode[8], au sens où les caractéristiques d'une mesure ne peuvent être obtenues sans la définition d'un minimum de règles spécifiques à cette mesure.
Nous allons donc préciser, dans la partie suivante, en quoi le processus d'analyse de risques peut être défini comme une méthode (aboutissant à l'élaboration de modèles).

1.1.2.2 L'analyse de risques

Dans [Desroches *et al.*, 2006], les auteurs définissent l'analyse de risques comme un « processus systématique d'utilisation et d'organisation d'informations disponibles sur les dangers et les vulnérabilités afin d'estimer les risques consécutifs pouvant contrarier le déroulement et les objectifs d'une activité ... L'analyse de risques permet d'approfondir la connaissance des risques identifiés ... Cette première approche permet notamment la hiérarchisation des risques en vue de donner des priorités de traitement. L'analyse de risques s'attache aussi à l'identification des causes racines, étape essentielle pour agir sur le risque ».

Si l'on considère à présent la définition normalisée ([ISO-CEI, 2002], [ISO, 2003], [ISO, 2007]), l'analyse de risques se positionne dans le processus (itératif) d'appréciation[9] et de réduction des risques (cf. figure 1.3).

Les trois premières étapes de la figure 1.3 forment le processus d'analyse de risques. Ainsi, quelle que soit la définition du risque retenue, ce processus devra suivre ces étapes : la définition des limites du système, l'identification des dangers (et/ou des opportunités, selon les vues choisies), et l'estimation des risques (à l'aide d'outils adaptés).

La première étape de ce processus d'appréciation des risques consiste à déterminer les limites de la machine (ou du système). Ces limites sont diverses :
- Limites d'utilisation, définies comme les limites de la machine lors d'une utilisation conforme à sa destination mais également lors d'un mauvais usage raisonnablement prévisible.
- Limites dans l'espace, définies comme les délimitations dans l'espace et la formation de systèmes partiels.

8. Une méthode est une technique de résolution de problèmes caractérisée par un ensemble de règles bien définies qui conduisent, pour le problème, à une résolution correcte. Toute méthode doit logiquement s'appuyer sur quatre facteurs indissociables : des modèles (représentation abstraite de la structure et/ou du comportement d'un système selon un point de vue.), des langages, une démarche et des outils informatiques [Calvez, 1990].

9. Appréciation des risques, selon [Desroches *et al.*, 2006] : « Processus informatif et pré-décisionnel regroupant l'identification, l'analyse et l'évaluation du risque. »

– Limites dans le temps, définies comme la durée de vie prévisible de la machine et/ou de certains de ses composants, en tenant compte de son utilisation normale.
– Autres limites, comme par exemple des limites environnementales, d'entretien ...

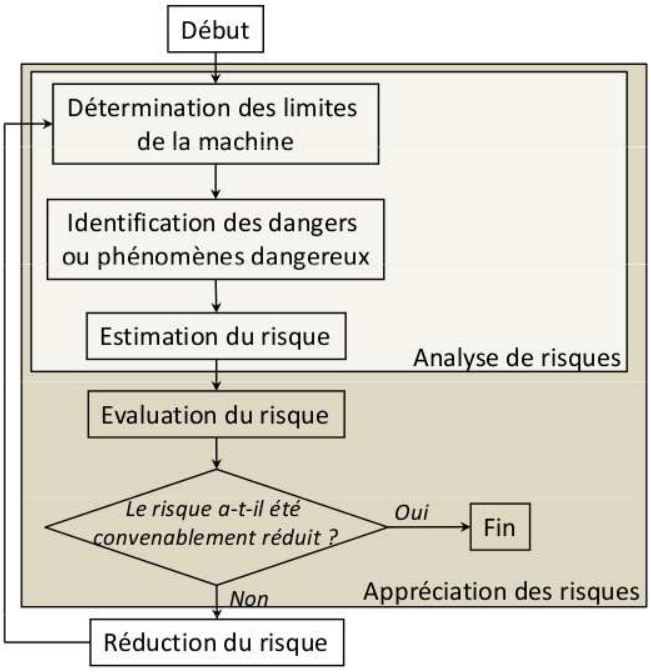

FIG. 1.3 – Processus d'appréciation et de réduction des risques selon [ISO, 2007]

La deuxième étape consiste à identifier les dangers, que l'on peut présenter comme un processus de recherche des risques de mise en présence d'un danger avec un élément vulnérable (identification des dangers, des situations dangereuses ou à risques, des situations accidentelles, des scénarios d'accidents).

Le troisième étape consiste à estimer le risque, c'est-à-dire à attribuer à un dommage une gravité probable et une probabilité (si l'on considère la définition normative), ou à exprimer les caractéristiques du risque de façon qualitative et quantitative (de manière plus générale). L'estimation du risque permet d'en mesurer intrinsèquement son importance indépendemment de toute décision de comparaison avec d'autres risques.

Afin de pouvoir identifier (ou décider) si le risque considéré est acceptable ou non, il convient de définir un référentiel d'acceptabilité (Evaluation du risque, cf. figure 1.3), au delà duquel le risque pris devient intolérable. Ces risques intolérables doivent être réduits, pour les rendre à nouveau acceptables, par le biais de moyens matériels, économiques, humains ... (Réduction du risque, cf. figure 1.3).

Le processus, présenté dans la figure 1.3, a pour vocation d'étudier le système d'un point de vue technique. Mais il existe aujourd'hui d'autres approches permettant d'expliquer (et d'estimer) ces risques. Ces approches sont, pour la plupart, centrées sur l'opérateur humain ([Villemeur, 1988], [Reason, 1990], [Amalberti, 1998]), et/ou sur l'organisation ([Perrow, 1990], [Roberts, 1990]). C'est pourquoi nous proposons d'adapter ce processus (cf. figure 1.4) pour pouvoir préciser les étapes de ces différents types d'analyses de risques.

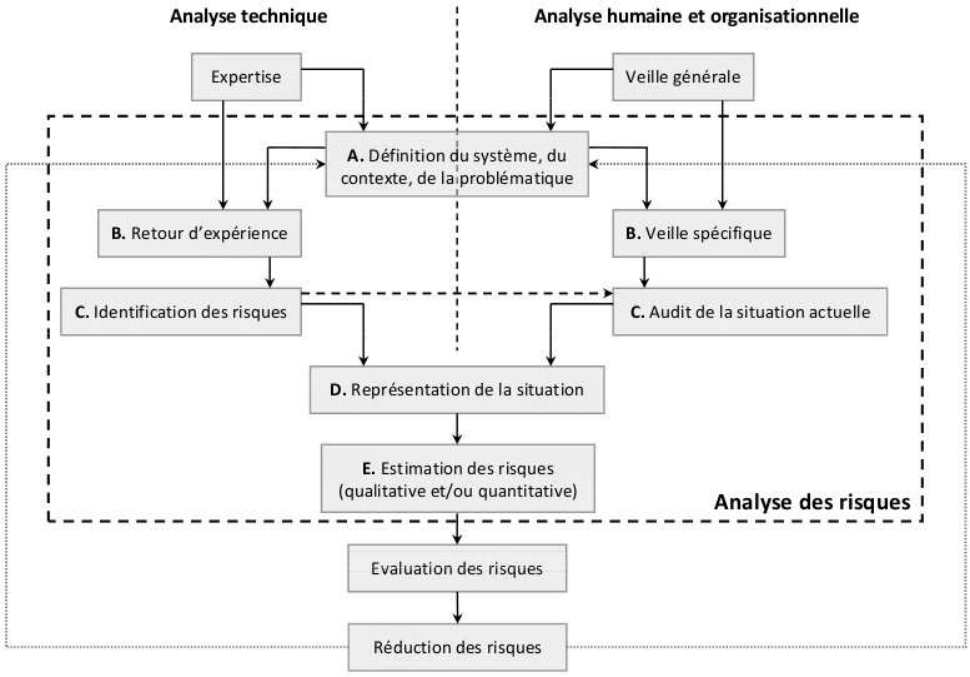

FIG. 1.4 – Démarche d'analyse de risques générale d'après [Duval *et al.*, 2006]

Il est possible de rattacher les étapes données dans la figure 1.4 à celles de la démarche d'analyse de risques « classique » (cf. figure 1.3) :

– L'étape A correspond à l'étape de « Détermination des limites de la machine ».
  À partir des connaissances disponibles dans le domaine concerné, cette étape permet de définir les limites du système considéré. Ces limites sont identiques à celles définies pour l'approche normative, avec un ajout : les limites liées aux ressources. Ces dernières permettent de définir quelles ressources (technique, humaine, organisationnelle ...) sont à considérer dans l'analyse.

– Les étapes B et C correspondent aux étapes d'« identification des dangers ou phénomènes dangereux ».
  L'étape B permet, à partir des connaissances générales du domaine (Expertise et Veille générale) et de la délimitation du système considéré, de selectionner les cas qui se rapprochent le plus de la situation étudiée (Retour d'expérience [10] et Veille spécifique).
  L'étape C permet d'identifier les dangers liés à l'installation étudiée.
  La nature du danger considéré peut être matérielle (dispositif mécanique, substance chimique) ou immatérielle (énergie potentielle, formation incomplète d'un opérateur). Le danger peut être la propriété d'une substance (produit chimique toxique), un objet (machine), un phénomène (foudre, séisme), une situation (conflit social) ou un processus mal défini ou mal réalisé (erreur humaine, erreur de stratégie, erreur de management) [Desroches *et al.*, 2006].
  Ainsi, pour pouvoir étudier les caractéristiques humaines et organisationnelles liées au système considéré, il est nécessaire de connaître les caractéristiques techniques du système

10. Selon [Rakoto, 2004], le Retour d'expérience est une démarche structurée de capitalisation et d'exploitation des informations issues de l'analyse d'événements positifs et/ou négatifs. Elle met en œuvre un ensemble de ressources humaines et technologiques qui doivent être managées pour contribuer à réduire les répétitions d'erreurs et à favoriser certaines pratiques performantes.

étudié.

– Les étapes D et E correspondent à l'étape d'« estimation des risques ».
L'étape E permet, à partir d'une représentation de la situation (modélisée dans l'étape D) de donner une estimation des risques identifiés dans l'analyse. Cette estimation peut être qualitative ou quantitative en fonction des objectifs recherchés dans l'analyse, et des dimensions du système considéré.

Ces différentes étapes montrent que l'analyse de risques doit suivre un ensemble de règles, supportées elles-même par un ensemble d'outils (ces outils pouvant être des guides méthodologiques et/ou des logiciels) permettant de représenter (ou modéliser) le système. C'est pour ces raisons que l'analyse de risques est définie comme une méthode aboutissant à la définition d'un ensemble de modèles. L'élaboration de tels modèles nécessite une étape d'approbation (ou de légitimation) par l'ensemble des parties prenantes de l'analyse. Cette étape permet de s'assurer de la cohérence des aspects représentés dans le modèle par rapport à la réalité.

Avant de poursuivre la caractérisation des approches d'analyse de risques, il nous paraît nécessaire de poser un ensemble de définitions concernant les notions de système, de complexité, et de modélisation. En effet, toute démarche d'analyse de risques se base sur ces concepts largement définis. Mais la profusion des définitions entraîne une ambiguïté lorsqu'on utilise ces termes. C'est pourquoi, nous proposons un positionnement qui vise à lever ces ambiguïtés, et à définir les caractéristiques retenues pour le développement de notre démarche.

1.1.3 La modélisation des systèmes complexes

1.1.3.1 La notion de système

Un système est défini de manière générale comme un ensemble de notions ou de concepts organisés de manière logique et ayant pour but de traduire à l'aide de symboles tout ou partie du réel (au sens intellectuel du terme), ou comme un ensemble de moyens matériels et de procédés techniques destinés à obtenir des résultats définis (au sens pratique du terme) [Lugan, 2006].
Mais selon le domaine considéré (naturel, artificiel, social ...), ces systèmes n'ont pas forcément le même niveau d'intelligibilité [11]. Ainsi certains systèmes sont qualifiés de compliqués et d'autres de complexes [Le Moigne, 1990].

1.1.3.2 Complication et Complexité

Est compliqué [12], ce qui est composé d'un grand nombre de parties ou d'éléments. La profusion des éléments rend l'ensemble confus, difficile à saisir parce que les parties sont trop nombreuses ou agencées de telle sorte que l'on ne voit plus le rapport qui existe entre elles.
Un système compliqué est un système dans lequel les éléments s'empilent les uns sur les autres et s'enchaînent de façon linéaire. Il est alors possible de le comprendre en le

11. Un fait intelligible est un fait dont on peut saisir aisément la signification, que l'on peut comprendre sans difficulté ou parce que l'on en connaît la cause, le déroulement.
12. Du latin *cum pliare*, empiler avec.

décomposant en pièces élémentaires dont chacune est expliquée en détail pour reconstituer ensuite le fonctionnement global du système [Narbonne, 2005]. Il a un comportement déterministe et peut être simplifié pour découvrir son intelligibilité.

Est complexe[13], ce qui contient beaucoup d'enchevêtrements, où « tout est lié », et pour lequel l'analyse d'une petite partie de l'objet d'étude de façon isolée n'est pas envisageable. Cette notion implique celle d'imprévisible possible, d'émergence plausible du nouveau et du sens au sein du phénomène que l'on tient pour complexe.
Un système complexe n'est pas directement décomposable[14] sous peine de détruire son intelligibilité, mais il est quasi-décomposable, lorsqu'on peut y identifier des sous-systèmes[15] reliés entre eux et avec l'environnement [Lugan, 2006]. Il est par essence même non déterministe et doit être modélisé pour construire son intelligibilité.

Il n'est donc pas possible de réduire ce qui est compliqué à ce qui est complexe (et inversement). La simplification du compliqué appliqué au complexe a pour conséquence une aggravation de la complexité par mutilation et non pas la résolution du problème considéré [Le Moigne, 1990].
Ainsi, un système complexe se définit comme une construction mentale, variable en fonction du contexte et de nos intentions, que nous élaborons pour faciliter la compréhension et la construction d'un réel complexe [Narbonne, 2005]. C'est un outil intellectuel permettant de se représenter la réalité en incluant l'observateur dans la problématique.

Nous retiendrons, pour nos travaux, la définition donnée par [Von Bertalanffy, 1968] : « un système est un ensemble d'éléments identifiables, interdépendants, c'est-à-dire liés entre eux par des relations telles que, si l'une d'elles est modifiée, les autres le sont aussi et par conséquent tout l'ensemble du système est modifié, transformé. C'est également un ensemble borné dont on définit les limites en fonction des objectifs (propriétés, buts, projets, finalités) que l'on souhaite privilégier ».

Notons par ailleurs que la compréhension d'un système complexe ne se fait pas en descendant au niveau des composants élémentaires mais en identifiant les sous-systèmes qui jouent un rôle dans le fonctionnement du système. Cela suppose de définir clairement les frontières de ces sous-systèmes pour faire ensuite apparaître les relations qu'ils entretiennent entre eux ainsi que leur finalité par rapport à l'ensemble [Donnadieu *et al.*, 2003].
Par conséquent, le degré de complexité d'un système dépend principalement :

- du nombre (phénomène quantitatif) de niveaux d'organisation, d'éléments par niveaux, de relations entre niveaux, et de relations entre éléments par niveaux,
- de la nature ou de la complication (phénomène qualitatif) des relations entre éléments et des relations entre niveaux.

13. Du latin *cum plexus*, attacher avec.

14. La somme des fonctions de chacune des parties le composant n'est pas réductible à la somme des fonctions du système global.

15. C'est un ensemble qui manifeste une certaine subordination à l'égard du système dont il est partie intégrante. On repère un sous-système à l'intérieur d'un système ou considéré comme tel, par une intensité plus grande des interactions entre certains composants par rapport aux autres composants.

1.1.3.3 La modélisation et les modèles

De nombreux auteurs ont reconnu l'importance de l'étape de modélisation pour la compréhension d'un système complexe :
- « La vision du monde que chacun d'entre nous s'est constitué n'est rien d'autre qu'un modèle. Toutes nos décisions sont prises à partir des modèles. Toutes les lois sont écrites en se fondant sur des modèles. » (J.W. Forrester dans [Lesbats *et al.*, 1997])
- « Nous ne raisonnons que sur des modèles. » (P. Valery dans [Narbonne, 2005])
- « Toute image mentale est un modèle, flou et incomplet, mais servant de base aux décisions. » [Narbonne, 2005]

Ce dernier point nous permet d'avancer qu'un modèle est sans doute plus simple que la réalité qu'il représente. C'est la raison pour laquelle nous le comprenons et nous pouvons l'utiliser pour orienter nos actions [Donnadieu *et al.*, 2003].

a - L'action de modéliser

La modélisation peut être définie, de manière générale, comme l'opération par laquelle on établit un modèle d'un phénomène (perçu complexe), afin d'en proposer une représentation interprétable, reproductible et simulable [Diebolt, 1998]. Mais la modélisation est aussi un art par lequel le modélisateur exprime sa vision de la réalité. En ce sens, la même réalité, perçue par deux modélisateurs différents, ne débouchera pas nécessairement sur le même modèle [Donnadieu *et al.*, 2003].
La modélisation postule également que l'action de modéliser n'est pas neutre et que la représentation du phénomène n'est pas disjoignable de l'action du modélisateur[16]. Elle veille également à expliciter les points de vue que se propose l'observateur concepteur qui la met en œuvre et à souligner son propre projet (qui est de proposer une des formes de compréhension intelligible du phénomène sans prétendre l'expliquer[17]) [Diebolt, 1998].

En ce sens, une approche de modélisation peut être décrite par un processus de modélisation, des vues de modélisation, des concepts de modélisation et des langages de modélisation [Zaidat, 2005].
Un processus de modélisation consiste au développement d'un ensemble de modèles de description du système étudié. La réalisation de ce processus requiert l'utilisation de techniques de modélisation appropriées.
Une vue de modélisation permet de se focaliser sur une partie particulière du modèle intégré du système étudié.
Les concepts et langages de modélisation représentent les règles, la sémantique et les objets définis par les méthodes utilisées pour construire les modèles.

b - Le modèle, une vision de la réalité

Un modèle est une représentation abstraite (composée de concepts et de symboles) de la structure et/ou du comportement d'un système selon un point de vue donné [Iung, 1992]. Il se construit pour répondre à une problématique relative à l'objet modélisé, d'où l'importance de l'objectif assigné au modèle qui doit alors précéder et orienter la conception et la

16. C'est ce que l'on nomme la projectivité du système de modélisation. C'est la capacité du modélisateur à expliciter ses projets de modélisation, *i.e.* les finalités qu'il propose au modèle d'un système complexe qu'il perçoit *a priori* finalisé et finalisant [Le Moigne, 1990].
17. Cela se passe « comme si », et non : Cela se passe « comme cela, et seulement comme cela ».

construction de ce modèle.
Le modèle est alors un « système de symboles » dont l'extrême souplesse potentielle permet de rendre compte de la plupart des perceptions dont on dispose lorsque l'on souhaite décrire un phénomène (observé ou imaginé) afin de l'interpréter intelligiblement [Diebolt, 1998]. Plutôt que de « commencer par simplifier », l'observateur peut aujourd'hui « commencer par modéliser », et ceci de façon intelligible, reproductible et communicable.
Nous pouvons donc avancer qu'un modèle n'est qu'une façon de représenter la réalité et est indépendante de cette même réalité (abstraction), il se peut fort bien que deux ou plusieurs modèles soient capables de rendre compte d'un même ensemble de phénomènes [Narbonne, 2005].

Ainsi, les principes définis dans cette partie, nous permettent d'aborder plus formellement les spécificités des différentes démarches d'analyse de risques. Ces spécificités portent d'une part, sur l'identification des propriétés des systèmes considérés (les acteurs et leurs interactions), et d'autre part, sur la caractérisation des méthodes, modèles et outils permettant d'analyser les risques liés à l'exploitation de ces systèmes.

1.2 L'analyse de risques sectorielle

Tout comme la notion de risque, l'avénement de l'analyse de risques s'inscrit dans l'histoire industrielle, et ses évolutions font échos aux accidents majeurs jalonnant cette histoire.
Ainsi cette partie présente tout d'abord les accidents ayant permis d'élargir le champ des analyses de risques, puis se focalise sur les méthodes actuellement utilisées pour mener à bien ces différentes analyses. La différence vient du fait qu'une analyse sectorielle se focalise sur une ressource du système. L'étude de cette ressource implique un champ d'expertise spécifique, et par conséquent un mode de représentation [18] particulier.

1.2.1 Les accidents industriels comme leviers de développement

Au delà des avancées technologiques qui ont contribué (et contribuent encore) à l'évolution du processus d'analyse de risques, certaines catastrophes ont mis en évidence une complexification des systèmes [19], et l'émergence de nouvelles causes liées à l'occurrence de ces accidents [20].
En effet si jusque dans les années soixante-dix, les études étaient focalisées sur les défaillances technologiques des systèmes [Villemeur, 1992], un certain nombre d'accidents ont mis en évidence l'importance du facteur humain dans l'occurrence de ces accidents (cf. tableau 1.1).
Si bien que dans les années quatre-vingts, de nombreuses méthodes consacrées à une meilleure prise en compte de ce type de facteurs ont émergées, comme les méthodes

18. Un mode de représentation définit la manière dont l'individu appréhende la réalité qu'il observe. Cette appréhension est rendue possible par le biais de processus de compréhension et de conceptualisation, eux-mêmes conditionnés par les connaissances et l'expérience de l'individu.

19. Cette complexification est à la fois technologique et interactionnelle (interactions entre composants et/ou systèmes, entre composants et opérateurs, entre systèmes et opérateurs ...).

20. Ces causes viennent du fait que le système considéré jusqu'alors était essentiellement axé sur sa dimension technique. Cette vision devient caduque lorsque l'on constate que cette technique se positionne dans un environnement, dont les interactions peuvent conduire à l'occurrence de situations critiques.

THERP [21], CREAM [22] ou ATHEANA [23] ...
Mais l'occurence d'autres accidents ont permis d'identifier des causes sous-jacentes à ces défaillances techniques et humaines : les dysfonctionnements organisationnels (cf. tableaux 1.2 et 1.3). L'étude de ces dysfonctionnements constitue un champ disciplinaire des sciences sociales modernes : la théorie des organisations [Clegg *et al.*, 1996]. Cette théorie se scinde en plusieurs communautés du fait des points de vues (fonctionnels, dysfonctionnels, optimistes, pessimistes ...) considérés pour aborder l'organisation d'un système et l'étude de ses évolutions.

Chacun de ces accidents, du fait de la criticité de ses conséquences (humaines, environnementales, économiques ...), a fait l'objet d'une analyse rendue publique : [Department of Transport, 1975] pour l'explosion de Flixborough, [Seveso, 1982] pour le nuage toxique de Seveso, [Kemeny, 1979] pour l'accident nucléaire de Three Mile Island, [Union Carbide Corporation, 1985] pour la catastrophe de Bhopal, [Roger's Commission, 1986] et [Roger's Commission, 1987] pour la perte de la navette Challenger, [Department of Energy, 1987] pour l'accident nucléaire de Tchernobyl, [Lord Cullen, 1987] pour l'explosion de la plate-forme Piper Alpha, [Lord Cullen, 2001] pour la collision de trains à Ladbroke Grove, [Barthelemy *et al.*, 2001] pour l'explosion de l'usine AZF, [CAIB, 2003] pour la perte de la navette Columbia.

Enfin les évolutions de ces dernières décennies, sur la compréhension des processus incidentels/accidentels, permettent aujourd'hui le développement d'approches de management global des risques (cf. figure 1.5). Ces approches sont qualifiées de globales car elles ne se restreignent pas à un type de causes possibles pour expliquer l'occurrence d'incidents ou d'accidents. En effet, ces approches expliquent comment la combinaison de ces différents types de causes peut, à terme, mener à l'occurrence de l'événement redouté.

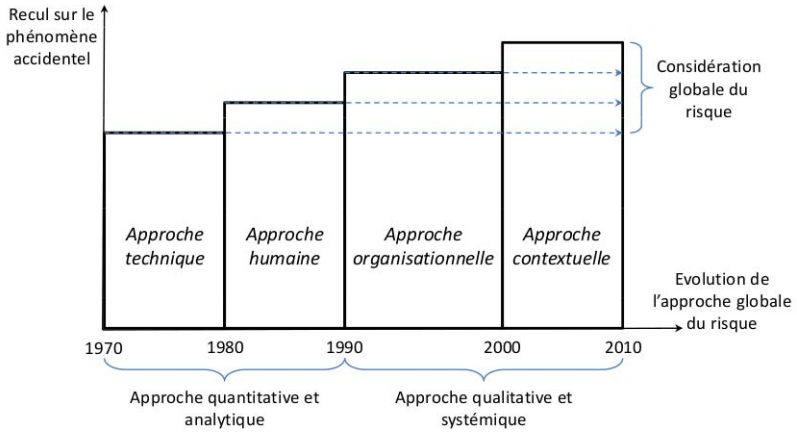

FIG. 1.5 – Représentation de l'évolution scientifique du Risque, selon [Dufour, 2008]

21. THERP : Technique for Human Reliability Analysis [Swain et Guttman, 1983].
22. CREAM : Cognitive Reliability and Error Analysis Method [Hollnagel, 1998].
23. ATHEANA : A Technique for Human Error Analysis [Barriere *et al.*, 2000].

Année	Intitulé	Caractéristiques de l'accident	Impacts	Enseignements
1974	Flixborough	Explosion de 50 tonnes de cyclohexane dans une usine chimique produisant un intermédiaire pour le nylon	- 28 morts - 36 blessés graves - Dommages matériels	- Gestion des modifications - Mises à jour des analyses de risques sur les systèmes modifiés - Définition du risque technologique majeur
1976	Seveso	Relâchement et diffusion de dioxine d'un réacteur d'une usine chimique	- Catastrophe écologique - 193 personnes malades - 1 mort indirecte	- Mise en place des installations classées (IC) - Elaboration de la directive 96/82/CE
1979	Three Mile Island	Fusion partielle du coeur du réacteur n°2 de la centrale nucléaire	- Trés faible relâchement de produits radioactifs dans l'environnement	- Compréhension et prise en compte du facteur humain - Révision des procédures accidentelles - Approche par états (actions données aux opérateurs en fonction des paramètres dont ils disposent.)

TAB. 1.1 – Accidents majeurs à l'origine du développement de l'étude des facteurs humains

Année	Intitulé	Caractéristiques de l'accident	Impacts	Enseignements
1984	Bhopal	Relâchement d'un nuage toxique dans une usine chimique de production de pesticides	- Catastrophe humaine (362 540 victimes diverses) - Dégats écologiques importants	- Respect des périmètres de sécurité - Importance du processus de retour d'expérience (REX) - Importance de la gestion des risques et de la gestion de crise - Importance de la formation - Responsabilisation de l'organisation
1986	Challenger	Désintégration d'une navette spatiale lors de son décollage (joint défectueux)	- Mort des 7 membres d'équipage	- Importance de la conception et du REX - Communication entre équipes - Culture d'infaillibilité
1986	Tchernobyl	Fusion du coeur du réacteur n°4 de la centrale nucléaire	- Catastrophe humaine (polémique sur le nombre de victimes) - Catastrophe écologique	- Importance de la conception, du REX et du respect des procédures - Importance du contrôle de sûreté par les pouvoirs publics - Anticipation des crises - Importance de l'organisation du travail et de la formation

TAB. 1.2 – Accidents majeurs à l'origine du développement de l'étude des dysfonctionnements organisationnels - Partie 1

Année	Intitulé	Caractéristiques de l'accident	Impacts	Enseignements
1988	Piper Alpha	Explosion puis incendie dans une plate-forme off-shore	- 167 morts	- Mise en évidence du rôle de la maintenance pour la sûreté - Importance de la conception - Mise en place d'un organisme de contrôles réglementaire
1999	Ladbroke Grove	Collision entre deux trains transportant des passagers (non-respect d'une signalisation)	- 31 morts - 520 blessés	- Complexification de l'exploitation du fait de la privatisation - Importance de la formation (des employés et des sous-traitants) - Importance de la communication - Partage des standards - Intégration de la sûreté à tous les niveaux hiérarchiques
2001	AZF	Explosion d'un stock de 400 tonnes de nitrate d'ammonium	- 30 morts - 2500 blessés - De lourds dégâts matériels	- Traumatisme de la population - Polémique sur les causes de l'accident (incompatibilité des produits, acte de malveillance, erreur de manipulation ...)
2003	Columbia	Désintegration d'une navette spatiale lors de sa rentrée atmosphérique (trou dans la protection thermique)	- Mort des 7 membres d'équipage	- Importance de la culture de sûreté - Importance des signaux faibles - Normalisation de la déviance - Importance de la communication - Pressions de production

TAB. 1.3 – Accidents majeurs à l'origine du développement de l'étude des dysfonctionnements organisationnels - Partie 2

Les caractéristiques et méthodes couramment utilisées pour réaliser ces différentes analyses sont abordées dans les parties suivantes et suivent les évolutions chronologiques présentées précédemment.

1.2.2 Les approches classiques : l'étude des systèmes techniques

1.2.2.1 La diversité des approches

a - Induction ou Déduction

Le raisonnement inductif part de la connaissance du comportement d'un ensemble de cas particuliers pour en extraire des règles généralisées ; alors que le raisonnement déductif définit des concepts génériques qui sont confirmés (ou non) par observations sur des cas particuliers.

Dans un objectif d'analyse de risques, l'approche inductive (souvent qualifiée d'approche montante, ou « bottom-up ») permet d'identifier les événements conséquences d'une situation donnée à partir de ses événements causes [Desroches *et al.*, 2007].

L'approche déductive (ou approche descendante, « top-down ») définit le processus inverse, à savoir : identifier les événements causes à partir de la connaissance des événements conséquences de la situation étudiée.

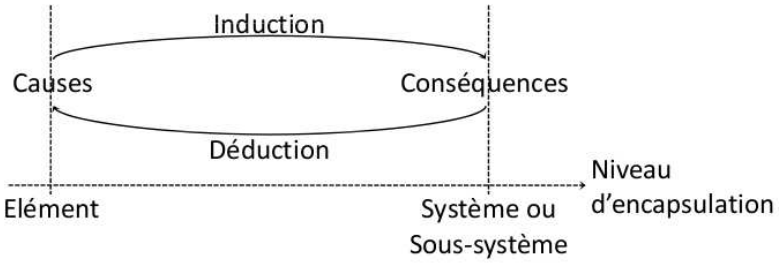

FIG. 1.6 – Principe des approches inductives et déductives

Ainsi dans l'approche inductive, l'analyste utilise des causes définies à un niveau élémentaire pour aboutir à des conséquences de niveau système (ou sous-système). Alors que dans l'approche déductive, ce sont ces conséquences de niveau système qui permettent d'aboutir à des causes de niveau élémentaire.

b - Qualification ou Quantification

La quantification consiste à donner une valeur numérique à certains éléments du système analysé (comme par exemple un taux de défaillance, la probabibilité d'occurrence d'un événement ...) alors que la qualification a pour objectif de donner une appréciation sur ces éléments (comme par exemple définir un risque comme étant de niveau faible, décrire textuellement une situation de travail ...). De manière générale, l'analyse qualitative des riques précéde leur analyse quantitative.

c - Approche Statique ou Dynamique

Une approche statique décrit les états d'équilibre du système étudié, alors qu'une approche dynamique décrit les états transitoires du système étudié, et donc ses évolutions dans le

temps (comme par exemple le vieillissement de certains composants ...). En ce sens, une représentation dynamique reste valable sur une fenêtre temporelle plus ou moins large (définie dans l'analyse), alors qu'une représentation statique est une vue plus globale considérée sur un espace temporel beaucoup plus large que pour l'approche dynamique et où toute modification dans le système nécessite d'actualiser manuellement l'analyse existante.

1.2.2.2 La diversité des outils supports à l'analyse

Il existe aujourd'hui de nombreuses méthodes qui couvrent, totalement ou partiellement, les étapes d'une analyse de risques [Villemeur, 1988], comme, par exemple, les tableaux, les représentations graphiques et les simulations à partir de jeux de données.

a - De l'usage des tableaux

Les approches abordées dans ce paragraphe utilisent les tableaux comme moyen de présentation synthétique des résultats de l'analyse, et regroupent principalement : l'analyse préliminaire des dangers/risques (**APD**, **APR**), l'analyse des modes de défaillances, de leurs effets et de leur criticité (**AMDE**, **AMDEC**), et la méthode « Hazard and operability » (**HAZOP**).

Ces démarches dysfonctionnelles[24] se basent sur des études fonctionnelles[25] du système étudié et s'utilisent généralement en amont d'études de sûreté de fonctionnement plus spécifiques.

En effet, ces démarches identifient les causes, effets et/ou conséquences relatives à des dangers (**APD**, **APR**), défaillances de composants (**AMDE**, **AMDEC**) ou dérives de paramètres (**HAZOP**), sans chercher à représenter précisément les scénarios pouvant mener à l'occurrence de ces événements critiques (cf. tableau 1.4).

Or, pour démontrer la maîtrise d'un risque industriel majeur, il est nécessaire d'identifier clairement l'enchaînement causal des événements menant à son occurrence [European Council, 1997].

Méthode	Raisonnement	Quantification	Evolutions temporelles
APD	Inductif	Non	Non
APR		Oui	
AMDE	Inductif	Non	Non
AMDEC		Oui	
HAZOP		Non	

TAB. 1.4 – Caractéristiques des méthodes utilisant les tableaux pour l'analyse de risques

b - La représentation graphique

La représentation des causalités d'un scénario accidentel ne peut être appréhendée que par un modèle. Ce dernier peut prendre différentes formes (textes, symboles, équations mathématiques ...), mais la forme graphique semble être celle qui s'adapte le mieux à la problèmatique

24. Une analyse dysfonctionnelle permet « d'identifier l'ensemble des défaillances pouvant apparaître dans le système, seules ou combinées entre elles, et à analyser l'impact de ces pannes ».

25. Une analyse fonctionnelle permet de « détailler la manière dont le système va opérer dans toutes ses phases de vie, ainsi que les autres systèmes avec lequel il va pouvoir intéragir » [Schneider Electric, 2004].

d'analyse de risques d'un système technique.
En effet, la représentation graphique peut être, à la fois, synoptique et globale, complète et détaillée, tout en restant directement intelligible pour l'esprit humain [Durand, 1994]. En effet, intégrant et reliant les qualités de l'écrit et de l'image, la représentation graphique est l'un des outils les plus performants de la modélisation [Le Gallou, 1993]. C'est un véritable langage, à côté des langages naturels discursifs, écrits ou parlés, et du langage mathématique formel. Tous ces langages recourent d'ailleurs volontiers au langage graphique par des schémas et idéogrammes ainsi que par la géométrie et la théorie des graphes [Donnadieu *et al.*, 2003]. On lui attribue par ailleurs quatre avantages :

- Elle permet, après apprentissage, une appréhension globale et rapide du système représenté.
- Elle contient une forte densité d'informations dans un espace limité.
- Elle offre, par son caractère monosémique et semi-formel, une faible variabilité d'interprétation.
- Elle possède une bonne capacité heuristique[26] et peut donc être facilement utilisée dans un travail de groupe.

Ainsi, l'utilisation de certaines propriétés de la théorie des graphes[27] et, par conséquent, la théorie des arbres, permet de représenter explicitement ces causalités. Cette catégorie de méthodes regroupe principalement, cf. tableau 1.5, les diagrammes de fiabilité (**DdF**), les arbres des causes (**AdC**), les arbres d'événements (**AdE**), les diagrammes causes-conséquences (**DCC**), et les nœuds-papillons (**NP**).
Ces approches permettent d'analyser globalement le fonctionnement du système (**DdF**), d'identifier l'ensemble des causes menant à un événement redouté (**AdC**), d'identifier les conséquences résultantes d'un événement indésirable (**AdE**), ou de représenter la chronologie d'un accident (**DCC**, **NP**). Les caractéristiques communes à ces approches sont la nécessité de les combiner à d'autres méthodes (telles que l'**APR**, ou l'**AMDE**) pour pouvoir identifier et étudier les événements indésirables les plus critiques du système étudié, et/ou l'indépendance supposée des événements de base.

Si l'analyse nécessite de plus une prise en compte des évolutions temporelles des systèmes étudiés, d'autres méthodes doivent être appliquées car celles présentées jusqu'à présent ne peuvent modéliser ces aspects temporels. L'analyse de l'évolution des systèmes peut être abordée par la méthode de l'espace des états (**MEE**) qui couvre les graphes de Markov (**GM**) et les réseaux de Petri (**RdP**).

L'élaboration de ces modèles graphiques (cf. tableau 1.5), et/ou les calculs associés, peuvent parfois être difficiles à mettre en œuvre du fait des spécificités des données disponibles. Pour remédier à cette limitation, il existe des approches basées sur le traitement de ces données, qui permettent de construire le modèle de risque et/ou d'effectuer des calculs de manière automatique (au moyen de simulations informatiques).

26. L'heuristique se définit comme l'utilisation de règles empiriques qui facilite la recherche des faits et l'analyse de situations, dans un objectif de résolution de problèmes et de prise de décision, et dans un domaine particulier.
27. Comme la notion d'orientation, de chaîne, de connexité, de cycle ...

Méthode	Raisonnement	Quantification	Evolutions temporelles
DdF	Inductif	Oui	Non
AdC	Déductif	Oui	Non
AdE	Inductif	Oui	Non
DCC	Inductif et Déductif	Oui	Non
NP			
MEE	Inductif	Oui	Oui
GM			
RdP			

TAB. 1.5 – Caractéristiques des méthodes d'analyse utilisant la théorie des graphes

c - La simulation à partir de jeux de données

Ces approches (cf. tableau 1.6) regroupent principalement les simulations de Monte Carlo (**SMC**) et les réseaux de neurones (**RN**). Elles permettent d'analyser le fonctionnement du système modélisé et d'en prédire les évolutions. Mais, elles sont souvent difficiles à mettre en œuvre pour des systèmes complexes du fait notamment des données nécessaires à la simulation et du temps de calcul associé. Précisons également que ces simulations viennent en support à d'autres méthodes d'analyse, comme les approches graphiques.

Méthode	Raisonnement	Quantification	Evolutions temporelles
SMC	Déductif	Oui	/
RN	Inductif	Oui	/

TAB. 1.6 – Caractéristiques des méthodes utilisant la simulation informatique pour l'analyse

Les différentes approches présentées dans cette partie (les tableaux, les graphes, et les simulations) permettent d'analyser, de manière exhaustive, comment les défaillances des composants techniques d'un système industriel peuvent influer sur l'occurrence (et/ou la gravité) des risques étudiés. Mais ces principes ne peuvent être appliqués à l'étude du facteur humain, car l'Homme, qui se caractérise par son imprévisibilité et de sa capacité à innover, n'évolue pas de manière déterministe. Ainsi, la prochaine partie présente les différentes disciplines et approches utilisées pour analyser ces facteurs humains.

1.2.3 Le facteur humain

1.2.3.1 Sûreté des systèmes industriels et Comportement humain

Comme le souligne Villemeur, « l'homme a toujours été présent dans les installations industrielles, que ce soit au niveau de leur conception ou au niveau de leur exploitation » [Villemeur, 1988].

Il paraît donc naturel d'étudier le comportement humain en situation de travail, pour analyser et comprendre son influence sur la sûreté des installations industrielles.

Les premières analyses, réalisées dans le domaine de l'aéronautique, considéraient l'opérateur humain comme un composant supplémentaire du système technique, et par conséquent comme une nouvelle source d'erreur (ou de défiabilité).

Mais cette vision élémentaire et restrictive de l'homme s'est rapidement avérée inapropriée. En effet, le comportement humain ne peut se résumer à un composant élémentaire auquel est associé une probabilité de défaillance :

- Le comportement de l'opérateur est différent de celui des matériels qu'il exploite. Il est caractérisé par l'intelligence et la capacité d'innovation et d'invention, la faculté d'adaptation, et l'extrême sensibilité de certains de ses capteurs ... Comprendre et prévoir les mécanismes d'erreurs humaines [28] nécessite l'analyse approfondie des opérations mentales liées à une activité [29] et la connaissance des modèles de représentation de la réalité utilisées par l'opérateur [Villemeur, 1988].
- Les individus ne sont pas de simples applicateurs de règles (à la différence des composants techniques), ils agissent avec des intentions, avec un but, par leur engagement dans le contexte, ils se font une représentation propre du système qu'ils conduisent ... La règle n'est qu'un des éléments caractérisant le travail, d'autant plus que la grande variabilité des situations à gérer induit une adaptation permanente en temps réel [Magne et Vasseur, 2006].

L'étude du facteur humain est un des processus qui vise, à terme, l'obtention d'un optimum [30] concernant l'efficacité [31] du système considéré ([Dejours, 1995], [Millot, 1997], [Millot et Vanderhaegen, 2008]). En effet, la compréhension des décisions (et actions) de l'opérateur humain en situation de travail permet d'identifier les scénarios pouvant mener à l'occurrence d'événements indésirables, et par la suite de proposer des solutions pour réduire ces risques d'occurrence.
Ainsi, les influences du comportement humain sur la sûreté d'un système industriel peuvent être étudiées par l'une ou l'autre des disciplines du facteur humain : l'ergonomie ou la fiabilité humaine.
De manière générale, l'ergonomie consiste à étudier les interactions entre l'opérateur et le système à conduire [32], afin de pouvoir concevoir des systèmes adaptés à l'homme qui soient les plus efficaces possibles. Plus précisément, les objectifs des analyses ergonomiques sont de permettre la conception et/ou l'évaluation de situations de travail, c'est-à-dire la définition et/ou l'analyse de cadres matériels, techniques et sociaux venant en support aux activités humaines [Magne et Vasseur, 2006].
La fiabilité humaine vise, quant à elle, à évaluer et comprendre la performance humaine (individuelle et/ou collective) dans un objectif d'efficacité industrielle, et si possible quantifiable [Hollnagel, 1993].
Ces aspects sont abordés plus précisément dans les paragraphes 1.2.3.2, pour l'ergonomie, et 1.2.3.3, pour la fiabilité humaine.

28. L'erreur humaine se définie comme un écart entre le comportement de l'opérateur et ce qu'il aurait dû être, cet écart dépassant des limites d'acceptabilité dans des conditions données.

29. L'activité, qui représente le travail réel de l'opérateur, est à distinguer de la tâche, qui définit le travail prescrit par l'organisation [Dejours, 1995].

30. La notion d'optimum, utilisée dans la décision multicritère, peut se définir comme la solution la plus favorable pour un problème donné et dans un contexte particulier.

31. Selon [Desroches *et al.*, 2006], l'efficacité se définit comme l'aptitude d'une entité à répondre à une demande de service de caractéristiques quantitatives données.

32. La conduite d'un système de production est définie par [De Terssac et Dubois, 1992] comme les processus par lesquels un ensemble d'acteurs se représente un système et tente d'orienter et de conduire sa vie.

1.2.3.2 L'approche ergonomique

Si, à ses débuts, l'ergonomie portait sur l'étude des aspects physiques du travail, elle a rapidement évolué vers l'étude de l'activité cognitive de l'opérateur.
La définition actuelle, donnée par la SELF [33], la décrit comme la discipline scientifique qui vise la compréhension fondamentale des interactions entre les êtres humains et les autres composantes d'un système, et la mise en œuvre dans la conception de théories, de principes, de méthodes et de données pertinentes afin d'améliorer le bien-être des hommes et l'efficacité globale des systèmes.
Cette vision de l'ergonomie souligne, d'une part, l'importance de l'opérateur humain dans la conduite des systèmes industriels et, d'autre part, la nécessité de l'intégrer dès la phase de conception de ces systèmes.

a - La place donnée à l'opérateur humain

Pour cette discipline, l'homme est vu comme un acteur rationnel qui a certes des limites physiologiques et cognitives, mais dont l'apport essentiel à la conduite du process se concrétise grâce à sa capacité à anticiper des évolutions du process, et sa capacité d'adaptation qui permet d'optimiser la performance en réalisant des compromis, en traitant les situations non prévues à la conception, et non couvertes par les procédures.
En effet, l'homme au travail est avant tout un homme, qui outre ses savoirs initiaux, développe des compétences et des connaissances, propres au système sur lequel il agit [Magne et Vasseur, 2006].
L'ergonomie a ainsi démontré l'existence d'un écart irréductible entre l'activité réelle de travail et les descriptions normatives de ce travail (procédures, guides opératoires ...), appelé aussi travail prescrit [Dejours, 1995].
Cette dernière remarque souligne la part d'initiative requise pour que les procédures puissent être appliquées avec efficience, car la principale caractéristique de la cognition humaine est de comprendre pour pouvoir agir. Ces étapes de compréhension et d'action passent par l'acquisition d'informations en provenance de la situation observée, le traitement de ces informations, la prise de décision, et enfin les réponses physiques associées (cf. figure 1.7).

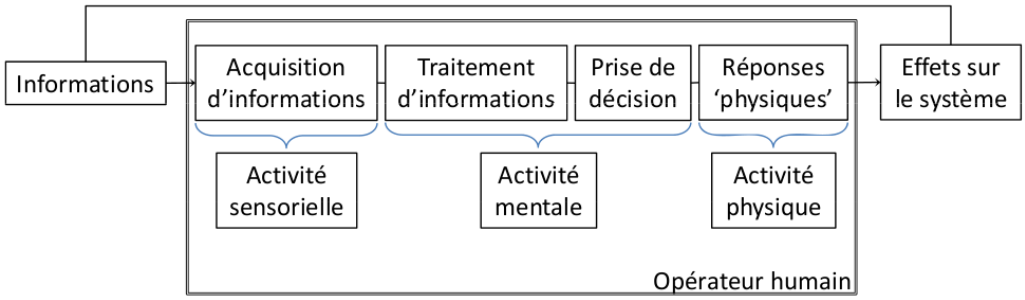

FIG. 1.7 – Représentation du fonctionnement de l'opérateur humain [Villemeur, 1988]

Ainsi, l'opérateur humain peut être vu comme une source potentielle d'erreurs [Reason, 1990] mais également comme un acteur de la performance et de la sûreté [Hollnagel *et al.*, 2006]. En ce sens, il peut être défini comme « un acteur de fiabilité faillible » [Magne et Vasseur, 2006]

33. SELF : Société d'Ergonomie de Langue Française

dont il est primordial d'étudier l'activité réelle pour pouvoir être en mesure de comprendre comment il agit et raisonne en situation.

b - La conception des dispositifs techniques

Dans [Magne et Vasseur, 2006], deux approches de conception des dispositifs techniques sont proposées. La première considère ces systèmes comme des prothèses cognitives, alors que la seconde les voit comme une aide au travail.

La conception basée sur la notion de prothèse cognitive considère le dispositif technique comme élément central de la réalisation du travail [Dejours, 1995]. Cette approche part de l'hypothèse que l'opérateur humain a des capacités de traitement de l'information limitées qui réduisent sa capacité à conduire un système complexe, et par conséquent c'est le système technique qui doit traiter cette information. L'opérateur sert alors d'intermédiaire pour fournir les données que le système ne peut obtenir par lui-même et doit agir en fonction de ce que lui demande ce système.
Ainsi, cette vision de la conception privilégie la prévention des erreurs plutôt que de permettre la gestion des imprévus.

Pour la conception en terme d'aide au travail, il s'agit de donner à des opérateurs considérés comme des acteurs compétents, la possibilité de contrôler la logique du système technique, afin de les aider à prendre des décisions et en leur laissant l'initiative pour agir.
Cette approche reconnaît la capacité des opérateurs en matière de cognition créatrice, dans le sens où ils peuvent interpréter la situation, où ils apprennent continuellement et qu'ils sont capables de s'adapter à de nombreux événements imprévus.
Ainsi cette vision de la conception a pour objectif :
- d'assister les processus décisionnels des opérateurs en augmentant leur capacité à s'adapter à de nouveaux problèmes à résoudre,
- d'intégrer l'imprévisible à la conception en faisant en sorte qu'à tout moment l'homme puisse être en capacité de maîtriser la situation.

Le dispositif technique n'est alors considéré que comme un outil qui favorise un engagement adaptatif et coopératif de l'homme au centre des décisions d'action, et l'homme garde alors un rôle actif dans la maîtrise de la situation de travail.

Ainsi en ergonomie, cette dernière approche a contribué à déplacer le champ d'investigation de l'interaction d'un acteur individuel à son poste de travail vers les équipes de travail en relation avec l'ensemble de leur situation de travail.

1.2.3.3 L'approche fiabiliste

a - L'évaluation de la fiabilité humaine

L'évaluation de la fiabilité humaine est une démarche prévisionnelle appliquée pour évaluer et comprendre la fiabilité des processus des systèmes à risques où intervient essentiellement l'homme [Magne et Vasseur, 2006]. Ce type de démarche requiert trois sources d'expertise : l'expertise de sûreté de fonctionnement, l'expertise de conception et l'expertise d'exploitation. Elle possède, en ce sens, un caractère interdisciplinaire[34], et se base sur

34. L'interdisciplinarité concerne l'étude d'un objet par plusieurs disciplines à la fois, en outre elle établit des relations entre diverses sciences ou disciplines et concerne le transfert des méthodes d'une discipline à

les modèles d'accidents proposés dans [Reason, 1997] (qui présente les niveaux individuel, « engineering », et organisationnel) et [Hollnagel, 2004] (qui décrit les modèles séquentiel, épidémiologique, et systémique).
Dans les domaines militaire et nucléaire, domaines pour lesquels ces études sont aujourd'hui régulièrement menées, il est plus courant de parler d'évaluation probabiliste de la fiabilité humaine (EPFH). En effet, cette démarche s'applique en parallèle et en complément des études probabilistes de sûreté [35] (EPS).

Une EPFH se base sur l'hypothèse que l'incohérence de l'erreur individuelle est réparée au niveau collectif [Dejours, 1995], par les systèmes redondants de récupération (matériels, procéduraux, ou organisationnels) [Magne et Vasseur, 2006]. Une EPFH doit remplir quatre objectifs :
- Identifier les actions importantes des opérateurs en conduite accidentelle et dont l'échec va à l'encontre de la sûreté de l'installation.
- Quantifier la probabilité d'échec de chacune de ces actions et les introduire dans les modèles EPS.
- Collecter les données de base à partir de l'expérience d'exploitation ou de l'observation de simulations.
- Contribuer à améliorer la sûreté en mettant en évidence le poids des échecs opérateurs selon leurs conséquences et leur probabilité d'occurrence.

Deux types de méthodes permettent de réaliser ce type d'études : les méthodes dites de « première génération », et celles dites de « deuxième génération ». Cette distinction trouve sa justification dans la manière de considérer et d'étudier le comportement humain au sein du système à conduire.

b - Les méthodes de première génération
Ces méthodes (cf. tableau 1.7) sont apparues avec les premières études des facteurs humains, et se fondent sur les deux hypothèses suivantes :
- L'ensemble du comportement de l'opérateur peut être déduit du comportement relatif à chaque sous-tâche décrite à partir de la décomposition de la tâche globale. Cette première hypothèse permet d'organiser un recueil de données statistiques.
- L'échec de l'exécution de chaque sous-tâche élémentaire est un processus stochastique dépendant de la variabilité des situations et de la variabilité des opérateurs eux-mêmes. Cette deuxième hypothèse permet d'inférer, à partir du recueil de données, la probabilité d'erreur de la tâche.

Ces approches s'appuient sur une universalité du comportement humain (*i.e.* en ne considérant pas le fonctionnement cognitif et social des opérateurs) et modélisent ainsi la défaillance humaine par une description décomposée et simplifiée de l'intervention des opérateurs. Or, cet opérateur n'a pas été « conçu » pour son métier. À la différence des matériels du système technique, ses caractéristiques fonctionnelles sont indépendantes de la conception de l'installation [Magne et Vasseur, 2006].
Cette situation oblige les concepteurs et utilisateurs de ces méthodes à revoir systématiquement la plausibilité du calcul final et éventuellement à le corriger en fonction de leur

l'autre [Lugan, 2006].

35. Une étude probabiliste de sûreté vise à identifier et évaluer un ensemble de scénarios accidentels menant à l'occurrence d'un événement redouté [Rasmussen, 1975].

expertise. L'expertise [36] induite par ces analyses prend ainsi le pas sur le calcul automatique lié aux modèles utilisés.
De plus, l'analyse du comportement humain évolue et fait apparaître la nécessité de prendre en compte la situation précise dans laquelle ce comportement est interprété ainsi que le collectif humain dans lequel il s'insère [Dejours, 1995]. C'est pourquoi, il est apparu nécessaire de développer de nouvelles méthodes permettant de considérer de façon beaucoup plus systémique les interactions entre opérateurs, procédures et interfaces [Research and Technology Organization, 2000].

Sigle	Intitulé	Référence
TRC	Time Reliability Correlation	[Hall *et al.*, 1982]
THERP	Technique for Human Error Rate Production	[Swain et Guttman, 1983]
HCR	Human Cognitive Reliability	[Hannaman *et al.*, 1984]
SHARP	Systematic Human Action Reliability Procedure	[Hannaman et Spurgin, 1984]
SLIM	Success Likelihood Index Method	[Embrey *et al.*, 1984]
HEART	Human Error Assessment and Reduction Technique	[William, 1986]
ASEP	Accident Sequence Evaluation Program	[Swain, 1987]

Tab. 1.7 – Principales méthodes EPFH de première génération

c - Les méthodes de deuxième génération
Ces méthodes (cf. tableau 1.8), enrichies par les apports des sciences humaines (notamment l'ergonomie, la psychologie, et la sociologie), rendent mieux compte de la complexité de la conduite accidentelle. En effet, elles considèrent l'évaluation de la fiabilié humaine comme l'évaluation d'une incertitude épistémologique [37] sur la conduite que tiendront les opérateurs d'un process industriel dans un contexte particulier. En ce sens, elles reconnaissent le statut central de l'analyste-expert et de l'expertise collective.

Sigle	Intitulé	Référence
ATHEANA	A Technique for Human Event ANAlysis	[Cooper *et al.*, 1996]
CREAM	Cognitive Reliability and Error Analysis Method	[Hollnagel, 1998]
MERMOS	Méthode d'Evaluation de la Réalisation des Missions Opérateurs pour la Sûreté	[Bieder *et al.*, 1998]
CESA	Commission Errors and Search Assessment	[Reer *et al.*, 2004]

Tab. 1.8 – Principales méthodes EPFH de deuxième génération

Le travail des experts consiste alors à identifier l'ensemble des scénarios d'échecs liès à la mission facteur humain étudiée. Plus précisément, il s'agit d'identifier, décrire et modéliser les conduites qui échouent, puis de quantifier l'incertitude sur l'occurrence des situations et des comportements collectifs de l'équipe expliquant chacun de ces échecs.
Les modèles génériques du comportement humain sont alors limités au minimum, et décrits

36. Le jugement d'expert n'est jusqu'alors utilisé que pour compenser l'absence de données d'entrée, car il est considéré comme exigeant en temps et en compétences, et manquant de répétabilité.

37. L'incertitude epistémologique peut être définie comme l'écart entre la représentation d'un système (i.e. sa modélisation) et sa réalité, ou comme le manque ou l'absence de connaissances concernant l'occurrence d'un événement.

de manière systémique : l'équipe est en interaction avec l'interface et les procédures, et le tout est considéré dans un contexte particulier.

Enfin, les développements actuels proposent de construire collectivement, réutiliser et mettre à jour la connaissance sur la conduite d'un système qui échoue, par le déploiement d'outils à base de connaissances tel que IDAFH [38].

Les disciplines présentées dans cette partie, l'ergonomie et la fiabilité humaine, se focalisent sur l'étude des comportements humains en situation de travail. Ce positionnement implique des analyses locales, i.e. centrées sur l'individu ou le collectif de travail.
Ainsi, du fait des objectifs de modélisation et de quantification liés à notre problématique, nous optons pour une approche fiabiliste [39] appliquée au petit collectif de travail [40].

Mais ces analyses locales s'avèrent limitantes lorsque l'on cherche à identifier les phénomènes globaux, résultants de choix managériaux, pouvant avoir une influence sur l'occurrence des événements critiques (observés au niveau technique du système). En ce sens, la partie suivante présente les disciplines et approches dédiées à l'analyse des organisations.

1.2.4 L'analyse organisationnelle

1.2.4.1 Les accidents normaux et les organisations hautement fiables

a - La Théorie de l'Accident Normal
La Théorie de l'Accident Normal (TAN), énoncée par C. Perrow dans [Perrow, 1990], considère que l'accident est lié aux propriétés techniques des systèmes hautement couplés et complexes [Marais *et al.*, 2004]. De ce fait, la structure organisationnelle n'a d'influence ni sur l'occurrence de cet accident, ni sur sa prévention ou sur son évitement. Ainsi les accidents sont inévitables même s'ils sont rares. Et c'est en ce sens qu'ils sont normaux, puisqu'ils sont un aboutissement logique de la technique (et de sa complexification).
Trois dimensions indépendantes doivent être considérées dans l'occurrence d'un accident normal : la complexité des interactions, le couplage et le potentiel de catastrophe.
La complexité des interactions représente l'ensemble des interactions possibles entre équipements, composants et/ou fonctions [Magne et Vasseur, 2006]. Ces interactions peuvent être linéaires (attendues, aisément compréhensibles) ou complexes (non prévues, non compréhensibles dans l'immédiat), en référence aux notions de basse et haute complexité proposées par E. Morin [Le Moigne, 1990].
Le couplage décrit le degré de dépendance et de flexibilité entre les différents éléments ou les différentes séquences d'un système. Ce couplage comprend des situations contraintes dans le temps et/ou des enchaînements figés, mais également des situations ayant une certaine souplesse dans l'ordre des séquences et dans les délais de réalisation.
Le potentiel de catastrophe se définit comme l'étendue théorique des conséquences d'un accident.

38. IDAFH : Intégration des Données et des Analyses de Fiabilité Humaine, [Weber *et al.*, 2005].
39. En effet, l'ergonomie ne répond pas correctement à nos objectifs car elle ne propose pas de quantification de la performance humaine.
40. La considération des comportements individuels entraîne une complexification de la représentation, et passe sous silence certaines notions importantes pour la mesure de la performance humaine (comme par exemple les notions de communication, coopération, et coordination).

Même si cette approche dégage en quelque sorte l'opérateur humain de sa responsabilité dans l'occurrence de l'accident, il ne faut pas négliger ses apports, qui sont de donner la possibilité de considérer l'opérateur autrement que comme une source d'erreurs à l'origine de l'occurrence de la majorité des événements, et de souligner que l'ajout de systèmes techniques (pour améliorer la sûreté) accroit la complexité globale du système.

b - Les Organisations Hautement Fiables
La théorie des Organisations Hautement Fiables (OHF), énoncée notamment par K. Roberts dans [Roberts, 1993], part du constat que de nombreuses entreprises à risques sont en fonctionnement et qu'il n'y a, finalement, que peu d'accidents. Cette approche se base sur l'hypothèse que la compréhension des défaillances organisationnelles est rendue possible uniquement si l'on dispose d'une meilleure connaissance des modalités de l'action collective au sein de ces systèmes à haut risque, c'est-à-dire en s'attachant à l'étude du fonctionnement normal [Magne et Vasseur, 2006].
Dans [Marais *et al.*, 2004], différentes caractéristiques des organisations démontrant un fonctionnement fiable sont proposées :
- Une priorité équivalente est donnée aux aspects liés à la sûreté et ceux liés à la performance (ou production).
- La culture de sûreté est intégrée dans toutes les phases du système, en fonctionnement normal comme en gestion de crise.
- L'utilisation du principe de l'organisation apprenante est appliqué afin de détecter rapidement un dysfonctionnement et d'optimiser le processus de retour d'expérience sur les accidents, incidents et presqu'accidents.
- La redondance, technique et/ou humaine, est largement utilisée afin de pouvoir bénéficier de processus souples pour la prise de décision (notamment en cas de situations inattendues).

Ainsi, les OHF s'appuient sur des politiques établies à un niveau centralisé, sur l'expertise acquise et maintenue de l'ensemble des acteurs pour que les actions de production n'obèrent pas la sécurité.
Cette démarche rappelle l'importance de la connaissance des propriétés réelles du fonctionnement normal des systèmes socio-techniques, à la fois comme moyen de définition des caractéristiques de résilience[41] des organisations et comme nécessité dans l'analyse d'un événement.

Ainsi, partant des caractéristiques spécifiques à chacune de ces théories (TAN et OHF), il est possible de proposer des modèles explicitant les mécanismes sous-jacents à l'occurrence d'un accident organisationnel. La définition des caractéristiques de ces modèles permet le développement de méthodes d'analyse dédiées à cette dimension du système.

1.2.4.2 Du modèle de l'accident organisationnel à son analyse

En sociologie des organisations, les premiers auteurs à s'intéresser à l'occurrence des événements (accidents, incidents ou crises) organisationnels identifient le fait que ces événements n'apparaîssent pas soudainement mais sont l'aboutissement d'une situation dégradée non (ou

41. La résilience d'une organisation est définie comme sa capacité à se reconfigurer pour absorber des variations anormales, des ruptures et une dégradation des conditions normales de travail [Seville *et al.*, 2006].

mal) identifiée par les acteurs du système étudié. Ils mettent ainsi en évidence, directement ou non, l'importance de la dimension historique dans l'occurrence de tels événements.
Selon B. Turner, l'avènement d'un accident se cristallise en six étapes : le fonctionnement théoriquement normal, la période d'incubation, l'événement déclencheur, le prélude, la récupération et la gestion de crise, le réajustement culturel complet [Turner et Pidgeon, 1997]. Ces étapes permettent de mettre en évidence la dynamique de l'événement et font apparaître qu'un accident s'inscrit souvent dans une histoire, caractérisée notamment par sa période d'incubation. Cette période décrit l'accumulation d'un ensemble d'événements non perçus et qui sont en opposition avec les croyances partagées par les acteurs du système.
Ainsi, un des apports fondamental de ce modèle est d'avoir montré qu'un accident n'est pas défini en terme technique par ses conséquences physiques mais en termes sociologiques, en tant que bouleversement ou échec important des normes et croyances culturelles existantes sur les risques et les moyens de les maîtriser [Pidgeon et O'Leary, 2000].
Pour D. Vaughan, certaines déviations dans l'organisation sont transformées, au cours du temps, en comportement acceptable et deviennent ainsi normalisés [Vaughan, 1996]. Ces déviations sont souvent mises en exergue par l'intermédiaire de signaux faibles, qui se définissent comme des informations dont la signification concernant la menace sur la sécurité d'un système n'est pas évidente [Magne et Vasseur, 2006].

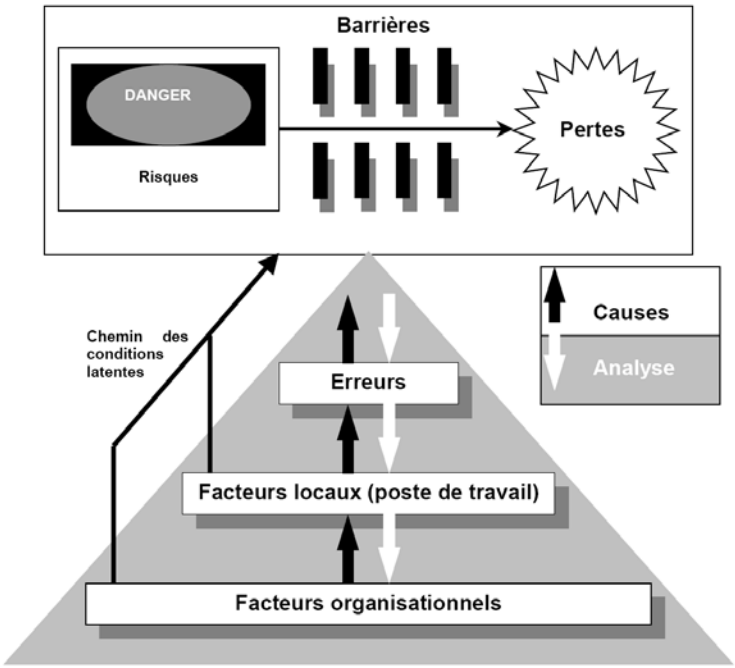

FIG. 1.8 – Représentation schématique du modèle de l'accident organisationnel selon [Reason, 1997]

Dans [Reason, 1997], l'auteur propose une représentation de l'accident organisationnel (cf. figure 1.8) qui résulte de la mise en commun des principaux éléments d'un événement (représenté par le « cheese model » [Reason, 1990]) et de l'émergence de conditions (ou défaillances) latentes [42]. Ces conditions latentes sont constituées par les erreurs (le plus

42. Une défaillance latente est une insuffisance, ou une erreur, qui intervient en amont pour favoriser ou précipiter une défaillance active (intervenant directement sur le processus technique et conduisant à l'accident) [Dien et Llory, 2008].

souvent considérées à un niveau individuel), et le contexte occasionnant ces erreurs (la situation de travail et l'organisation).

Ainsi, ce dernier modèle permet d'identifier deux autres dimensions nécessaires à la compréhension d'un événement organisationnel : les dimensions transversale et verticale [Magne et Vasseur, 2006]. Cette représentation tri-dimensionnelle (cf. figure 1.9) représente les aspects que l'analyse organisationnelle doit aborder, et s'explicite de la manière suivante :

- La dimension historique permet de remonter en amont, dans l'histoire des organisations, pour mettre en lumière les dysfonctionnements significatifs de l'evolution défavorable de la situation. Le but est de remonter dans le temps pour appréhender et analyser les dynamiques, les tendances d'évolution et les phénomènes de dégradation qui se sont manifestés pour aboutir à la situation accidentelle ou incidentelle.
- La dimension transversale, ou réseau organisationnel, est un moyen permettant de visualiser les interactions complexes et nombreuses qui sont survenues. Le réseau organisationnel souligne la complexité des relations fonctionnelles entre entités (groupes d'individus, lanceurs d'alertes ...), et dans certains cas il met à jour l'absence de certaines relations qui devraient exister.
- La dimension verticale permet de mettre en évidence et de comprendre, les interactions entre les instances hiérarchiques et d'expertise. En effet, les organisations sont des systèmes hiérarchisés [Mintzberg, 1995], où il est nécessaire d'identifier et comprendre les modes de relation, de communication, de circulation des informations et, surtout, les modes de coopération existant entre les différentes catégories de personnels (afin de ne pas focaliser les causes de l'événement uniquement sur le personnel de terrain).

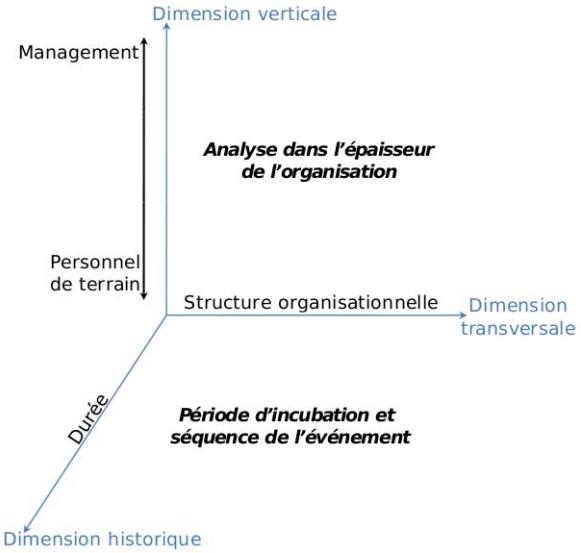

FIG. 1.9 – Axes de l'analyse organisationnelle selon [Pierlot, 2007]

Au delà de ces considérations, l'analyse organisationnelle d'un événement ne peut être traçée (pour alimenter, par exemple, un retour d'expérience) sans une représentation partagée par les experts. Cette « trace » peut être réalisée en utilisant la notion de facteur organisationnel, notion que nous allons aborder dans le paragraphe suivant, en ayant à l'esprit que ces facteurs ne peuvent se substituer à l'analyse organisationnelle de l'événement.

1.2.4.3 Les facteurs organisationnels comme support à l'analyse

Sans mentionner explicitement la notion de facteur organisationnel et en se basant sur l'analyse de quatre-vingts cinq événements, [Turner et Pidgeon, 1997] identifient huit phénomènes répétitifs impliqués dans l'occurrence de ces événements : (1) les rigidités dans la perception et (2) les croyances dans les qualités organisationnelles, (3) la mise en place de leurres pour détourner l'attention des véritables problèmes, (4) la tendance à ne pas écouter les alertes externes, (5) les défauts d'informations, (6) le non-respect des règlements existants, (7) la minimisation du danger émergent, et (8) la nature superficielle des recommandations après un accident.

Quelques années plus tard, S. Sagan définit cinq critères caractérisant les organisations à haute fiabilité [Sagan, 1993] : (1) un intérêt de haut niveau de la part des leaders (pour la fiabilité et la sûreté), (2) une redondance significative, (3) des opérations continuelles de formation et d'alerte, (4) une forte culture de fiabilité, et (5) une attention et un soin poussés vis-à-vis des crises.

Le premier auteur à utiliser le terme de facteur organisationnel est J. Reason [Reason, 1997]. Pour ce dernier, ces facteurs se situent aux niveaux supérieurs du système et engendrent les défaillances qui ont une influence sur l'aval. En d'autres termes, ils génèrent des facteurs négatifs sur les postes de travail ou favorisent l'occurrence d'actions dangereuses, et ont comme propriété d'annihiler ou d'atténuer les défenses du système considéré. Et de ce fait, les actes dangereux et les facteurs locaux de travail doivent être considérés comme étant seulement les expressions locales des problèmes organisationnels de niveaux plus élevés.
Il définit ainsi huit facteurs organisationnels, qui sont (1) la structure organisationnelle, (2) le management du personnel, (3) la fourniture et la qualité des outils et des équipements, (4) la formation et la sélection du personnel, (5) les pressions commerciales et opérationnelles, (6) la planification et la programmation, (7) la maintenance des bâtiments et des équipements et (8) la communication.

Par la suite, différents groupes de travaux ont cherché à définir (et évaluer) les facteurs organisationnels impactant la sûreté des centrales nucléaires. Citons [OCDE, 1999], qui propose douze facteurs organisationnels importants pour la sûreté : (1) les influences extérieures, (2) les buts et stratégies, (3) les fonctions et vues d'ensemble du management, (4) les allocations de ressources, (5) la gestion des ressources humaines, (6) la formation, (7) la coordination du travail, (8) la connaissance organisationnelle, (9) la procéduralisation, (10) la culture organisationnelle, (11) l'apprentissage organisationnel et (12) la communication.

Enfin, dans les cindyniques, [Kervern et Rubise, 1991], ces facteurs sont appelés des Déficits Systémiques Cyndinogènes (DSC) et sont au nombre de trois : (1) les déficits culturels (culture d'infaillibilité, culture de non-communication ...), (2) les déficits organisationnels (subordination des fonctions de gestion des risques aux fonctions de production, dilution des responsabilités ...) et (3) les déficits managériaux (absence d'un système de retour d'expérience, absence d'un programme de formation adapté ...).

Notons, comme le soulignent [Pierlot *et al.*, 2007], que la plupart de ces facteurs organisationnels se rapporte au fonctionnement normal d'une organisation à risques. À aucun

moment, la question des accidents et de leurs enseignements n'est évoquée, bien que ces facteurs caractérisent clairement la sûreté. C'est pourquoi, en se basant sur la méthaphore médicale de Reason [Reason, 1997], les auteurs proposent de s'intéresser aux éléments pathogènes de l'organisation, en d'autres termes, aux facteurs organisationnels qui ont joué un rôle dans l'occurrence d'un événement.

Pour reprendre leur propos, « pour déterminer si une organisation est en bonne santé, il est beaucoup plus simple de connaître les causes des maladies. En l'occurrence, il est beaucoup plus simple de définir pourquoi un organisme vivant est malade que de donner l'ensemble des éléments qui permettraient de caractériser pourquoi un individu, de façon générique, est en bonne santé. Notre postulat est qu'il en est de même dans les organisations à risques. Il est plus accessible de définir un ensemble de facteurs organisationnels pathogènes que de lister de manière exhaustive les facteurs organisationnels nécessaires et suffisants pour assurer un bon niveau de sûreté à une organisation ».

En ce sens, un facteur organisationnel pathogène est identifiable par ses effets divers dans l'organisation, assimilables à des marqueurs ou à des signes (ou symptômes). L'analyse de plus de vingt cas avérés a permis la définition de sept facteurs organisationnels pathogènes[43] : (1) l'insuffisance de la culture organisationnelle de sûreté, (2) la défaillance de la gestion quotidienne de la sûreté, (3) la faiblesse des organismes de contrôle, (4) le mauvais traitement de la complexité organisationnelle, (5) la difficulté à faire vivre un retour d'expérience, (6) les pressions de production et (7) l'absence de réexamen des hypothèses de conception.

Cette notion de facteurs organisationnels intéresse particulièrement notre problématique car, d'une part, elle permet de fédérer les connaissances liées à l'organisation d'un système industriel et, d'autre part, elle permet de tracer dans le temps les évolutions de cette organisation. C'est pour ces raisons que nous basons nos travaux sur ce type de représentation, et plus particulièrement sur la notion de facteurs organisationnels pathogènes (tels qu'ils sont définis dans [Pierlot *et al.*, 2007]).

Mais, avant de pouvoir présenter notre contribution, il est nécessaire d'identifier et d'étudier les travaux portant sur la problématique d'analyse intégrée des risques. Cette étude a deux objectifs : permettre l'identification des caractéristiques communes à toute démarche d'intégration et mettre en évidence les verrous actuels de cette discipline.

1.3 L'analyse intégrée des risques - Etude comparative de différentes approches

Le recul acquis sur les phénomènes accidentels a permis, durant la dernière décennie, le développement de différentes approches intégrant différents aspects des analyses de risques réalisées jusqu'alors de manière sectorielle [Zio, 2009]. Cette intégration (ou globalisation) des différentes sphères permet de se rapprocher du fonctionnement réel du système industriel étudié en donnant la possibilité à l'analyste de considérer les interactions des différentes

43. Ces facteurs seront définis plus précisément dans la suite de ce mémoire.

ressources impliquées dans les méthodologies concernées.

Sans prétendre à l'exhaustivité, cette partie présente une étude comparative de différentes approches dont l'objectif vise à intégrer, dans une même analyse, différents aspects des sphères décrites dans les parties précédentes (technique, humain, et/ou organisationnel). Nous considérerons, pour cette étude, les travaux de :

- [Paté-Cornell et Murphy, 1996] qui présentent l'approche SAM (System-Action-Management) et les résultats de l'application de cette dernière pour l'analyse de cas avérés.
- [Deleuze, 2002] qui définit les principes de l'approche GLORIA (GLObal RIsk Assessment).
- [Svedung et Rasmussen, 2002] qui démontrent, par le biais d'une représentation graphique des flux causaux des accidents (AcciMap), l'importance de considérer les influences des différents acteurs pour l'analyse de risques d'un système industriel.
- [Delmotte, 2003] qui propose un cadre socio-technique permettant d'intégrer les facteurs humains et organisationnels dans les différentes étapes de la gestion de projets et des analyses de risques.
- [Papazoglou *et al.*, 2003] qui développent une méthodologie (I-Risk) intégrant les ressources techniques et organisationnelles pour l'analyse de risques d'installations dangereuses dans le domaine de la chimie.
- [Plot, 2004] qui décrit une méthode d'évaluation des systèmes de gestion des risques majeurs en prenant en compte les facteurs techniques, organisationnels et humains (MIRIAM [44]/ATHOS [45]).
- [Chevreau *et al.*, 2006] qui démontrent comment intégrer et faciliter le processus d'apprentissage organisationnel en utilisant une modélisation des scénarios accidentels sous forme de nœuds-papillons (tels que développés dans le cadre du projet ARAMIS [46]).
- [Kim et Seong, 2006], puis [Lee *et al.*, 2008], qui proposent une nouvelle méthode probabiliste permettant d'estimer le niveau de sûreté de systèmes où l'interaction homme-machine est importante.
- [Galàn *et al.*, 2007] qui développent une approche intégrant explicitement les facteurs organisationnels dans les études probabilistes de sûreté.
- [Gregoriades et Sutcliffe, 2008] qui présentent une méthode et un outil pour analyser et prédire la charge de travail des opérateurs dès la phase de conception de systèmes socio-techniques complexes, et ce afin d'en éviter la défaillance.
- [Mohaghegh *et al.*, 2008] qui proposent de compléter les cadres de modélisation des études probabilistes de sûreté en introduisant l'effet des facteurs organisationnels.

Dans un premier temps, nous présentons les quatre critères de comparaison utilisés dans cette étude. Puis nous abordons, pour chacun de ces critères, les spécificités des démarches mentionnées ci-avant. Enfin, nous terminons cette partie par un ensemble de conclusions concernant la situation actuelle dans le domaine des analyses intégrées des risques.

44. MIRIAM : Maîtrise Integrée des Risques Industriels d'Accidents Majeurs
45. ATHOS : Analyse Technique, Humaine, et Organisationnelle de Sécurité
46. ARAMIS : Accidental Risk Assessment Methodology for Industries in the framework of SEVESO II directive, [Andersen *et al.*, 2004].

1.3.1 Présentation des critères de comparaison

Notre étude se focalise sur quatre critères : les ressources considérées, les objectifs de la méthodologie, les outils utilisés et l'applicabilité de la démarche. Définissons plus précisément ce que nous cherchons à identifier au travers de ces critères :

- Identifier les dimensions considérés dans l'analyse permet de déterminer les limites des systèmes étudiés et donc les disciplines impliquées dans la démarche, i.e. représenter les aspects techniques et/ou humains et/ou organisationnels, et analyser leurs interactions.
- Les objectifs de la méthodologie permettent de déterminer la (les) finalité(s) de l'approche développée, i.e. analyser qualitativement et/ou quantitativement les risques.
- Répertorier les outils utilisés, pour le recueil des informations et la modélisation du système, permet d'analyser comment l'information est extraite puis introduite et exploitée dans les modèles.
- L'applicabilité de la démarche vise à définir quels sont les domaines d'application d'une telle approche (i.e. générique ou pour un secteur d'activités précis, en situation pre-accidentelle ou post-accidentelle).

Ces critères sont primordiaux, pour notre problématique, afin d'identifier l'existant et les manques dans les développements actuels.

1.3.2 Critère n°1 : Dimensions

De manière générale, l'ensemble de ces travaux s'accordent sur le fait qu'il est réducteur d'étudier un risque industriel uniquement sous l'angle technique car cela revient à passer sous silence les interactions qui existent entre les différentes sphères des systèmes étudiés et leur influence sur la sûreté du système considéré.
Cependant ces approches ne proposent pas les mêmes niveaux d'intégration. En effet, certains travaux se focalisent sur l'étude des aspects techniques et humains ([Kim et Seong, 2006], [Lee *et al.*, 2008], [Gregoriades et Sutcliffe, 2008]), d'autres sur les aspects techniques et organisationnels ([Svedung et Rasmussen, 2002], [Chevreau *et al.*, 2006], [Galàn *et al.*, 2007]) et, enfin, un dernier groupe s'attache à intégrer les dimensions techniques, humaines et organisationnelles ([Paté-Cornell et Murphy, 1996], [Deleuze, 2002], [Delmotte, 2003], [Papazoglou *et al.*, 2003], [Plot, 2004], [Mohaghegh *et al.*, 2008]). En revanche, aucuns travaux ne portent sur l'intégration des aspects humains et organisationnels. En effet, la problématique qui nous intéresse porte sur l'analyse de risques liés à l'exploitation d'un système industriel. Ce positionnement implique la considération d'événements apparaîssant au niveau technique (ou physique) du système et pouvant être initiés par l'ensemble des sphères de ce système.

L'intégration des aspects techniques et humains peut être abordée différemment selon que l'analyse vise à évaluer comment l'opérateur humain interagit avec le système technique ([Kim et Seong, 2006], [Lee *et al.*, 2008]) ou qu'elle cherche à évaluer la charge de travail des opérateurs ([Gregoriades et Sutcliffe, 2008]), pour au final étudier leurs influences sur la sûreté du système.

Concernant l'intégration des aspects techniques et organisationnels, les différents travaux utilisent une représentation sous forme de scénarios (ou phénomènes) incidentels/accidentels pour représenter la dimension technique du système. La différence apparaît dans la manière de considérer l'organisation.
Ainsi, [Svedung et Rasmussen, 2002] intègrent différents niveaux organisationnels (internes et externes à l'installation étudiée) afin de pouvoir identifier les décideurs/managers de haut niveau impliqués dans la situation incidentelle/accidentelle analysée (défaillances matérielles et/ou humaines).
De manière similaire, l'approche développée par [Galàn *et al.*, 2007] considère les défaillances organisationnelles (internes à l'installation) pouvant conduire à la réalisation du scénario étudié.
Enfin, dans [Chevreau *et al.*, 2006], les auteurs se focalisent sur l'étude des notions de coopération/coordination/communication par le biais de nœuds-papillons modélisant les scénarios accidentels et montrent ainsi que ces nœuds-papillons peuvent être considérés comme des vecteurs de développement de l'apprentissage organisationnel par l'expérience.

Dans les travaux portant sur l'intégration des aspects techniques, humains et organisationnels, l'ensemble des travaux se basent sur la configuration proposée par [Paté-Cornell et Murphy, 1996]. Cette approche décompose un système industriel en trois niveaux distincts : le niveau managérial qui influence le niveau humain qui influence à son tour le système technique.
Plus précisément, pour cette méthodologie, l'opérateur humain (au travers de ses décisions et actions) est considéré comme l'intermédiaire nécessaire entre les performances du système technique et l'organisation (représentée par des facteurs organisationnels).
Les principales différences observées entre les approches se situent dans la construction du lien entre les différentes dimensions et dans les variables considérées pour représenter les aspects humains et organisationnels :

- Les travaux de [Deleuze, 2002], [Delmotte, 2003] et de [Mohaghegh *et al.*, 2008] proposent une configuration similaire à celle proposée dans [Paté-Cornell et Murphy, 1996].
- [Papazoglou *et al.*, 2003] proposent une approche articulant un modèle « technique » (comprenant déjà les aspects humains), un modèle du management (basé sur la notion de système de management de la sécurité) et une interface permettant de faire le lien entre ces deux modèles.
- Enfin, [Plot, 2004] propose une approche basée sur la modélisation de scénarios d'accidents intégrant l'influence des comportements humains et organisationnels au niveau de l'évaluation de l'efficacité des barrières de défense [47].

1.3.3 Critère n°2 : Objectifs

L'ensemble des approches étudiées cherche à expliciter les mécanismes ayant mené, ou pouvant aboutir, à l'occurrence d'un incident/accident en allant au-delà des défaillances matérielles immédiates. Certaines approches décrivent ces mécanismes uniquement de manière qualitative ([Svedung et Rasmussen, 2002], [Delmotte, 2003], [Chevreau *et al.*, 2006]) alors

47. Une barrière de défense est un élément implanté dans une installation afin de prévenir ou limiter l'occurrence d'événements critiques [Forest *et al.*, 2007].

que d'autres cherchent également à quantifier la probabilité d'occurrence des risques étudiés ([Paté-Cornell et Murphy, 1996],[Deleuze, 2002], [Papazoglou *et al.*, 2003], [Plot, 2004], [Kim et Seong, 2006], [Lee *et al.*, 2008], [Galàn *et al.*, 2007], [Gregoriades et Sutcliffe, 2008], [Mohaghegh *et al.*, 2008]).
Ainsi, au delà de la problématique commune d'analyse de risques, chacune de ces approches a des objectifs qui lui sont propres. Ce sont ces caractéristiques que nous allons à présent aborder.

Les approches qualitatives ont les spécificités suivantes :
- [Svedung et Rasmussen, 2002] proposent une approche interdisciplinaire qui cherche à structurer le système socio-technique, après l'occurrence d'un accident, pour expliciter les conditions contributrices à son développement, et qui sont fonctions des interactions des différents niveaux du système impliqué (niveaux organisationnels et phénomènes dangereux spécifiques).
- [Delmotte, 2003] développe et évalue un cadre de formalisation qui couvre toutes les étapes d'un projet et qui intègre une évaluation des risques, pour la conception de systèmes ultra-sûrs.
- [Chevreau *et al.*, 2006] montrent comment la modélisation par nœud-papillon des scénarios incidentels/accidentels peut être utilisée et adaptée pour permettre d'apprendre de ces événements et pour servir de point de départ de la boucle du retour d'expérience.

Concernant les approches quantitatives, notons tout d'abord que la plupart des données utilisées sont issues de données existantes (issues du retour d'expérience, de statistiques ...) et/ou de jugements d'experts, et qu'aucunes de ces démarches ne traite les incertitudes inhérentes aux données manipulées (facteurs humains et/ou organisationnels, et leurs interactions).
Les caractéristiques de ces approches sont les suivantes :
- [Paté-Cornell et Murphy, 1996] proposent une extension des analyses probabilistes des risques des systèmes physiques, en y introduisant une analyse des décisions et actions qui affectent les probabilités des événements de base de l'APR, et en y intègrant également une étude des facteurs organisationnels influençant ces décisions et actions.
- [Deleuze, 2002] propose une méthode de cartographie subjective des risques. Cette approche, en définissant le risque de manière stratégique (et non plus technique), permet l'analyse de la « sûreté de fonctionnement » d'une organisation (par une adaptation des analyses de risques des systèmes techniques).
- Dans [Papazoglou *et al.*, 2003], les auteurs cherchent à intégrer un modèle d'analyse quantitative des risques et un Système de Management de la Sécurité (SMS). L'intérêt d'une telle approche réside dans le fait que les causes et défaillances des opérateurs et du matériel sont directement liées à la performance du SMS.
- La méthodologie développée dans [Plot, 2004] a pour principale mission de vérifier que l'efficacité réelle des barrières de défense correspond à l'efficacité attendue et que les scénarios d'accidents sont gérés de manière acceptable (i.e. l'occurrence de l'événement redouté engendre des conséquences qui restent dans la zone d'acceptation, et ce, du fait des barrières installées dans le système).
- [Kim et Seong, 2006] cherchent à développer une nouvelle méthode pour l'évaluation quantitative de la sûreté des systèmes d'instrumentation et de contrôle faisant intervenir des opérateurs humains.
- [Lee *et al.*, 2008] proposent une méthode permettant de concevoir des systèmes (haute-

ment fiables) supports à la décision basés sur la cognition des opérateurs et de les évaluer afin de valider leur efficacité. Cette approche suppose que les systèmes supports à la décision sont une aide permettant de réduire les probabilités de défaillance des opérateurs.
- L'approche développée dans [Galàn *et al.*, 2007] vise à quantifier explicitement l'influence des facteurs organisationnels sur le taux de défaillance d'un composant spécifique (technique ou humain). En d'autres termes, cette méthode permet de calculer la probabilité qu'un opérateur ou un composant soit défaillant lors de la réalisation d'une tâche particulière, et ce, du fait d'erreurs organisationnelles.
- [Gregoriades et Sutcliffe, 2008] proposent une méthode et un outil pour estimer la charge de travail des opérateurs dès la phase de conception du système. Cette estimation se traduit par une mesure probabiliste de la performance humaine couplée à une estimation subjective de la charge de travail.
- [Mohaghegh *et al.*, 2008] proposent une approche hybride (basée sur différents outils) pour analyser les effets dynamiques des facteurs organisationnels sur le risque. Cette démarche permet ainsi d'évaluer et d'adapter les techniques de modélisation appropriées, et de construire des interfaces, pour créer une technique hybride adaptée à la problématique de l'analyse.

1.3.4 Critère n°3 : Outils

Afin de pouvoir être appliquées en milieu industriel, ces approches se basent sur des outils d'analyse, de modélisation et/ou de quantification partagés par les experts des domaines concernés.

Ainsi, la plupart des approches utilisent une représentation par graphes de type causes et/ou conséquences pour expliciter la causalité des événements techniques menant à l'occurrence de l'événement redouté et/ou celle des conséquences afférentes à cet événement. Citons, à titre d'exemple : les études probabilistes de sûreté ([Kim et Seong, 2006], [Galàn *et al.*, 2007]), les arbres des causes ([Delmotte, 2003], [Papazoglou *et al.*, 2003], [Mohaghegh *et al.*, 2008]), les arbres d'événements ([Papazoglou *et al.*, 2003], [Lee *et al.*, 2008], [Gregoriades et Sutcliffe, 2008]), les diagrammes causes-conséquences ([Svedung et Rasmussen, 2002]) et les nœuds-papillons ([Plot, 2004], [Chevreau *et al.*, 2006]).

Concernant l'élicitation et la représentation du facteur humain, les approches se basent sur les approches classiquement utilisées dans ce domaine : les enquêtes de terrain ([Paté-Cornell et Murphy, 1996]), les « Performance Shaping Factors » ([Gregoriades et Sutcliffe, 2008], [Lee *et al.*, 2008], [Mohaghegh *et al.*, 2008]), les méthodes de première génération ([Gregoriades et Sutcliffe, 2008], [Plot, 2004], [Delmotte, 2003]) et les méthodes de fiabilité humaine de deuxième génération ([Kim et Seong, 2006], [Lee *et al.*, 2008], [Plot, 2004], [Delmotte, 2003]).

La dimension organisationnelle est abordée par des analyses terrain ([Paté-Cornell et Murphy, 1996], [Chevreau *et al.*, 2006]) utilisant des protocoles d'analyse (questionnaires, tableaux ...), et représentée par des facteurs propres aux différentes analyses. Citons, à titre d'exemple, les facteurs utilisés dans [Galàn *et al.*, 2007] : la connaissances du management (comme la coordination du travail), la communication, la culture (comme

la culture de sûreté), la prise de décision (comme la centralisation) et l'allocation des ressources humaines (comme le choix du personnel).

Enfin, l'intégration de ces différents aspects se fait par l'intermédaire de composants spécifiques comme les barrières de défense ([Delmotte, 2003], [Plot, 2004], [Chevreau *et al.*, 2006]), et/ou de méthodes et outils particuliers comme les diagrammes d'influences ([Paté-Cornell et Murphy, 1996]), les réseaux bayésiens ([Kim et Seong, 2006], [Lee *et al.*, 2008], [Gregoriades et Sutcliffe, 2008], [Galàn *et al.*, 2007], [Mohaghegh *et al.*, 2008]), le raisonnement à partir de cas ([Gregoriades et Sutcliffe, 2008]), les w-factors ([Galàn *et al.*, 2007], [Mohaghegh *et al.*, 2008]), et les portes « noisy-or » ([Gregoriades et Sutcliffe, 2008], [Galàn *et al.*, 2007]).

1.3.5 Critère n°4 : Applicabilité

Un point commun peut être souligné pour l'ensemble de ces approches : elle ne peuvent s'appliquer qu'à des systèmes à haut risques ou à des scénarios critiques[48], et pour lesquels il est nécessaire de démontrer la maîtrise des risques, et/ou de concevoir des sous-systèmes ultra-sûrs.
En ce sens, nous avons identifié deux groupes de méthodologies : les démarches dédiées qui ne s'appliquent qu'à un domaine d'activité particulier, et les démarches génériques qui s'appliquent à différents types de systèmes et/ou domaines d'activités.

Ainsi, parmi les approches dédiées, certaines sont appliquables aux systèmes de production d'énergie en général ([Deleuze, 2002]) et aux centrales nucléaires en particulier ([Kim et Seong, 2006], [Galàn *et al.*, 2007], [Lee *et al.*, 2008]), d'autres à l'exploitation des chemins de fer français ([Delmotte, 2003]) et d'autres, enfin, aux installations chimiques dangereuses ([Papazoglou *et al.*, 2003]).

Les démarches développées de manière générique sont quant à elles, illustrées par une application particulière afin d'en démontrer la faisabilité :
- L'approche SAM ([Paté-Cornell et Murphy, 1996]) est ainsi appliquée à l'analyse de l'accident de Piper Alpha, puis à l'analyse de la perte de la navette Challenger et, enfin, à l'analyse des risques liés à l'anesthésie de patients en milieu hospitalier.
- [Svedung et Rasmussen, 2002] proposent une application permettant d'expliciter certains risques liés au transport de matières dangereuses.
- [Chevreau *et al.*, 2006] se focalisent sur des scénarios spécifiques à l'industrie pharmaceutique.
- [Gregoriades et Sutcliffe, 2008] analysent la charge de travail des opérateurs en salle de commande de navires militaires.
- [Mohaghegh *et al.*, 2008] expliquent leur démarche sur le système de maintenance des avions d'une compagnie aérienne.

48. En effet, ces approches sont fortement consommatrices de ressources (temps, personnel ...).

1.3.6 L'analyse intégrée des risques - Situation actuelle

Dans cette analyse, nous avons pu souligner les principales caractéristiques de travaux (récents) portant sur l'intégration des différentes sphères (techniques, humains et/ou organisationnels) au sein d'une même approche d'analyse de risques d'un système.
Ces démarches s'organisent généralement autour de trois étapes distinctes :
- La définition des dimensions des sytèmes considérés, qui permet d'identifier les méthodes d'analyse adaptées (à partir de méthodes couramment utilisées dans chacun des domaines d'expertise) pour extraire les connaissances relatives aux différentes sphères du système.
- Le développement de méthodes spécifiques pour organiser les connaissances ainsi obtenues.
- La proposition de méthodes et/ou modèles à l'interface des différentes dimensions, permettant de faire le lien entre ces connaissances de nature différentes et de propager les influences d'une sphère à une autre (généralement des dimensions organisationnelles et/ou humaines vers la dimension technique).

Mais cette intégration n'est aujourd'hui encore que partielle au sens où les démarches développées ne considèrent qu'une partie des sphères du système, et/ou qu'elles ne proposent pas la quantification des risques étudiés, et/ou qu'elles sont dédiées à un domaine d'activité particulier.
Ces limites s'expliquent principalement par la difficulté à faire communiquer des connaissances issues de disciplines différentes pour aboutir à une mesure du risque qui fasse sens.
Ainsi, pour dépasser ces limites, certains aspects doivent encore être étudiés :
- Comment traduire les connaissances, extraites à différents niveaux d'abstraction, afin de pouvoir identifier les influences de l'ensemble des dimensions du système qui pourraient mener à l'occurrence d'un événement indésirable ?
- Comment, à partir des données disponibles, quantifier les influences ainsi obtenues pour pouvoir proposer une mesure du risque pertinente ?
- Est-il possible de développer des méthodes et/ou modèles à un niveau générique, afin de pouvoir les appliquer à différents domaines d'activités ?

1.4 Conclusions

Dans ce chapitre, nous avons abordé différents aspects de la problématique de l'analyse de risques incidentels/accidentels liés à l'exploitation d'un système industriel.
Le développement de l'histoire de cette discipline a permis de définir et positionner différents concepts et approches nécessaires pour le développement de notre contribution.
Partant de la notion de risque, que nous avons définie comme l'association d'un ensemble d'événements causes et conséquences d'une situation donnée [Gouriveau, 2003], nous avons ensuite spécifié les principales étapes de son analyse (la détermination des limites du système, l'identification des dangers et l'estimation des risques).
Considérant ensuite les accidents majeurs comme vecteurs de développement, nous avons souligné l'évolution du sujet central des analyses : tout d'abord techno-centrées, elles se sont ensuite focalisées sur l'étude du facteur humain, puis sur l'analyse des causes profondes que sont les dysfonctionnements organisationnels, pour aboutir aujourd'hui au développement d'approches intégrant ces différentes sphères (pour se rapprocher du fonctionnement réel de l'installation étudiée).

Ainsi, nous avons souligné, pour chacune de ces disciplines sectorielles, les différentes approches permettant d'aborder ces analyses et celle qui semblait la plus adaptée à notre problématique :
- La dimension technique peut être étudiée au moyen de méthodes basées sur des tableaux, des graphes, et/ou des simulations. Mais l'approche graphique semble être l'approche la plus adaptée à notre problématique car elle permet de représenter et montrer l'enchaînement causal des événements menant à l'occurrence de l'événement redouté.
- La dimension humaine peut être analysée soit par une approche ergonomique, soit par une approche fiabiliste. Notre problématique s'inscrit plus dans le courant fiabiliste car il permet une quantification de l'influence de la composante humaine sur la sûreté du système, qui n'est pas développée dans le courant ergonomique.
- La dimension organisationnelle est actuellement représentée par la notion de facteurs organisationnels, notion qui permet de « tracer » l'analyse organisationnelle de cas avérés. Ces facteurs organisationnels peuvent être définis selon les principes de la théorie de l'accident normal, ou selon ceux des organisations hautement fiables.

Concernant les approches qui visent une intégration de ces différentes sphères dans une démarche globale, nous avons pu, d'une part identifier les étapes nécessaires à leur construction (la définition des dimensions des systèmes, l'organisation des connaissances, et le développement d'outils permettant de lier ces connaissances) et, d'autre part souligner le fait que cette intégration reste aujourd'hui encore partielle du fait de la difficulté à traiter conjointement des connaissances issues de sphères différentes.
Les limites actuellement rencontrées par ces approches concernent principalement les dimensions des systèmes considérés (la technique, les opérateurs, et/ou l'organisation), la quantification des variables représentatives des modèles utilisés et la généricité des principes développés.

Or, pour démontrer la maîtrise des risques d'une installation critique, il s'avère aujourd'hui nécessaire de dépasser la vision sectorielle encore ancrée dans les analyses. Ce dépassement peut être facilité en proposant des méthodologies qui :
- ne cherchent plus à responsabiliser un acteur particulier du système, mais visent à expliciter comment la conjonction de différents types d'acteurs peut mener à l'occurrence d'un événement redouté,
- proposent une quantification des risques de ces systèmes complexes, afin d'avoir une hiérarchisation claire et objective pour aider à la prise de décision,
- fournissent des méthodes, outils et modèles génériques permettant des applications dans différents domaines d'activités, afin que les résultats de ces applications puissent à terme alimenter une base de retour d'expérience.

Notre contribution porte sur l'élaboration d'une méthodologie, basée sur les principes utilisés et/ou développés dans les approches existantes (systémique, barrières de défense ...), supportant l'analyse probabiliste des risques de systèmes socio-techniques ([Duval *et al.*, 2005b], [Léger *et al.*, 2006], [Duval *et al.*, 2007]). L'objectif de notre approche est d'intégrer, de manière générique et dans un même modèle de risque, les différents niveaux d'analyse (technique, humain et organisationnel) afin d'estimer l'occurrence de scénarios de risques et l'impact de composants clés pour la prévention des risques que sont les barrières de défense.

Notre démarche s'organise, comme le montre la figure 1.10, en cinq étapes : la définition des limites du système, l'extraction des connaissances et leur unification, la construction du modèle de risque et sa représentation [Léger *et al.*, 2008c].
La définition des limites du système permet de spécifier les ressources considérées dans les systèmes étudiés ainsi que les dimensions contextuelles considérées. Il est alors possible d'identifier les méthodes adaptées pour collecter les informations de chacune des dimensions du système (extraction de la connaissance) et de proposer une représentation partagée de ces différents types de connaissances (unification de la connaissance) permettant leur aggrégation dans un modèle de risque (construction du modèle de risque). Enfin, les méthodes de quantification du modèle ainsi obtenu sont conditionnées par l'outil de modélisation utilisé (représentation, par réseaux bayésiens, du modèle de risque).
Les deux dernières étapes de la figure 1.10 permettent d'identifier les composants du système à l'interface des différentes dimensions de ce dernier (les barrières de défense), les résultats recherchés pour ces composants (l'estimation de leur efficacité et de leurs impacts sur le système), et de montrer les applications possibles de l'approche (scénarios industriels).

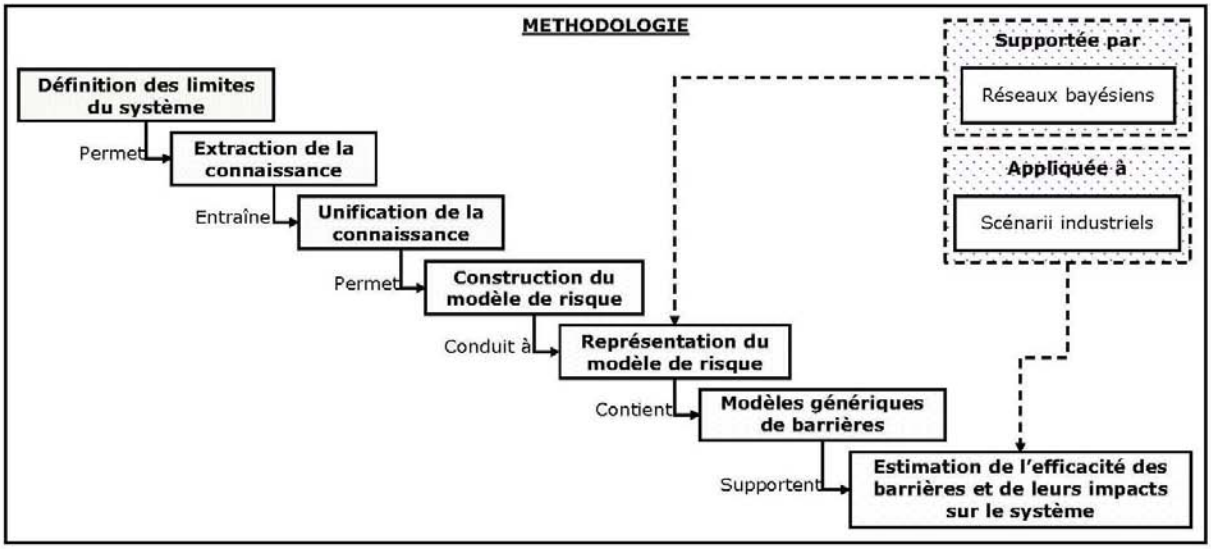

FIG. 1.10 – Étapes de la méthodologie proposée

Ces différents points sont abordés dans les chapitres suivants de ce mémoire :
- le chapitre 2 décrit les étapes liées à la construction du modèle de risque,
- le chapitre 3 développe les principes permettant de représenter ce modèle sous un formalisme probabiliste,
- le chapitre 4 présente une application de la méthodologie à un cas industriel réel. Cette application vise à démontrer la validité et la faisabilité de la démarche proposée.

Chapitre 2

Extraction de la connaissance et formalisation de l'intégration

Ce chapitre constitue la première partie de notre contribution[1]. Il porte sur le développement des phases de la méthodologie proposée (cf. partie 1.4) qui permettent de définir les objectifs de l'étude et de délimiter le cadre de l'analyse, afin de pouvoir identifier les différentes théories/méthodes à utiliser pour représenter les dimensions du système.
Les travaux présentés dans ce mémoire de thèse ont comme objectifs de proposer une méthodologie qui permette d'intégrer les résultats des approches existantes dans un même modèle de risque et non de développer de nouvelles méthodes d'analyse sectorielles.

En ce sens, la démarche que nous développons vise à offrir une vue globale du niveau de sûreté d'un système où les points faibles techniques, humains et/ou organisationnels peuvent être identifiés et pour lesquels des investigations spécifiques peuvent être menées. Ces études sont réalisées par le biais des méthodes classiquement utilisées dans le domaine concerné comme les méthodes d'analyse sectorielles citées ci-avant. En ce sens, notre approche ne se substitue pas aux méthodes d'analyse sectorielles existantes (EPS, EPFH, analyses organisationnelles ...).

Ainsi, la première partie de ce chapitre explicite, en se basant sur des travaux préalablement menés par EDF et l'INERIS, la structuration des systèmes considérés (*i.e.* les différentes dimensions de ces systèmes et les interactions considérées entre ces dimensions).

Cette étape permet d'aborder, dans la deuxième partie du chapitre, d'une part, la problématique du recueil des connaissances liées à chacun de ces niveaux d'abstraction[2] et, d'autre part, celle de l'extraction de ces connaissances dans un objectif d'intégration.

Enfin, la dernière partie du chapitre présente un ensemble de mécanismes permettant d'organiser ces connaissances et de réaliser leur intégration. Cette dernière s'effectue en deux étapes distinctes : l'intégration des aspects techniques et humains puis celle des aspects humains et organisationnels.

1. La seconde partie, qui porte sur la formalisation de la connaissance au travers d'un outil de modélisation spécifique, sera présentée dans le chapitre 3 de ce mémoire.

2. En effet, la différence des sphères considérées entraîne une approche multi points de vue, qui justifie l'utilisation de la notion de niveau d'abstraction.

2.1 Structuration du système

Au regard des observations faites dans le chapitre précédent sur les évolutions des sujets centraux des analyses de risques et sur l'état de l'art concernant la problématique des analyses de risques intégrées, le point de départ de toute démarche consiste à définir les limites des systèmes considérés. La définition de ces limites, qui se traduit par la définition des acteurs considérés dans l'analyse du système étudié, dépend des objectifs recherchés par l'analyse.
Or, la problématique de ces travaux de thèse vise à expliciter comment les interactions de l'ensemble des acteurs d'un système industriel de production peuvent influer sur l'occurrence d'un événement redouté. Cette caractéristique implique de considérer l'ensemble des acteurs des systèmes étudiés et ne peut faire l'économie de l'analyse d'une de ces ressources.
En effet, notre démarche a pour objectif d'aller au-delà de la désignation de responsables potentiels de l'occurrence d'une situation critique donnée, en donnant la possibilité de proposer des solutions à tous les niveaux du système permettant d'éviter l'occurrence d'un tel événement.
Il est par conséquent nécessaire de pouvoir identifier les fragilités des systèmes étudiés, ces fragilités pouvant apparaître autant au niveau physique, qu'au niveau des opérateurs, et/ou au niveau de l'organisation (cf. figure 2.1).

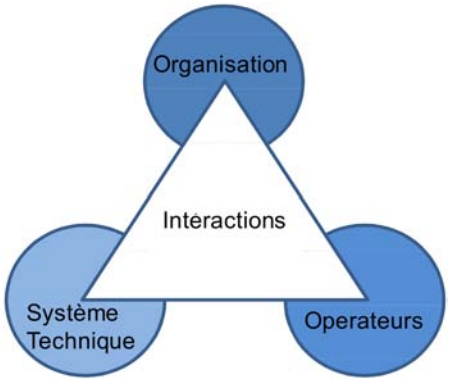

FIG. 2.1 – Définition des dimensions des systèmes étudiés

En cela, nous partageons la vision proposée dans [Paté-Cornell et Murphy, 1996] et redéfinies dans [Duval *et al.*, 2005a], qui décompose un système industriel en trois niveaux : la technique, les décisions (et actions) des opérateurs et l'organisation. Ces mêmes auteurs avancent également le fait que les influences de l'organisation sur le système technique ne sont pas directes mais se font par l'intermédiaire des opérateurs en situation de travail (et notamment par leurs décisions et actions).
De plus, [Reason, 1997] précise que les défaillances organisationnelles ont la propriété d'annihiler ou d'atténuer les défenses (prévenant l'occurrence des événements redoutés) du système considéré.

Partant de ces caractérisitiques, nous proposons de construire notre approche à partir de la définition des systèmes, décrite dans la figure 2.2.
Les dimensions contextuelles qui sont mentionnées dans cette conceptualisation permettent de positionner le système dans son environnement et de représenter les influences de ces dimensions sur les différents acteurs du système étudié.

Les dimensions retenues[3] permettent de représenter des éléments liés à l'environnement physique et/ou à l'environnement social et sociétal du système. Ces aspects sont importants dans certaines configurations de systèmes, comme par exemple :

- L'exploitation de centrales nucléaires en bord de fleuve, qui compte de nombreux sous-systèmes, dont certains dépendent fortement des changements de caractéristiques du fleuve (niveau de l'eau, flore ...) ; ces changements pouvant avoir un impact sur la sûreté de l'installation s'ils ne sont pas détectés à temps.
- La manipulation de produits chimiques dangereux en atmosphère explosive (ATEX). Ce domaine d'activité doit respecter une réglementation spécifique, la directive 1999/92/CE [Parlement européen et Conseil, 2000], imposant aux exploitants d'utiliser des matériels et composants conformes à l'environnement dans lequel ils sont implantés et de réaliser des études de dangers dédiées aux ATEX susceptibles d'apparaître dans leurs installations.

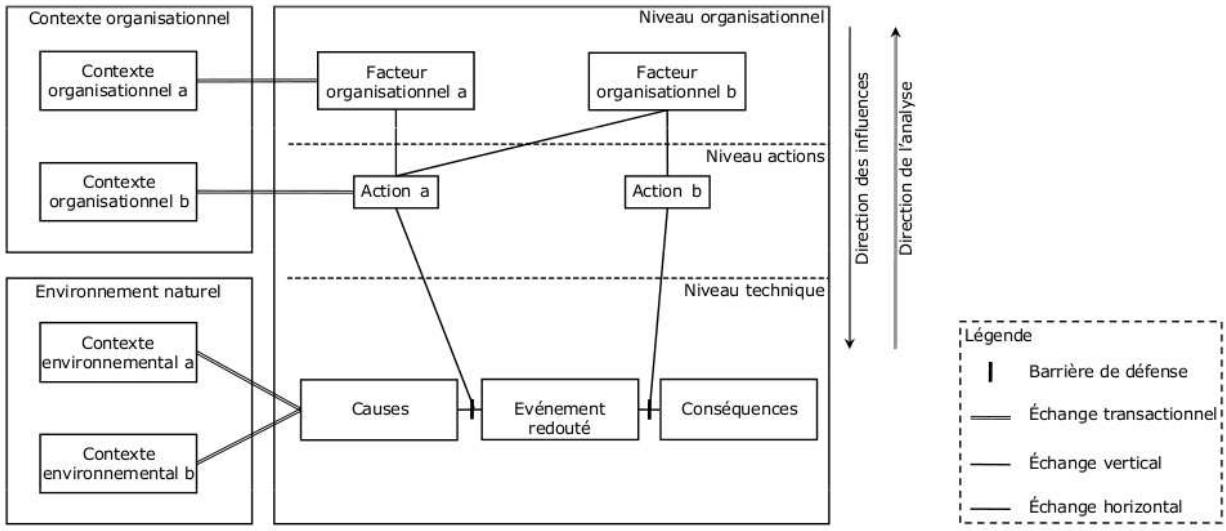

FIG. 2.2 – Définition des différents types d'interactions et des dimensions contextuelles

Ainsi le contexte environnemental permet de représenter les processus liés à l'évolution physique et climatique (comme, par exemple, des inondations, la foudre ... ou tout autre élément fonction de l'implantation géographique de l'installation) et le contexte organisationnel représente le climat social dans lequel le système évolue (comme, par exemple, les évolutions réglementaires, le niveau de concurrence ...).
La prise en compte de ces dimensions contextuelles ne complexifie pas la méthodologie dans le sens où les données relatives à l'environnement naturel peuvent généralement être obtenues par le biais de statistiques (données météorologiques). Celles relatives à l'environnement social peuvent être obtenues lors de l'étude de la dimension organisationnelle.

Ayant explicité les différentes dimensions considérées dans cette approche, il est à présent nécessaire d'identifier quelles sont les influences possibles entre ces niveaux.

3. La démarche systémique précise qu'un système se différencie de son environnement notamment par le fait qu'il est impossible d'appréhender l'ensemble des dimensions de cet environnement.

Ainsi, comme le montre la figure 2.2, trois types d'influences ont été définies d'après [Auger, 1992] :
- les échanges horizontaux qui traduisent l'influence de variables du système appartenant à une même dimension,
- les échanges verticaux qui traduisent l'influence de variables du système appartenant à des dimensions différentes (généralement deux niveaux contigus),
- les échanges transactionnels qui traduisent l'influence de variables exogènes au système (provenant des dimensions contextuelles) sur des variables du système. Ces échanges ont été définis car les variables exogènes sont subies par le système alors que ses variables internes peuvent être contrôlées.

2.2 Recueil et extraction de la connaissance

Dans cette partie, nous abordons les spécificités des méthodes utilisées pour représenter chacune des dimensions des systèmes étudiés, en les positionnant par rapport aux finalités de notre démarche. En effet, ces finalités conditionnent les aspects à étudier dans chacune des dimensions du système et justifie le fait que l'on se focalise sur certaines caractéristiques. Ces dernières sont alors utilisées pour définir les variables représentatives du comportement des différentes ressources considérées dans l'analyse.
Par conséquent, pour chaque niveau d'abstraction du système (technique, humain et organisationnel), nous présentons les objectifs de l'analyse de cette ressource pour notre approche, et le choix de la méthode permettant le recueil et la représentation de la connaissance associée.

2.2.1 La dimension technique

2.2.1.1 Objectifs

L'objectif de cette dimension est de représenter des scénarios incidentels/accidentels critiques [4] afin de pouvoir estimer les risques d'atteinte aux personnes, à l'environnement et aux biens, et de pouvoir étudier l'impact du fonctionnement des barrières de défense sur le système et sur ses performances.
Il est donc nécessaire, pour notre approche, de pouvoir identifier et représenter les causes de l'événement redouté étudié ainsi que ses conséquences. Ces particularités orientent notre choix vers une approche graphique car, comme nous l'avons explicité dans la partie 1.2.2, les méthodes utilisant une représentation graphique permettent d'identifier clairement ces enchaînements causaux. Le scénario peut alors être abordé par l'utilisation de deux approches distinctes, l'une inductive (arbres d'événements) et l'autre déductive (arbres des causes), ou par une seule approche qui combine induction et déduction (diagrammes causes-conséquences, nœuds-papillons).
Pour « simplifier » la construction de cette dimension, et donc limiter la complexité de mise en œuvre de la méthodologie, nous optons pour l'utilisation d'une approche à la fois inductive et déductive.
Trois points doivent ensuite être abordés pour pouvoir opter soit pour une approche par

4. Un scénario critique est une situation pouvant avoir des conséquences importantes en terme de gravité (impacts sur la population riveraine, pollution environnementale ...)

diagramme causes-conséquences, soit pour une approche par nœuds-papillons : la possibilité de proposer une quantification des risques étudiés, l'étude des barrières de défense impliquées dans les scénarios étudiés et l'applicabilité de la démarche.
Si l'on considère uniquement l'aspect quantification du risque, il n'est pas possible d'opter pour une représentation par diagrammes causes-conséquences ou par nœuds-papillons. En effet, ces deux approches permettent d'estimer le risque de manière quantitative. Par contre, les deux derniers points permettent d'arrêter notre choix sur l'approche par nœuds-papillons telle qu'elle est abordée dans [Andersen *et al.*, 2004]. En effet, les nœuds-papillons représentent explicitement le fonctionnement des barrières de défense et sont utilisés comme outils supports à l'implantation de la directive SEVESO II, [ISO-CEI, 2002], pour les installations classées. Leur construction est donc normalisée et générique, car devant pouvoir s'adapter à l'ensemble des domaines d'activités à risques (nucléaire, chimie, industrie pétrolière, aéronautique ...).

2.2.1.2 Recueil et représentation

La modélisation d'un scénario incidentel/accidentel par nœud-papillon, cf. figure 2.3, résulte de l'application du module MIMAH [5], puis de l'identification des barrières de défense telles que définies dans la méthodologie ARAMIS [Andersen *et al.*, 2004].
Concernant le module MIMAH, il est constitué de sept étapes : la collecte des informations auprès des agents de terrain, l'identification des équipements potentiellement dangereux de l'installation, la sélection des équipements dangereux pertinents, l'association d'événements rédoutés (ou critiques) à chaque équipement sélectionné, la construction d'un arbre de défaillances, puis d'un arbre d'événements pour chaque événement redouté, et la construction de nœuds-papillons complets pour chaque équipement sélectionné.

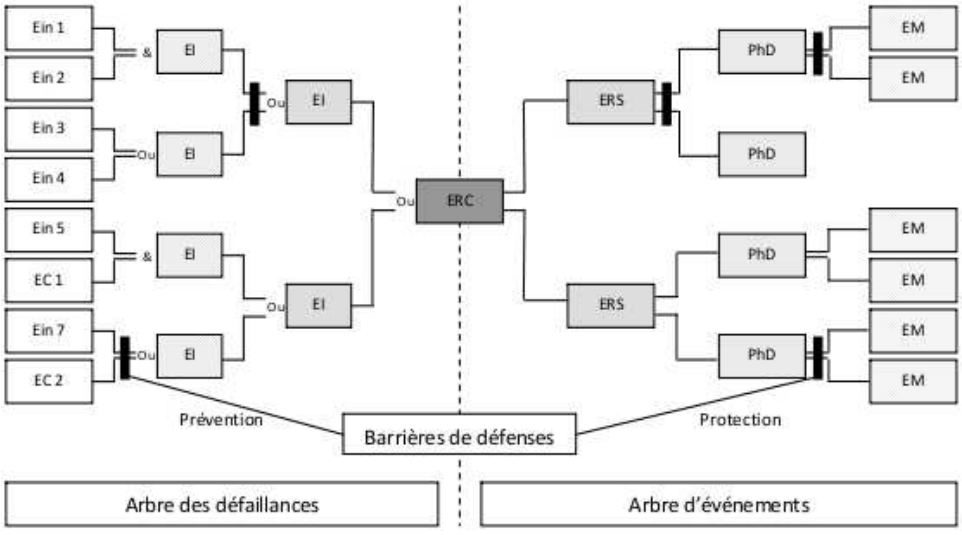

FIG. 2.3 – Nœud-papillon d'un scénario incidentel/accidentel

5. MIMAH : Methodology for the Identification of the Major Accident Hazards

Les différentes variables constitutives d'un nœud-papillon se définissent de la manière suivante :

- Les événements indésirables, **Ein** (cf. figure 2.3), sont des dérives ou défaillances sortant du cadre des conditions d'exploitation usuelles définies, comme par exemple un surremplissage de réservoir ou un départ d'incendie.
- Les événements courants, **EC**, sont des événements admis survenant de façon récurrente dans la vie d'une installation, comme la fatigue d'équipements.
- Les événements initiateurs, **EI**, sont les causes directes d'une perte de confinement ou d'intégrité physique. Ce sont des phénomènes de corrosion ou d'érosion, des agressions mécaniques, des montées en pression ...
- L'événement redouté central, **ERC**, décrit la perte de confinement sur un équipement dangereux ou la perte d'intégrité physique d'une substance dangereuse. Il se caractérise par une rupture, une brèche, une ruine, ou la décomposition d'une substance.
- Les événements redoutés secondaires, **ERS**, sont les conséquences directes de l'événement redouté central. L'événement redouté secondaire, comme par exemple la formation d'une flaque ou d'un nuage lors d'un rejet, caractérise le terme source de l'accident (ou incident, presque accident, presque incident).
- Les phénomènes dangereux, **PhD**, sont les phénomènes physiques pouvant engendrer des dommages majeurs. Ces phènomènes peuvent prendre la forme d'incendies, d'explosions, ou de dispersions de nuages toxiques.
- Les événements majeurs, **EM**, sont les dommages occasionnés au niveau des cibles (personnes, environnement ou biens) par les effets d'un phénomène dangereux. Ce sont par exemple les effets létaux ou irréversibles sur la population.

Chaque chemin définit ainsi un scénario d'accident, depuis les initiateurs jusqu'aux conséquences finales en prenant en compte le fonctionnement des barrières de défense.

2.2.1.3 Notion de barrière de défense

Une barrière de défense, dans la représentation par nœud-papillon, est une entité implémentée dans le système qui s'oppose au développement du scénario accidentel étudié. En ce sens, elle constitue un élément clé de la prévention des risques industriels.
En fonction de sa position dans le scénario, la barrière considérée peut être de nature préventive ou protective. Ainsi, une barrière de prévention se situe dans l'arbre des défaillances du nœud-papillon, et permet de prévenir ou limiter l'occurrence de l'événement redouté. Alors qu'une barrière de protection se situe dans l'arbre des événements du nœud-papillon, et permet de réduire les conséquences liées à l'occurrence de l'événement redouté [Forest *et al.*, 2007].
Ces entités se déclinent en deux groupes : les composants techniques simples et les combinaisons de composants techniques.
Un composant technique simple (ou composant de sûreté) peut être actif, s'il n'a besoin que d'une énergie mécanique pour fonctionner (comme, par exemple, une soupape de sûreté), ou passif, lorsqu'il ne nécessite aucune énergie et fonctionne de manière permanente (comme, par exemple, les bassins de rétention, les murs coupe-feu ...).
Une combinaison de composants est une entité qui doit être activée de manière externe pour pouvoir fonctionner, et se définit comme un Système Instrumenté de Sécurité (SIS).
Un SIS, selon la norme [IEC, 2004], est composé de trois phases : une phase de détection

permettant une phase de traitement puis une phase d'action. Ces différentes étapes peuvent être réalisées automatiquement par des composants techniques [Ayrault et Bouchet, 2005] et/ou manuellement par le biais d'une action humaine [Miché *et al.*, 2006] (cf. tableau 2.1 et tableau 2.2).
Ainsi dans cette approche, nous considérerons que les barrières de type composants de sûreté (CS) sont une particularisation des barrières de type SIS, du fait qu'elle ne contiennent en général qu'un seul composant.

Détection
C'est un équipement qui délivre, à partir d'une grandeur physique (température, pression, débit), une autre grandeur, souvent électrique (tension, courant, résistance), fonction de la première et directement utilisable pour la mesure ou la commande.
Traitement
Le traitement vise soit à acquérir une grandeur mesurée par un capteur et à l'indiquer, soit à activer la commande d'un ou plusieurs actionneurs à partir d'une fonction combinatoire des informations délivrées par différents capteurs.
Action
Les actionneurs (moteur, servomoteur ...) transforment un signal (électrique ou pneumatique) en phénomène physique qui permet de commander le démarrage d'une pompe, la fermeture ou l'ouverture d'une vanne ... Ils sont couplés aux éléments terminaux, qui sont commandés par un actionneur. On retrouve notamment sous cette terminologie, les vannes, les machines tournantes (pompe, compresseur ...), les alarmes sonores et visuelles. Notons que la finalité de la fonction de sécurité remplie par le SIS réside dans la détection du phénomène dangereux et dans la mise en position finale de sécurité de ces éléments (ouvert/fermé, arrêt/démarrage).

Tab. 2.1 – Définition des sous-systèmes SIS de nature technique

Détection
Il s'agit d'obtenir une ou plusieurs informations permettant d'identifier ou de détecter une défaillance ou une dérive pouvant mener à un accident majeur ou au phénomène en lui-même. La détection est souvent relayée par un système technique. L'opérateur a ainsi un rôle plus ou moins actif dans l'obtention de cette/ces information(s).
Traitement
Il s'agit de produire un diagnostic à partir de la ou des informations obtenues à l'issue de la phase précédente et de faire le choix de l'action de sécurité qui devra être réalisée.
Action
Il s'agit d'une action manuelle ou relayée par un système technique qui, sous condition de son efficacité, s'oppose au scénario d'accident majeur prévu.

Tab. 2.2 – Définition des sous-systèmes SIS de nature humaine

Partant du fait que ces barrières de défense contiennent, au moins, un composant technique, elle ne peuvent empêcher l'occurrence d'un scénario accidentel que si elles sont disponibles. La disponibilité d'un bien matériel, selon la norme [AFNOR, 2001], se définit comme son aptitude à être en état d'accomplir une fonction requise dans des conditions données, à un

instant donné ou durant un intervalle de temps donné, en supposant que la fourniture des moyens extérieurs nécessaires est assurée.

Implicitement, cette définition précise que la disponibilité est fonction de caractéristiques intrinsèques et contextuelles. Les caractéristiques intrinsèques sont propres au composant technique considéré (données constructeurs), alors que les caractéristiques contextuelles sont fonction de la situation dans laquelle se trouve ce composant (environnement physique, humain et organisationnel). Nous verrons par la suite les opportunités qu'apporte ce découplage entre caractéristiques propres et caractéristiques contextuelles [6].

Le point qui nous intéresse à présent concerne la caractérisation des aspects humains pouvant avoir une influence sur l'occurrence de situations critiques.

2.2.2 La dimension humaine

2.2.2.1 Objectifs

L'objectif de cette dimension est d'estimer l'efficacité d'actions humaines spécifiques. Il ne s'agit donc pas de caractériser l'influence des interactions homme-machine sur l'efficacité de l'action mais plutôt de qualifier l'impact de l'organisation sur les caractéristiques de l'action humaine impactant à leur tour l'efficacité de cette action. Cette spécificité implique de considérer des concepts issus plus particulièrement du domaine de la fiabilité humaine.
La fiabilité humaine porte sur l'analyse et l'impact des opérateurs sur la fiabilité et la sûreté des systèmes [Hollnagel, 1993], en considérant les actions humaines non seulement comme source d'erreurs [Reason, 1990], mais également comme source de performance [Hollnagel *et al.*, 2006].
Cette caractéristique implique une extension des analyses classiques de la tâche humaine vers l'analyse de scénarios de travail plus larges [Research and Technology Organization, 2000]. Cette extension est réalisée en se focalisant sur les comportements collectifs qui peuvent être vus comme une aggrégation des différents comportements individuels agissant ensemble pour l'efficacité de la mission.
Ainsi, les développements que nous proposons (variables représentatives, méthodes de quantification) considèrent l'action du point de vue du collectif de travail et cherchent à quantifier l'influence de ce collectif sur la disponibilité des composants constitutifs des barrières de défense.
Ce positionnement implique des spécificités concernant l'analyse et la représentation de cette dimension, qui sont abordées dans la partie suivante.

2.2.2.2 Recueil et représentation

En étudiant le fonctionnement des systèmes, il peut être observé que la disponibilité des composants techniques est influencée par différents types d'actions humaines.
Ces actions sont regroupées en deux catégories : les actions de maintenance et les actions de conduite.
La maintenance est définie, dans la norme [AFNOR, 2001], comme la combinaison de

6. Ce découpage est notamment abordé pour la fiabilité des systèmes, dans [Despujols, 2004b], afin de montrer que les interventions préventives de maintenance transforment la fiabilité intrinsèque en une fiabilité opérationnelle.

l'ensemble de toutes les actions techniques, administratives et de management durant le cycle de vie d'un bien, destinées à le maintenir ou à le rétablir dans un état dans lequel il peut accomplir la fonction requise. Selon A. Despujols dans [Magne et Vasseur, 2006], la maintenance est un ensemble d'activités coordonnées qui participent à la gestion des risques industriels, notamment en contribuant à leur appréciation et à leur traitement.
Ces mêmes auteurs proposent une typologie de ces actions, typologie qui est présentée dans l'annexe A de ce mémoire.

Une action de conduite est un processus qui permet, toujours selon A. Despujols, le maintien d'une installation en conditions opérationnelles. Citons à titre d'exemple, les tâches de surveillance, de diagnostic, de limitation des contraintes de fonctionnement ou d'approvisionnement en matières consommables.

Pour décrire les spécificités de ces actions humaines, une étude comparative des méthodes utilisées à EDF (dans les études probabilistes de sûreté sur le risque Incendie) et à l'INERIS (dans l'approche MIRIAM-ATHOS) par les experts du facteur humain, cf. annexe B, a été menée. Cette étude a conduit à la définition de caractéristiques de telles actions humaines, que nous nommons « items ».

Certains de ces items sont relatifs aux caractéristiques du collectif :

- La Délégation (**De**) qui est le fait de remettre la responsabilité d'une tâche à une autre personne, généralement un subordonné. Cette délégation peut être mise en place par l'organisation (délégation formalisée) ou non (délégation ponctuelle, informelle). L'hypothèse sous-jacente consiste à considérer que cette personne (à qui l'on a délégué la responsabilité de la tâche) est compétente pour réaliser cette tâche. Notre définition ne porte pas sur le jugement de la décision prise (Est-ce que le décideur a effectué une bonne délégation ?) mais sur les compétences de la personne en charge de l'action.

- L'Expérience (**Ex**) qui se définit comme la connaissance acquise par la pratique accompagnée d'une réflexion sur cette pratique, ce qu'Henri Fayol exprimait en écrivant : l'expérience, « c'est le souvenir des leçons qu'on a soi-même tiré des faits » [Fayol, 1999].

- La Formation (**Fo**) qui est vue comme l'ensemble des activités (mises en place par l'entreprise) visant à assurer l'acquisition des capacités pratiques, des connaissances et des attitudes requises pour occuper un emploi (et donc s'assurer de l'aptitude des opérateurs à réaliser les actions).

- La Gestion Collective et Dynamique de Groupe (**Gcdg**) qui est composée de régles (formelles et informelles) et des techniques de travail utilisées par le collectif pour atteindre les objectifs. Cet item peut également être défini comme la capacité du collectif à s'adapter à une situation spécifique et à compenser une dérive potentielle. Cet item regroupe les notions de régulation conjointe[7], de la gestion collective de l'action[8], la

7. Notion définie dans [Reynaud, 1997], comme le fruit de conflits aboutissant à un compromis entre la régulation autonome et la régulation de contrôle. C'est un mode de formation de règles. Elle peut être vue comme l'ensemble des règles effectives au moment de réaliser l'action.

8. Elle identifie les actions mises en œuvre par le collectif de travail pour atteindre/réaliser les objectifs.

reconfiguration en intervention [9], le métier [10] et la concurrence des différents objectifs [11].

D'autres items sont spécifiques aux outils et procédures utilisés par ce collectif pour accomplir leurs actions :

- Les Aides (**Ai**) qui sont l'ensemble des procédures, outils et moyens (prise de décision ...) utilisés par le collectif en support à leur activité (pour atteindre les objectifs). La procédure est définie comme l'ensemble des documents opératoires prescriptifs (obligatoires comme les consignes, les gammes d'essais ...) et non prescriptifs (non obligatoires) utilisés par les opérateurs en support à leur activité. Les outils se définissent comme l'ensemble des autres documents (modes d'emploi ...) et appareillages venant également en support à l'activité des opérateurs.

- La (possibilité de) Respect du cahier des charges (**Rcc**). Le cahier des charges contient les informations sur le système, les objectifs à atteindre et les moyens permettant d'atteindre ces objectifs. L'atteinte de ces objectifs est possible si les informations ont été correctement définies et que les objectifs sont réalisables/atteignables. On suppose que le cahier des charges est correct (*i.e.* les informations concernant le système, les objectifs à atteindre et les moyens permettant d'atteindre ces objectifs sont correctement définis et réalisables). Pour le caractériser, on se posera la question de savoir si le collectif peut toujours l'appliquer, s'il est toujours appliqué.

- Le Contrôle et l'atteinte des objectifs (**Cao**), définis par les contrôles (évaluation de la conformité du résultat attendu par rapport au résultat réel, en considérant les moyens mis en œuvre pour atteindre ce résultat, comme par exemple le suivi des procédures ...) et l'atteinte des objectifs (moyens mis en œuvre pour juger de la visibilité des résultats d'une action, sans considérer ceux utilisés pour atteindre ce résultat).

- Le Retour d'expérience (**Rex**). Le retour d'expérience est une démarche structurée de capitalisation et d'exploitation des informations issues de l'analyse d'événements positifs et/ou négatifs. Elle met en œuvre un ensemble de ressources humaines et technologiques qui doivent être managées pour contribuer à réduire les répétitions d'erreurs et à favoriser certaines pratiques performantes.

La dernière variable :
- Les Facteurs contextuels (**Fc**), représente les éléments externes influençant le collectif durant la réalisation de cette action, *i.e.* sur lesquels on a peu de prise. Citons par exemple, les conditions de travail, les autres actions en cours, un local enfumé, l'éclairage ...

La définition de ces caractéristiques des actions humaines entraîne certaines observations

9. Elle se définit par le changement de stratégie de conduite de l'action durant sa réalisation (du fait de son caractère déviant). Cette reconfiguration peut aboutir à l'élaboration d'une nouvelle règle à suivre pour la prochaine réalisation de cette action.

10. C'est l'ensemble des connaissances partagées de manière collective pour une activité donnée ainsi que les moyens mis en œuvre pour transmettre ces connaissances.

11. Elle se caractérise par le fait de privilégier un ou plusieurs objectifs (sûreté, disponibilité, maintien du patrimoine) au dépend des autres.

qu'il est nécessaire de formuler :
- L'état de ces items spécifique à chaque action étudiée, ou leur efficacité, est identifié par le biais d'analyses d'activités.
- L'ensemble de cette caractérisation vise une exhaustivité de représentation. En ce sens, elle peut être adaptée pour des contextes particuliers, *i.e.* il est possible d'ajouter ou de retirer certaines caractéristiques.
- L'état de ces items dépend du climat organisationnel dans lequel les opérateurs évoluent. C'est pourquoi il est nécessaire de définir comment étudier et représenter cette dimension.

2.2.3 La dimension organisationnelle

2.2.3.1 Objectifs

L'objectif de cette dimension est de représenter les caractéristiques de l'organisation pouvant impacter les actions des opérateurs (la maintenance ou la conduite) et contribuer à l'occurrence d'une situation incidentelle/accidentelle.
Les travaux présentés dans la partie 1.2.4.3 énoncent différentes manières de représenter ces caractéristiques organisationnelles. Mais l'analyse des accidents et leurs enseignements ne sont souvent pas considérés dans la construction de ces représentations. Or, une telle approche permet de construire une représentation proche de la réalité des observations faites sur le terrain car elle se base sur l'analyse d'un ensemble d'événements avérés.
Ainsi, partageant la vision de [Pierlot *et al.*, 2007] sur le fait qu'il est plus aisé de définir un ensemble de facteurs organisationnels pathogènes que de « lister de manière exhaustive les facteurs organisationnels nécessaires et suffisants pour assurer un bon niveau de sûreté à une organisation », nous proposons de considérer la représentation par facteurs organisationnels pathogènes pour définir la dimension organisationnelle des systèmes considérés dans notre approche.

2.2.3.2 Recueil et représentation

Lors de l'analyse organisationnelle d'une situation particulière, l'identification des facteurs organisationnels pathogènes (FOP) suit la logique décrite dans la figure 2.4.

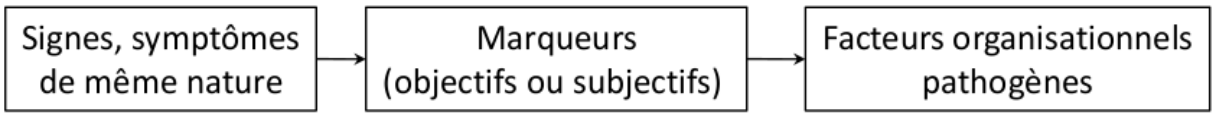

FIG. 2.4 – Identification des marqueurs et facteurs d'une situation donnée

Ainsi, pour chaque FOP, l'expert cherche à identifier les marqueurs caractéristiques de ce facteur par le biais de signes et symptômes qui sont eux-mêmes spécifiques à ces marqueurs.

Les marqueurs peuvent être objectifs, lorsqu'ils relèvent d'une approche explicative ou causaliste, ou subjectifs, lorsqu'ils relèvent d'une approche compréhensive (par entretien).

L'hypothèse de départ, énoncée par les experts organisationnels utilisant la représentation par FOP, consiste à considérer que si aucun FOP n'est présent à la suite de l'analyse, alors il est possible d'annoncer que la situation analysée est sûre ; par contre si certains de ces

facteurs sont présents alors la sûreté de l'installation peut être dégradée [12].

Sept facteurs organisationnels ont ainsi été définis par [Dien *et al.*, 2006] : la faiblesse de la culture organisationnelle de sûreté, la défaillance dans la gestion quotidienne de la sûreté, la faiblesse des organismes de contrôle, le mauvais traitement de la complexité organisationnelle, la difficulté à faire vivre un retour d'expérience, les pressions de production et l'absence de réexamen des hypothèses de conception.
Définissons à présent chacun de ces facteurs organisationnels pathogènes :

– Faiblesse de la culture organisationnelle de sûreté (**COS**)
  La culture organisationnelle de sûreté est un ensemble de connaissances, de pratiques et de valeurs partagées et soutenues de façon volontaire par l'ensemble des membres de l'organisation. Elle vise à assurer que la sûreté des installations bénéficie à tout moment (et en toute circonstance) de toute l'attention requise dans l'atteinte des objectifs de production. Une culture de sûreté peut être jugée insuffisante lorsque l'on constate un manque de moyens et de compétences dédiés à cette priorité, et/ou défaillante lorsque l'on constate un divorce entre les pratiques de sûreté et les valeurs officiellement prônées dans les discours (notamment ceux du management du site).
  Un exemple de marqueurs, signes et symptômes spécifiques à ce facteur [13] est fourni dans le tableau 2.3.

Marqueur : Signes et symptômes associés
Formation insuffisante du personnel à la sécurité : - Phénomènes dangereux négligés dans la formation - Absence ou insuffisance d'indications des vulnérabilités graves
Analyses de risques insuffisantes ou inexistantes : - Analyses non effectuées, retardées, incomplètes, falsifiées, erronées - Points de vulnérabilité majeurs laissés en suspens sur le plan de l'analyse de risques
Documentation concernant la sûreté insuffisante : - Documentation lacunaire - Documentation trop complexe et difficilement exploitable

Tab. 2.3 – Exemple de marqueurs, signes et symptômes pour le facteur COS

– Défaillance dans la gestion quotidienne de la sûreté (**GQS**)
  La gestion quotidienne de la sûreté concerne la mise en œuvre pratique des exigences de sûreté au sein de l'organisation. Elle vise en particulier à assurer une bonne adéquation entre tâches à accomplir et compétences des personnels, à fournir une formation adaptée aux personnels, à s'assurer de la transmission des savoir-faire de sûreté tout au long des parcours professionnels, y compris pour la sous-traitance.
  Cette gestion peut être jugée insuffisante lorsque les moyens et les ressources alloués sont faibles, compte-tenu des tâches à accomplir, ou déficiente lorsqu'en dépit des moyens et des ressources alloués, les objectifs ne sont pas atteints faute d'une appréciation correcte des besoins et des tâches.

12. C'est alors à l'analyste d'évaluer l'état de la situation (caractère plus ou moins dégradé) en tenant compte du ressenti des acteurs.
13. Les autres facteurs sont abordés en annexe C de ce mémoire.

– Faiblesse des organismes de contrôle (**OC**)
Les organismes de contrôle permettent de vérifier que les opérateurs respectent les obligations de sûreté. Il y a plusieurs types d'organismes de contrôles : ils peuvent être internes ou externes à l'installation. La faiblesse des autorités de contrôle renvoie à la position occupée par les membres de ces services, corps d'inspection ou instances dans le jeu d'acteurs. La défaillance des autorités de contrôle renvoie à des activités qu'elles sont censées réaliser et qui ne le sont pas, ou qui ne l'ont pas été, ou encore dont le soin dans l'analyse et le suivi laisse à désirer.

– Mauvais traitement de la complexité organisationnelle (**MT**)
La complexité organisationnelle se réfère aux dispositions qui compliquent les relations de travail et les décisions ainsi que les communications portant sur les risques et la sûreté. Cette complexité organisationnelle peut avoir plusieurs origines. Elle est liée à la complexité technologique, à l'émergence irrésistible de cloisonnements et à la multiplication des parties prenantes rendant la coordination inter-organisationnelle très délicate. Une organisation complexe et inadaptée se traduit par au moins deux phénomènes observables : une communication organisationnelle qui fait défaut et une coordination défaillante. La communication organisationnelle défaillante renvoie à des situations ou la transmission d'éléments importants pour le travail de chacun (nouvelle directive, nouvelle organisation ...) n'est pas faite ou est faite mais de manière incomplète. La coordination défaillante renvoie à l'ensemble des travers couramment en place dans les organisations (bureaucratisation, lutte entre bureaux, cloisonnement, baronnies, isolement) et à leur non prise en compte explicite dans l'organisation.

– Difficulté à faire vivre un retour d'expérience (**REX**)
Le retour d'expérience événementiel est un processus itératif et dynamique qui consiste à recueillir et analyser dans l'activité les dysfonctionnements qui ont pu survenir, et ce, afin d'être en mesure de prévenir l'occurrence de nouveaux incidents et accidents. La faiblesse du retour d'expérience concerne à minima deux cas : un premier cas où le processus de retour d'expérience est complet mais trop peu de moyens et de ressources y sont associés ; un second cas lorsque là encore le processus est complet mais qu'il n'est pas porté dans l'organisation, en particulier lorsque les résultats des analyses ne diffusent pas dans l'ensemble de l'organisation. L'insuffisance du retour d'expérience apparaît lorsque le processus de retour d'expérience est incomplet, *i.e.* plusieurs phases de ce processus manquent. Le manque de profondeur de l'analyse se traduit par des mesures correctives inefficaces ou superficielles, qui ne permettent pas d'enrayer les dysfonctionnements à traiter.

– Pressions de production (**PP**)
Sont considérées pressions de production, des injonctions visant à passer outre ou à volontairement ignorer certaines dimensions de la sûreté, de manière à favoriser les critères de rentabilité à court terme. Les pressions de production apparaissent lorsque les activités de production ne sont plus contrebalancées par la culture de sûreté. Il s'agit de toutes les pressions de production rencontrées par les membres de l'organisation en cause, au détriment de la sûreté.

– Absence de réexamen des hypothèses de conception (**AR**)
La conception de tout système technologique s'appuie sur la définition et sur la prise

en compte d'hypothèses de dimensionnement (technique et social). Ces hypothèses sont basées sur une vision du fonctionnement futur du système. Il peut s'avérer, avec le temps, que certaines hypothèses deviennent caduques, *i.e.* inadaptées aux caractéristiques du nouveau mode de fonctionnement nominal, ou se révèlent fausses compte-tenu des caractéristiques réelles du mode de fonctionnement. On considère qu'il y a présence de ce facteur organisationnel pathogène lorsque l'obsolescence ou le caractère erroné d'une hypothèse de conception n'a pas été détecté.

Cette approche, focalisée sur l'influence négative de l'organisation, pourra être complétée par des experts de cette discipline, d'une part, en définissant d'autres facteurs pathogènes et, d'autre part, en considérant un ensemble de facteurs résilients permettant de représenter les influences positives d'une organisation (pouvant alors contrer l'effet de ces facteurs pathogènes). Mais la définition de tels facteurs génériques nécessite l'analyse de nombreuses autres situations incidentelles/accidentelles. C'est pourquoi nous considérerons ces sept facteurs comme étant une représentation suffisante pour notre problématique, qui pourra être complétée par la suite et particularisée pour chaque situation analysée.

2.3 Formalisation des mécanismes de structuration et d'intégration des connaissances

Cette partie vise à définir, à partir des représentations proposées précédemment, les démarches de structuration et d'intégration des connaissances des différentes dimensions du système. Nous présentons tout d'abord les concepts de base (valables pour l'ensemble du système), puis nous nous focalisons sur les intégrations spécifiques du système : l'intégration des dimensions technique et humaine et l'intégration des dimensions humaine et organisationnelle.

2.3.1 Les concepts de base

Les notions abordées dans cette partie portent sur l'intérêt et la justification d'une approche à la fois ascendante et descendante, la définition des spécificités des processus de changements (d'état) pour les composants du système technique et les actions humaines et l'organisation des analyses sur le terrain (constitution des équipes, personnes à interviewer ...).

2.3.1.1 Approche ascendante ou approche descendante ?

Les interactions présentes dans le fonctionnement réel d'un système socio-technique sont à la fois ascendantes et descendantes. En effet, certaines informations en provenance du terrain (système technique, opérateur en situation de travail) sont remontées vers les instances organisationnelles alors que d'autres cheminent dans le sens opposé. Les premières concernent, par exemple, le fait que certains composants de l'installation ont des dysfonctionnements récurrents qu'il est nécessaire d'analyser, alors que les secondes portent, par exemple, sur les règles instaurées par le département sécurité du site concernant le port des EPI [14] (matériel à utiliser, zones à respecter ...).

14. EPI : Equipement de Protection Individuel

Les démarches d'analyse intégrée des risques, abordées dans la partie 1.3, utilisent ces interactions (ascendantes et descendantes) pour expliciter les causes d'un événement et/ou proposer des solutions adaptées à la situation analysée. Cette configuration est explicitée dans [Paté-Cornell et Murphy, 1996] selon la figure 2.5.

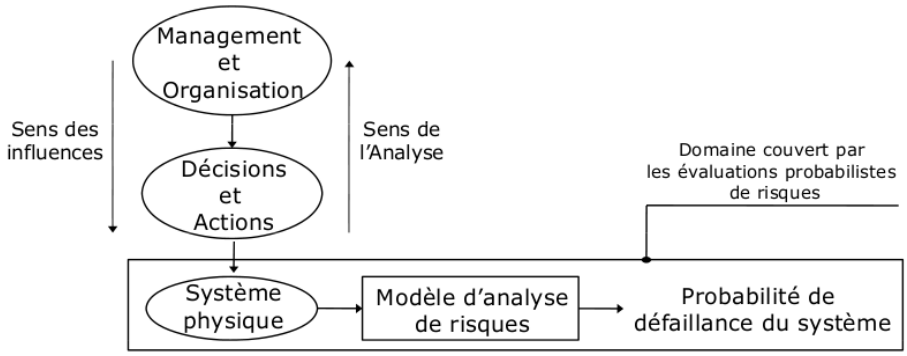

FIG. 2.5 – Structure des effets des opérateurs et du management sur le risque

Ainsi, alors que la direction des influences décisionnelles va du management, aux opérateurs humains, puis au système technique, la méthode d'analyse développée dans [Paté-Cornell et Murphy, 1996] fonctionne dans le sens opposé. Cette analyse ascendante est utilisée pour développer des recommandations descendantes pour les stratégies du management visant à réduire les risques de défaillances du système.

Cette dernière remarque souligne l'intérêt, pour notre démarche d'intégration, de combiner approche ascendante (pour la construction de la représentation du système étudié) et approche descendante (pour la proposition d'un ensemble de solutions, à la fois techniques, humaines et organisationnelles).

Mais, la validité des modèles et solutions proposés par ces approches est conditionnée par la connaissance de l'état courant du système analysé. Cet état courant, qui peut être un état stable ou un état transitoire, est fonction des processus de changement considérés comme étant actifs au moment des observations faites sur le système.

2.3.1.2 Le processus de changement ...

a - ... relatif au système technique

Un changement d'état, selon [Vogel, 1988], se caractérise par le fait que le destinateur (les opérateurs humains pour notre problématique) oriente son action vers le changement d'état du destinataire (le composant technique) et prend donc temporairement le contrôle de celui-ci. Ce contrôle du destinateur correspond à un contact physique entre destinataire et destinateur (cf. figure 2.6). « L'instrument est souvent le support explicite de ce contact, et c'est à travers ce contact qu'il fournit l'énergie nécessaire à la transformation du destinataire par le destinateur ». L'instrument est qualifié et quantifié, et « le concours qu'il prête à la transformation entraîne généralement une consommation perceptible de la ressource qu'il représente ».

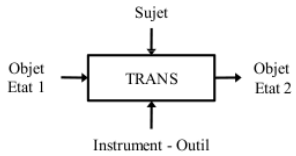

FIG. 2.6 – Représentation de l'actème, selon [Vogel, 1988]

Ainsi, pour notre approche, cette caractéristique permet d'avancer :
- qu'à chaque action humaine est associée un composant spécifique du système technique étudié qu'il est nécessaire d'identifier clairement,
- que le contact entre ce composant technique et l'action humaine se fait au travers des caractéristiques de l'action (qui incluent notamment les outils supports à l'activité des opérateurs).

Par conséquent, dans notre approche nous faisons l'hypothèse qu'une action humaine ne peut impacter directement un phénomène physique, comme par exemple l'explosion d'un réservoir. Il faut d'abord représenter l'état (et plus particulièrement la disponibilité, cf. partie 2.2.1.3) du composant technique (le réservoir dans notre exemple), pour pouvoir introduire les influences de l'action humaine considérée (cf. figure 2.7). L'occurrence du phénomène physique est alors directement impactée par l'état du composant technique associé.

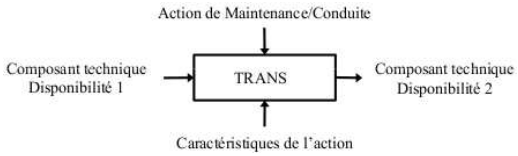

FIG. 2.7 – Processus de changement d'état d'un composant pour notre problématique

b - ... relatif aux actions humaines

Une action humaine peut être vue comme un processus de changement organisationnel mais appliqué à un niveau local. Le changement organisationnel est défini par [Siebenborn, 2005] comme le passage d'un état (stable) de l'organisation à un autre état (stable). Ce processus, habituellement abordé sur un intervalle de temps défini, doit être discrétisé en un ensemble de phases (réparties sur cet axe temporel) pour pouvoir être analysé.
Différents travaux portant sur cette problématique peuvent être cités.
- [Lewin, 1951] propose un modèle en trois étapes, Dégel - Mouvement - Regel, traduisant le fait qu'une organisation doit être portée hors de ses valeurs et de son mode de fonctionnement courant, puis être changée, et enfin replacée sur de nouvelles valeurs et un nouveau mode de fonctionnement [Siebenborn, 2005].
- [Vogel, 1988] propose un découpage du concept de séquence[15] en trois phases, Ouverture - Noyau - Clôture. L'ouverture de la séquence consiste à la préparation de l'objet qui va être destinataire du noyau, permettant la réalisation des événements des transformations. La clôture restaure un état final stable, libère les ressources utilisées et réinsère dans l'environnement les protagonistes des actèmes (cf. figure 2.6).

15. La séquence constitue la trame de l'actinomie (qui est une représentation, une combinaison d'images mentales orientant et organisant l'action).

– [Siebenborn, 2005] propose une formalisation en trois phases, Préparation - Action - Mise au point/stabilisation, s'inspirant d'observations faites sur le terrain. Cette représentation est utilisée, selon l'auteur, pour souligner l'importance de la phase de préparation dans un projet de changement et le fait que négliger cette phase entraîne une phase de stabilisation plus longue.

Enfin, en reprenant les propos de [Siebenborn, 2005], les différents découpages « se rejoignent sur l'idée d'un premier temps dédié à la projection intellectuelle du changement, un second dédié à la mise en œuvre concrète d'un ensemble d'actions de changement et, enfin, un dernier temps dédié à la stabilisation du nouveau système. Ces trois temps distinctifs de la démarche laissent entrevoir la possibilité de découper tout acte de changement en trois phases relativement homogènes. Le caractère générique de ce découpage permet en outre une appréhension reproductible et organisée de l'acte de changement par nature unique et complexe dans son contexte comme dans son déroulement ».

Nous proposons donc d'adapter la formalisation de [Siebenborn, 2005] à notre problématique. Cette adaptation passe par l'étude des pratiques courantes concernant le déroulement des actions de maintenance et de conduite.
Les différentes références étudiées ([Méchin, 2000], [AFNOR, 2002], [Despujols, 2004a]) proposent trois étapes essentielles au déroulement d'une action de maintenance : la préparation (qui peut être formalisée ou non en fonction de la complexité de l'action à réaliser), la réalisation et la clôture, découpage que nous supposons applicable également pour les actions de conduite au regard des observations faites sur le terrain [16].

Ainsi nous proposons de structurer les actions humaines selon la représentation proposée dans la figure 2.8 et de définir les différentes phases d'une action humaine de la manière suivante :

– La préparation permet l'organisation, la spécification et la caractérisation de toutes les conditions nécessaires à la bonne exécution de l'intervention (par le collectif de travail). Elle permet de choisir les moyens les mieux adaptés aux différentes exigences de coûts et de délais.
– La réalisation permet d'implémenter l'intervention dans le fonctionnement du système par la mise en œuvre des moyens et leur coordination.
– La clôture permet d'assurer la bonne intégration de l'intervention dans le système et de confirmer sa continuité. Elle se décompose en différentes sous-étapes qui sont le contrôle des travaux, la réception des travaux, l'analyse des informations collectées en cours et en fin de travaux et le retour d'expérience.

Ces phases concourent toutes, en se positionnant au niveau du collectif de travail, à l'efficacité de l'action humaine étudiée.

16. Si l'on prend l'exemple du remplissage d'une cuve en produits réactifs, on peut observer que les opérateurs préparent tout d'abord les produits, puis introduisent ces derniers dans le réservoir et, enfin, consignent certaines informations concernant l'action qui vient d'être effectuée (comme, par exemple, la quantité de produit utilisée, les problèmes rencontrés ...).

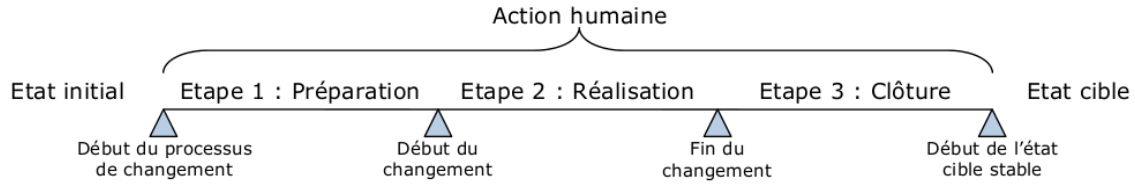

FIG. 2.8 – Représentation du processus de changement

Cette représentation permet de structurer la connaissance et peut être utile pendant et après les entretiens pour contrôler la collecte d'informations et organiser ces dernières. Nous proposons ainsi d'associer à chacune de ces phases, les items définis dans la partie 2.2.2.2 (cf. tableau 2.4).

Phase de l'action	Items associés
Préparation	Délégation, Aides, Formation
Réalisation	Expérience, Respect du cahier des charges, Facteurs d'environnement, Gestion collective et dynamique de groupe
Clôture	Contrôle et atteinte des objectifs, Retour d'expérience

TAB. 2.4 – Phases de l'action et items associés

La structuration « Préparation-Réalisation-Clôture » peut être particularisée pour certaines applications (comme par exemple pour des structures de petites tailles où le nombre d'équipes de travail est restreint). Cette particularisation se traduit par une simplification du nombre de phases liées à l'action [17], et impose une nouvelle structuration des items afin de garantir la complétude de la connaissance.

2.3.1.3 Le déroulement des analyses terrain

Pour les analyses faites sur le site industriel étudié, il est recommandé de constituer des binômes d'experts (un expert pour la partie technique et un autre pour la partie humaine et organisationnelle). Ce travail en binôme permet de recueillir et analyser les informations de manière complémentaire et permet ainsi d'avoir une vision complète (à la fois technique, humaine et organisationnelle) de la situation analysée.

Concernant les acteurs à interviewer, il est important d'aborder l'ensemble des niveaux hiérarchiques du système. En effet, chacun de ces acteurs peut apporter un éclairage différent et/ou complémentaire à la situation analysée.
Le risque, lorsque l'on se réfère uniquement aux dires d'un groupe de personnes appartenant à un même niveau, est de recueillir un discours uniforme et sans contradictions ne révélant pas la réalité de la situation vécue par d'autres acteurs. Ainsi, il est primordial de s'entretenir autant avec des opérateurs (de maintenance, de production, novices, expérimentés, sous-traitants ...), qu'avec des contrôleurs (internes et externes) et des managers (ingénieurs sûreté, responsable de production, directeur HSE [18] ...).

17. Ce type de particularisation est notamment utilisée par l'INERIS.
18. HSE : Hygiène - Sécurité - Environnement

2.3.2 L'intégration des dimensions technique et humaine

Cette partie a pour objectif de décrire comment se fait l'intégration entre les dimensions technique et humaine du système. Dans un premier temps, nous définissons les principes généraux de cette intégration, puis nous nous focalisons sur les variables qui permettent de faire le lien entre ces dimensions, et, enfin, nous présentons une méthode permettant de qualifier les influences.

2.3.2.1 Principes généraux et variables caractéristiques

Partant des différences existantes entre le fonctionnement d'un système technique et les comportements collectifs, nous proposons de considérer (et d'étudier) les influences des opérateurs sur le système technique comme des contraintes externes, au sens où le système technique passe d'un état stable (valide avant l'intervention humaine) à un autre état stable (valide après cette intervention). Entre ces états, le système technique évolue dans un état transitoire (cf. figure 2.7) pouvant conduire à des situations dangereuses.

Il est par conséquent nécessaire d'identifier les composants critiques du système technique, dont les dysfonctionnements doivent être minimisés du fait de leur importance pour le maintien, à un niveau acceptable, de la sûreté du système. Ces composants, que nous avons préalablement présentés dans la partie 2.2.1.3, sont les barrières de défense. La caractéristique qui nous intéresse plus particulièrement est leur disponibilité.

Cependant, l'efficacité des actions[19] de maintenance et de celles de conduite ont-elles la même influence sur la disponibilité de ces composants ?

Les caractéristiques respectives de ces actions, présentées dans la partie 2.2.2.2, permettent de définir deux types d'influences : les influences indirectes et les influences directes.
Cette configuration s'explique par le fait que la capacité d'un système industriel à fournir le produit pour lequel il a été conçu dépend notamment de sa disponibilité. En d'autres termes, cela sous-entend que la disponibilité du système, assurée dans un premier temps par l'efficacité des actions de maintenance, dépend également de sa capacité à produire, assurée par l'efficacité des actions de conduite. Ainsi, les actions de maintenance ont des influences indirectes alors que les actions de conduite ont des influences directes.

2.3.2.2 Méthode de qualification des influences

La méthode de qualification de ces influences (directes et indirectes) est construite en six étapes :
- Identifier le type de la barrière de défense étudiée (SIS ou CS, cf. partie 2.2.1.3).
- Identifier les composants de cette barrière (capteurs, actionneurs ...).
- Pour chacun de ces composants, estimer sa disponibilité intrinsèque par le biais des données constructeurs (si elles sont disponibles) et/ou par le retour d'expérience et la documentation à disposition.
  Cette disponibilité intrinsèque est associée à l'état initial (par conséquent stable) du composant étudié.

19. Nous rappelons qu'une action est efficace si elle remplit la fonction pour laquelle elle a été mise en place. Si cette fonction n'est remplit que partiellement, l'action est jugée inefficace.

- Estimer l'influence de l'efficacité et de l'inefficacité de l'action de maintenance considérée sur cette disponiblité intrinsèque. Cette étape permet de définir la disponibilité initiale du composant et constitue un premier état transitoire pour ce dernier.
- Estimer l'influence de l'efficacité et de l'inefficacité de l'action de conduite considérée sur cette disponibilité initiale. Cette étape permet de définir la disponibilité opérationnelle du composant, et est associée à un deuxième état transitoire pour ce dernier.
- Estimer la disponibilité opérationnelle de la barrière de défense étudiée en fusionnant les disponibilités opérationnelles de chacun de ses composants. La disponibilité opérationnelle de la barrière est associée alors à l'état final du processus de changement du niveau de disponbilité de la barrière.

De manière schématique, cette méthode se représente de la manière suivante :

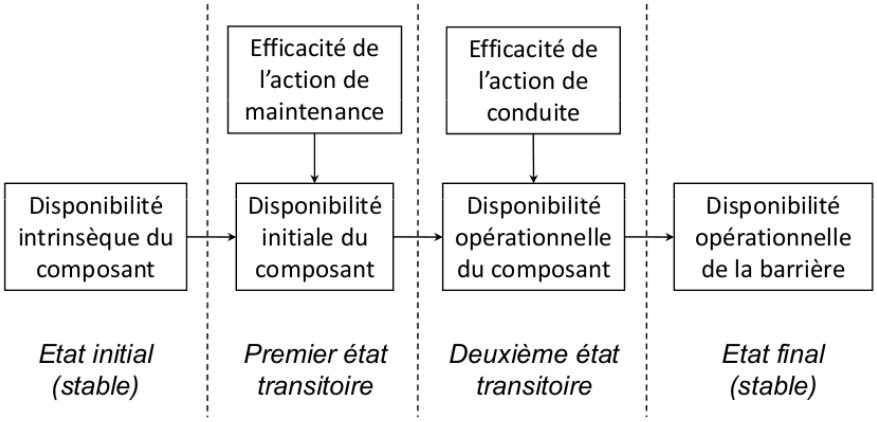

FIG. 2.9 – Qualification des influences des actions humaines sur la disponibilité d'un composant

L'estimation des influences de ces actions se fait par jugements d'experts, à partir des informations recueillies sur site (par entretiens et/ou analyse de la documentation à disposition), et dépend notamment de la complexité de l'action à réaliser et des moyens (techniques, humains ...) mis à disposition pour cette action.
En effet, la complexité d'une action réside dans le nombre de ses actions élémentaires, dans la nature des outils supports à sa réalisation, et/ou dans les compétences et connaissances nécessaires à son exécution [Miché *et al.*, 2006].

Enfin, la distinction proposée entre l'efficacité d'une action et son inefficacité s'explique par le fait que l'efficacité peut améliorer la disponibilité du composant alors que son inefficacité peut la dégrader. Prenons, par exemple, le cas du remplacement d'un composant défectueux (qui est une action de maintenance), et celui de la fermeture manuelle d'une vanne (qui est une action de conduite) :
- Dans le premier cas, si l'action de remplacement (*i.e.* le fait de retirer le composant défectueux et de le remplacer par un composant identique mais neuf) est efficace alors ce composant passe d'un état d'indisponibilité à un état de disponibilité[20]. La disponibilité (initiale) de ce composant a donc été améliorée par l'action de remplacement.

20. Si cette action est inefficace alors le composant reste indisponible.

– Dans le deuxième cas, si l'action de fermeture (*i.e.* fermer manuellement le robinet d'une vanne pour éviter l'épandage d'une substance) est inefficace (action mal réalisée, non réalisée ou non réalisable) alors la disponibilité (opérationnelle) du composant est dégradée. En effet, l'action humaine n'ayant pas remplie sa fonction, le composant ne se trouve pas dans la postion adaptée (*i.e.* fermée) pour que la barrière puisse également remplir sa fonction.

Il se peut également qu'un composant ne soit influencé que par des actions de maintenance, comme par exemple une soupape de sûreté. La méthode de qualification des influences présentée reste valable, mais doit être simplifiée pour ne considérer que l'étude des actions de maintenance, cf. figure 2.10.

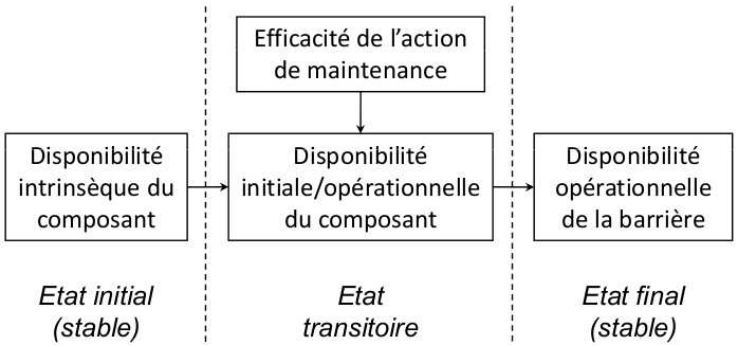

FIG. 2.10 – Qualification des influences des actions de maintenance sur la disponibilité d'un composant

2.3.3 L'intégration des dimensions humaine et organisationnelle

Cette partie a pour objectif de décrire comment se fait l'intrégration des dimensions humaine et organisationnelle du système. Comme précédemment, nous définissons les principes généraux de cette intégration, puis nous nous focalisons sur les variables qui permettent de faire le lien entre ces dimensions et, enfin, nous présentons une méthode permettant de qualifier ces influences.

2.3.3.1 Principes généraux et variables caractéristiques

Le comportement des opérateurs en situation de travail dépend non seulement d'interactions avec les dispositifs techniques du système, mais également du contexte organisationnel de leurs activités.
Ce contexte est représenté, dans notre approche, par sept facteurs organisationnels pathogènes (FOP). Ces facteurs, basés sur une vision dysfonctionnelle de l'organisation, sont considérés comme source d'aggravation des caractéristiques des actions humaines étudiées. Ainsi, ils peuvent être la source (indirecte) de l'inefficacité de ces actions.
Ce choix trouve sa justification dans la différence de granularité des disciplines considérées. En effet, l'étude des caractéristiques de l'organisation s'effectue à un niveau global (ou macroscopique), alors que celle concernant l'efficacité des actions humaines est réalisée à un niveau plus local. Il est par conséquent nécessaire de définir un ensemble de caractéristiques des collectifs de travail pouvant impacter l'efficacité de ces actions humaines, et être influencées par les facteurs organisationnels pathogènes.

Les comportements de ces collectifs de travail sont caractérisés par les items (cf. partie 2.2.2.2) et phases (cf. partie 2.3.1.2) des actions de maintenance et de conduite.

L'objectif de cette démarche d'intégration est de proposer une méthode permettant d'élaborer une structure d'influence générique, *i.e.* applicable à plusieurs types de structures organisationnelles et à différents secteurs d'activités, pouvant être particularisée pour la situation analysée. Cette particularisation se traduit alors par la suppression de certaines influences, et/ou l'identification de nouvelles influences.

2.3.3.2 Méthode de qualification des influences

La démarche développée distingue la méthode d'identification des influences et la construction du modèle de risque. En effet, la méthode d'identification des impacts permet de proposer une configuration humaine-organisationnelle quasi-générique [21], alors que le modèle de risque contient une méthode permettant de valuer ces influences (cette méthode sera abordée dans le chapitre suivant).

Les influences, entre les facteurs organisationnels pathogènes (FOP) et les variables caractéristiques d'une action humaine, sont identifiées en utilisant les caractéristiques locales des FOP, à savoir leurs signes, symptômes et marqueurs spécifiques (cf. annexe C).
Il s'agit d'identifier s'il existe des similitudes entre certaines caractéristiques de ces signes, symptômes et marqueurs, et les items et phases des actions humaines.
Il est nécessaire de souligner, à ce stade, l'importance des définitions associées à l'ensemble des variables représentatives des FOP, items et phases car ce sont ces définitions qui vont servir de support à l'identification des influences.

Notre approche, décrite dans la figure 2.11, est construite autour de trois étapes :
- L'identification de liens possibles entre, d'une part, les items et les signes/symptômes et, d'autre part, les phases et ces signes/symptômes (liens 1 et 1').
- La justification de la présence (ou de l'absence) d'influences entre, d'une part, les items et les FOP et, d'autre part, les phases et les FOP (liens 2, 2', 3 et 3'). Cette justification se fait de proche en proche, *i.e.* (a) l'identification de plusieurs liens entre un item (ou une phase) et des signes/symptômes de même nature permet d'identifier un lien entre cet item (ou cette phase) et le marqueur correspondant, (b) s'il existe un ensemble de liens entre un item (ou une phase) et plusieurs marqueurs caractéristiques d'un facteur, alors il est possible de définir un lien entre cet item (ou cette phase) et ce facteur organisationnel, puis de le justifier.
- La représentation, dans le modèle de risque, de ces influences si leur présence peut être justifiée (liens 4 et 4').

La mise en œuvre de cette démarche, rendue possible par la combinaison des connaissances et de l'expérience d'un ensemble d'experts (des systèmes techniques et des études organisationnelles), a permis de définir la configuration quasi-générique illustrée dans les tableaux 2.5 et 2.6 (les cases grisées contenant un « X » représentent la présence d'une influence, alors que les cases blanches représentent l'absence d'influence), justifiée en annexe D de ce mémoire (la justification porte autant sur la présence des liens que sur leur absence).

21. Nous explicitons par la suite pourquoi nous utilisons le terme « quasi-générique ».

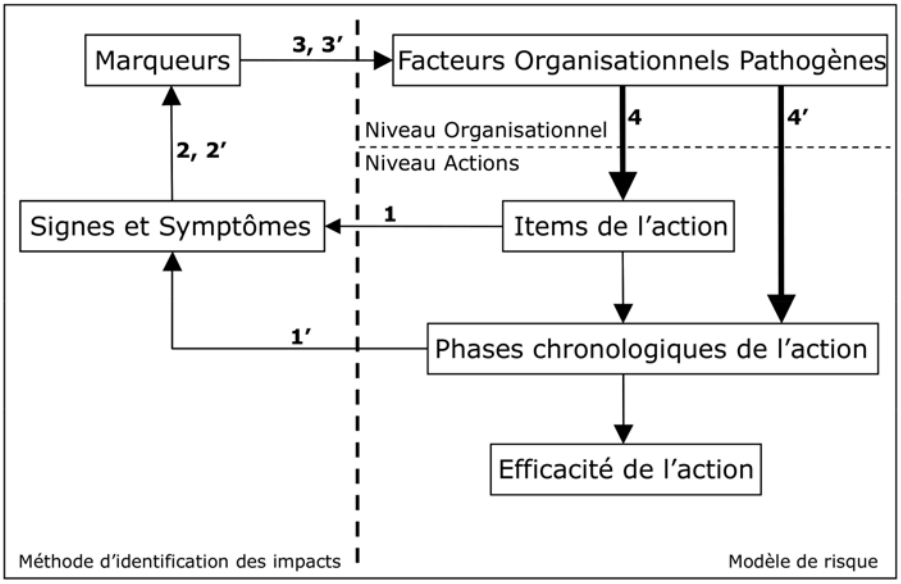

FIG. 2.11 – Construction des influences entre FOP et caractéristiques d'une action humaine

		Facteurs organisationnels pathogènes						
		COS	GQS	OC	MT	REX	PP	AR
Items	De				X		X	
	Ai	X		X		X	X	X
	Fo		X	X	X	X	X	
	Ex		X				X	
	Rcc	X	X	X	X		X	
	Fe				X	X	X	X
	Gcdg	X	X		X	X	X	
	Cao			X		X	X	X
	Rex	X	X		X	X	X	

TAB. 2.5 – Configuration quasi-générique des influences entre FOP et items

		Facteurs organisationnels pathogènes						
		COS	GQS	OC	MT	REX	PP	AR
Phases	Préparation	X	X	X	X	X	X	X
	Réalisation	X	X		X	X	X	
	Clôture		X	X	X	X	X	X

TAB. 2.6 – Configuration quasi-générique des influences entre FOP et phases

Illustrons à présent la justification associée à cette configuration quasi-générique. Ainsi, pour l'item Aides[22], la justification de la présence des influences est la suivante :

– **COS** - Si les risques sont mal identifiés alors la définition des plans d'actions peut être inadaptée aux risques réellement présents dans l'installation.

22. Rappelons que la justification associée aux autres variables est présentée en annexe D de ce mémoire.

- **OC** - L'absence de contrôle sur les procédures, et les dérives potentielles (banalisation des déviances) qui peuvent survenir par rapport à ces dernières, ont un impact sur la qualité des aides. On considérera à minima les organismes de contrôle interne.
- **REX** - Si des problèmes au niveau des aides (outils, documents, procédures ...) ont été identifiés durant une action et qu'ils ne sont pas résolus au moment de refaire cette action, alors les problèmes risquent d'apparaître à nouveau du fait du non-traitement de ce dysfonctionnement.
- **PP** - Le temps, les budgets, les moyens et les ressources sont revus à la baisse mais les objectifs restent constants, ce qui peut avoir pour effet une mauvaise adéquation des outils et de la tâche à réaliser.
- **AR** - Si la définition des plans d'actions n'évolue pas au même rythme que les modifications du système alors les documents utilisés pour préparer l'action risquent de devenir caduques.

Et, la justification de l'absence des influences est la suivante :

- **GQS** - Les aides définissent les documents et outils permettant aux collectifs de réaliser convenablement leurs activités. La définition du facteur organisationnel est axée sur les notions de formation, parcours professionnel, veille, tenue des habilitations ... Ces définitions ne permettent pas de faire un lien direct entre ce facteur organisationnel et cet item.
- **MT** - Si des problèmes apparaissent au niveau des aides cela provient d'autres facteurs (difficultés à faire vivre un retour d'expérience, pressions de production). Absence de connaissance suffisante pour permettre une justification de la présence du lien.

Ainsi, lors de l'analyse de situations particulières, ces configurations génériques sont adaptées (*i.e.* simplifiées, au sens ou certaines influences peuvent disparaître) aux spécificités de l'organisation en place et des actions humaines étudiées.

Plusieurs remarques, concernant la configuration générique ainsi obtenue, peuvent être soulignées :

- Tous les facteurs organisationnels n'influencent pas tous les items et toutes les phases d'une action humaine.
- Tous ces facteurs sont représentés dans le modèle de risque, *i.e.* ils ont au moins une influence sur un des items d'une action humaine (ou sur une de ses phases).
- Une limite à cette démarche réside dans les définitions données à chacun des items, phases et FOP. En effet, l'utilisation de définitions différentes (à celles proposées dans ce mémoire) peut conduire à une configuration différente. C'est en ce sens que nous qualifions de quasi-générique la configuration obtenue.

2.4 Conclusions

Ce chapitre nous a permis, d'une part, de définir le contenu des dimensions constitutives des systèmes considérés dans notre démarche [23] et, d'autre part, de proposer les principes utilisés pour réaliser leur intégration dans un modèle de risque. Ainsi, les dimensions retenues ont été rappelées et concernent les trois principales ressources nécessaires à l'exploitation d'un système industriel : le système technique, l'opérateur humain et l'organisation.
Cette intégration se base sur l'extraction des connaissances liées à chacune des ressources considérées, ainsi que sur la structuration de ces connaissances. Cette structuration consiste à utiliser les connaissances disponibles pour définir les variables représentatives du système

23. Ces dimensions ont été préalablement identifiées par EDF et l'INERIS dans le cadre du projet DIRIS [Duval *et al.*, 2005a].

et élaborer des méthodes permettant d'identifier et de construire les influences possibles entre ces variables.
L'analyse et la représentation de chacune de ces dimensions est abordée de manière sectorielle : la méthode des nœuds-papillons est utilisée pour les aspects techniques, l'étude des caractéristiques des collectifs en charge des actions de maintenance et de conduite (items et phases) est utilisée pour représenter la dimension humaine, et la caractérisation par facteurs organisationnels pathogènes est proposée pour analyser la situation organisationnelle. Chacune des démarches utilisées dans l'approche est justifiée par l'adéquation entre ses spécificités et les objectifs de notre méthodologie :

- Les nœuds-papillons permettent une représentation graphique complète des scénarios accidentels, *i.e.* de leurs causes à leurs conséquences finales.
- Considérer le collectif de travail (et non l'individu) en charge des actions de maintenance et de conduite permet d'aborder les notions de coopération, coordination et communication, qui sont des notions primordiales pour compenser les dérives individuelles, et de couvrir l'ensemble des activités humaines venant en support de l'exploitation de tout système industriel.
- La représentation par facteurs organisationnels pathogènes permet de souligner les faiblesses d'une organisation pouvant mener à l'occurrence d'une situation critique.

L'intégration de ces connaissances, issues de différentes disciplines, se fait au niveau des éléments clés pour la prévention des risques : les barrières de défense. En effet, l'indisponibilité de ces éléments est souvent significative d'autres problèmes sous-jacents ayant pour origine les opérateurs humains et l'organisation, et peut précipiter l'occurrence de l'événement redouté.
Une autre caractéristique de l'intégration proposée concerne le fait que l'organisation n'impacte pas directement le système technique mais se fait au travers du comportement des collectifs de travail, comme le développe [Paté-Cornell et Murphy, 1996]. Cette spécificité nous a permis de définir une méthode permettant d'identifier, de manière générique, les influences existantes entre les facteurs organisationnels et les caractéristiques des actions humaines (items et phases). L'adaptation de cette démarche à des situations particulières se traduit en maintenant un sous-ensemble des relations identifiées de manière générique.
En ce sens, notre approche propose d'analyser comment l'efficacité des actions de maintenance et de conduite est influencée (dégradée) par la présence de facteurs organisationnels pathogènes et comment cette efficacité influence (améliore ou dégrade) la disponibilité des barrières de défense du scénario analysé.
L'ensemble des principes développés dans ce chapitre ont un caractère générique, au sens où ils peuvent être adaptés pour différents types d'installations ayant à gérer des risques majeurs (nucléaire, chimie, aéronautique ...), en fonction des objectifs de l'analyse et des moyens à disposition.
Rappelons enfin que la méthodologie développée dans ce mémoire ne cherche pas à remplacer les méthodes classiquement utilisées dans les analyses sectorielles. C'est pourquoi nous ne représentons pas l'ensemble des caractéristiques de chacune des dimensions des systèmes considérés mais nous nous focalisons sur un ensemble de variables représentatives, ces dernières visant une exhaustivité qui permet de localiser les points faibles (techniques, humains et/ou organisationnels) de l'installation pour lesquels il est nécessaire de mener des études (sectorielles) spécifiques.

En effet, notre approche propose une vision globale pour l'analyse des risques d'une installation ([Léger *et al.*, 2008a], [Léger *et al.*, 2008b], [Duval *et al.*, 2008]). De par ses spécificités, la démarche que nous proposons peut être utilisée comme un outil support à la prise de décision.

A ce stade, la méthodologie ne permet pas de construire le modèle de risque associé à la situation analysée, ni d'estimer les risques étudiés. En effet, les aspects abordés dans ce chapitre ont été définis sans considérer l'outil de modélisation support à la quantification. Ainsi, les étapes de la méthodologie qui doivent à présent être présentées portent sur l'identification et l'utilisation d'un outil de modélisation qui permette, d'une part, la représentation du système sous la forme d'un seul modèle de risque et, d'autre part, la quantification du modèle et l'estimation des risques associés.

Chapitre 3

Unification des connaissances via le modèle de risque

Les aspects méthodologiques développés jusqu'à présent dans ce mémoire portent sur l'extraction et la structuration des différentes connaissances nécessaires pour la résolution de notre problématique d'analyse intégrée des risques.
Cependant ces mécanismes ne permettent pas, en l'état, de proposer une estimation quantitative des risques étudiés. En ce sens, ce chapitre présente une démarche permettant d'automatiser ces principes de structuration et de les unifier au travers d'un modèle de risque. Cette démarche se traduit globalement par un ensemble de modèles génériques auxquels sont associées des méthodes de quantification spécifiques aux types différents de variables concernées.

Ainsi, la première partie de ce chapitre porte d'une part, sur la justification de l'outil [1] de modélisation retenu (les réseaux bayésiens) au regard des autres outils utilisés dans le domaine des analyse de risques des systèmes industriels, et d'autre part, les spécificités de l'outil retenu.
La deuxième partie développe, quant à elle, les étapes nécessaires à la construction de la structure du modèle de risque, *i.e.* l'organisation des variables du modèle et de leurs influences.
En premier lieu, nous proposons, en nous basant sur des travaux existants (notamment ceux de [Portinale et Bobbio, 1999] et [Bobbio *et al.*, 2001]), un ensemble de mécanismes permettant la traduction des nœuds-papillons (représentant les scénarios incidentels/accidentels) en réseaux bayésiens.
Ensuite, nous abordons la modélisation des éléments constitutifs des barrières de défense et plus particulièrement la modélisation de leurs aspects techniques.
Enfin, nous explicitons la modélisation des dimensions humaine et organisationelle, ainsi que leurs interactions.

La dernière partie de ce chapitre propose, quant à elle, un ensemble de méthodes permettant la quantification des variables des scénarios non couvertes lors de la traduction des nœuds-papillons : les éléments techniques des barrières de défense, et les variables représentant les aspects humains et organisationnels.

1. Nous optons pour un formalisme unique afin de faire interopérer les différentes dimensions des systèmes considérés.

3.1 Choix de l'outil de modélisation

Cette partie porte sur la justification du choix de l'outil support à la modélisation : les réseaux bayésiens, et sur la présentation de leurs principales caractéristiques. Cette justification se base sur les objectifs liés à notre problématique d'analyse de risques et sur les travaux existants dans ce domaine.

3.1.1 L'intérêt des réseaux bayésiens

Les systèmes considérés dans notre approche, comme nous l'avons présenté dans les chapitres précédents, sont constitués par plusieurs sphères de connaissances (technique, humaine, et organisationnelle) en interaction, et en ce sens sont définis comme des systèmes complexes. Cette complexité s'illustre notamment au travers des structures d'influence existantes au sein des systèmes représentés, et de la nature des connaissances impliquées dans l'analyse (déterministes ou probabilistes). Enfin, les objectifs de l'analyse visent une quantification des risques associés au scénario étudié.

Ainsi, la modélisation de ces systèmes dans un objectif de quantification de leurs risques ne peut s'abstraire d'un outil supportant leurs caractéristiques (importance du nombre de variables représentatives, dépendances entre ces variables, connaissances issues de différentes disciplines ...). Différents outils sont susceptibles, *a priori*, de répondre aux besoins de notre problématique : les réseaux de Pétri stochastiques, les graphes de Markov, et les réseaux bayésiens. Mais un examen des spécificités de ces différents outils nous permet d'opter pour les réseaux bayésiens. En effet, un réseau bayésien permet de représenter et de quantifier, sous un formalisme unique, les différentes dimensions des systèmes considérés.

Les réseaux de Petri stochastiques, [Dutuit *et al.*, 1997], sont difficiles à mettre en œuvre du fait notamment de la nécessité de réaliser des simulations (de type Monte Carlo) pour obtenir des données de fiabilité. Or, ces simulations ont comme inconvénients de ne pas permettre de considérer correctement les événements non fréquents, et d'induire des temps de simulations importants.

Concernant les chaînes de Markov, même si ce formalisme permet une analyse précise de la probabilité de défaillance de composants dépendants entre eux, leur principal inconvénient réside dans l'explosion combinatoire du nombre d'états pour l'étude de systèmes industriels réels [De Souza et Ochoa, 1992]. Or, les systèmes considérés dans notre approche sont des systèmes industriels réels, dont les modèles sont composés d'un grand nombre de variables et d'interactions, et utilisant des connaissances issues de plusieurs disciplines. Ces caractéristiques ne sont pas compatibles avec une modélisation par chaînes de Markov.
De plus, cette explosion combinatoire est réduite lorsque les chaînes de Markov sont représentées par le biais de réseaux bayésiens dynamiques ([Weber, 2002], [Weber et Jouffe, 2003], [Boudali et Dugan, 2005]).

Les réseaux bayésiens sont des graphes orientés, sans circuits [2], dans lesquels chaque nœud représente une variable et chaque arc traduit une dépendance conditionnelle entre ces variables [Jensen, 2001]. Ce formalisme, initialement développé pour permettre la représentation de

2. Un graphe orienté est sans circuit s'il n'existe pas de chemin direct $X_1 \rightarrow ... \rightarrow X_n$, sauf si $X_1 = X_n$.

connaissances incertaines (dans le domaine de l'intelligence artificielle), est aujourd'hui de plus en plus utilisé pour des problématiques de fiabilité, d'analyse de risques, et de maintenance ([Boudali et Dugan, 2005], [Weber et Jouffe, 2006], [Langseth et Portinale, 2007]).
En ce sens, [Medina Oliva *et al.*, 2009] propose une analyse bibliographique portant sur les travaux publiés, dans ces domaines, au cours de la dernière décennie. Cette analyse montre que 23% des travaux, appliquant les réseaux bayésiens aux études de sûreté de fonctionnement, recensés portent sur la problématique d'analyse de risques (contre 64% pour les travaux portant sur la fiabilité, et 13% pour ceux portant sur la maintenance), et que le nombre de ces travaux a été multiplié par 4 sur la période 2001-2007.

Ces mêmes auteurs soulignent l'intérêt des réseaux bayésiens par rapport à d'autres outils, comme les arbres de défaillances, les réseaux de Pétri stochastiques, et les chaînes de Markov. Les hypothèses liées à l'utilisation des arbres de défaillances, comme la représentation par variables booléennes et l'indépendance des événements élémentaires, sont relâchées lorsque l'on opte pour une modélisation par réseaux bayésiens. Cette particularité est notamment due au fait que les réseaux bayésiens, qui se basent sur la théorie des graphes, peuvent être considérées comme une généralisation du formalisme des arbres. Nous pouvons citer en ce sens, et à titre d'exemples, les travaux de :
- [Torres-Toledano et Sucar, 1998], qui proposent une démarche, basée sur la notion de polyarbre [3], permettant l'analyse et la modélisation des dépendances entre défaillances (dans des systèmes complexes).
- [Bobbio *et al.*, 2001], qui développent une méthode qui permet de traduire les arbres de défaillances en réseaux bayésiens, et soulignent le fait que les réseaux bayésiens sont une extension de la modélisation booléenne classique (en introduisant les variables n-aires ou multi-états).

D'autres travaux montrent la capacité des réseaux bayésiens à modéliser les systèmes complexes dans un objectif d'analyse de sûreté de ces derniers (études de fiabilité, analyse de risques ...). En ce sens, certains des travaux présentés dans le chapitre 1 de ce mémoire, et notamment ceux de [Paté-Cornell et Murphy, 1996], [Kim et Seong, 2006], [Lee *et al.*, 2008], [Gregoriades et Sutcliffe, 2008], [Galàn *et al.*, 2007], et [Mohaghegh *et al.*, 2008], utilisent les réseaux bayésiens comme outil support à la modélisation des systèmes analysés dans leurs approches. Nous pouvons également citer les travaux de :
- [Embrey, 2002], qui propose une méthode utilisant des diagrammes d'influences, et intégrant les facteurs humains pour l'analyse et la prédiction de défaillances de systèmes critiques.
- [Weber *et al.*, 2004] qui considèrent un ensemble de variables exogènes aux systèmes étudiés afin de rapprocher les résultats de l'analyse du fonctionnement réel de ces systèmes.
- [Weber et Jouffe, 2006] qui formalisent une méthode de modélisation globale des systèmes complexes par l'utilisation de réseaux bayésiens dynamiques orientés objets, et qui se basent à la fois sur des données fonctionnelles et sur des données dysfonctionnelles.
- [Trucco *et al.*, 2008], qui développent une approche étudiant l'influence des facteurs organisationnels dans l'occurrence de collisions de navires.

Ainsi, les différents constats énoncés dans cette partie nous permettent de justifier, pour notre démarche méthodologique, le choix des réseaux bayésiens comme outil support à la

3. Un polyarbre est un graphe acyclique orienté pour lequel il n'y a qu'un chemin entre toute paire de nœuds.

modélisation.

Cet outil permet notamment de modéliser des variables multi-modales pouvant avoir des dependances conditionnelles (du fait du caractère multidisciplinaire de notre approche), et de traiter des cas de simulations et de diagnostics avec un seul modèle (et sur la base de données issues de l'expertise).
Nous pouvons cependant souligner les spécificités et limites inhérentes à l'utilisation de cet outil pour la modélisation des systèmes considérés dans notre approche :
- L'uniformité de traitement qui accorde la même importance aux données explicitant une connaissance réaliste, et celles qui expriment une méconnaissance totale de la situation.
- L'augmentation exponentielle de la dimension des tables de probabilités conditionnelles des variables filles, en fonction du nombre de variables parents associées.

3.1.2 Caractéristiques des réseaux bayésiens

Les caractéristiques que nous présentons dans cette partie sont celles jugées nécessaires à la construction des méthodes et modèles que nous proposons par la suite. Comme nous l'avons mentionné précédemment, un réseau bayésien est un graphe orienté sans circuit qui permet de représenter, par factorisation, la loi jointe :

$$P(S,T) = P(S|T).P(T) = P(T|S).P(S) \tag{3.1}$$

Avec : S, un événement ; T, un événement parent de S ; $P(S,T)$, la probabilité jointe de l'événement $(S \cap T)$; $P(S|T)$, la probabilité conditionnelle de S sachant T ; $P(T)$, la probabilité marginale de T ; $P(T|S)$, la probabilité de T sachant S ; et $P(S)$, la probabilité marginale de S.

Ces expressions permettent de formuler le théorème de Bayes :

$$P(S|T) = \frac{P(T|S).P(S)}{P(T)} \tag{3.2}$$

Et enfin, le calcul des probabilités marginales s'exprime par :

$$P_{post}(T) = \sum_S P(S,T) = \sum_S P(S).P(T|S) = \sum_S P_{prior}(S).\left(\frac{P(S|T).P_{prior}(T)}{P_{prior}(S)}\right) \tag{3.3}$$

Avec : $P_{post}(T)$, la probabilité *a posteriori* de T ; $P_{prior}(T)$, la probabilité *a priori* de T ; et $P_{prior}(S)$, la probabilité *a priori* de S.

Ainsi, dans un réseau bayésien, le calcul des probabilités marginales et l'actualisation de ces probabilités se fait par inférence.

Un réseau bayésien se traduit par le couple : G((N,M),P), où (N,M) représente le graphe (N, étant l'ensemble des nœuds, et M, l'ensemble des arcs orientés) et P définit l'ensemble des distributions de probabilités associées à chacun des nœuds du graphe [Weber et Jouffe, 2006].

Cette définition illustre celle proposée par [Jensen, 2001] qui décrit un réseau bayésien par :
- un ensemble de variables, et un ensemble d'arcs orientés entre ces variables,
- le fait que chaque variable possède une nombre limité d'états mutuellement exclusifs,
- le fait qu'à chaque variable S, ayant un ensemble de parents T_i (avec i allant de 1 à n), est associée une table de probabilités conditionnelles du type : $P(S|T_1, ..., T_n)$. Si cette variable S n'a pas de parent, alors sa table de probabilités n'est pas conditionnée ($P(S)$) mais sa probabilité *a priori* doit être spécifiée.

Les réseaux bayésiens étant des graphes causaux, ils supportent la notion de d-séparation. Cette notion précise que deux variables distinctes (V et W) sont d-séparées si, pour tous les chemins existants entre V et W, il existe une variable intermédiaire (Z, différente de V et W) telle que :
- La connexion est série ou divergente et Z est instanciée [4].
- La connexion est convergente, et ni Z, ni ses descendants ne sont instanciés.

Si les variables V et W ne sont pas d-séparées, elles sont d-connectées.

Une connexion est dite « série » si V influence Z, qui influence à son tour W (cf. figure 3.1). Ainsi la connaissance de l'état de V aura une influence sur l'état de Z, et indirectement sur l'état de W. Et inversement, la connaissance de l'état de W aura une influence sur V au travers de Z. Mais si l'état de Z est connu, alors V et W deviennent indépendantes.

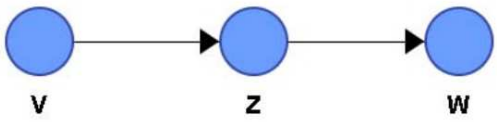

FIG. 3.1 – Connexion série

Une connexion est dite « divergente » lorsque les influences entre les variables filles de Z (les variables V et W) ne sont effectives que lorsque l'état de Z est connu (cf. figure 3.2).

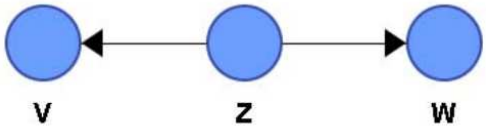

FIG. 3.2 – Connexion divergente

Une connexion est dite « convergente », que l'on nomme également V-structure, lorsque la connaissance ne peut se propager si l'état de la variable au centre de cette connexion (ou l'une de ses variables filles) est connu. Dans notre cas, V et W sont indépendantes si l'état de Z est connu (cf. figure 3.3).

4. L'instanciation décrit ici le fait de connaître, de manière sûre, l'état de la variable Z. En ce sens, il est également possible de parler d'évidence (la variable concernée se trouve dans un seul de ses états possibles).

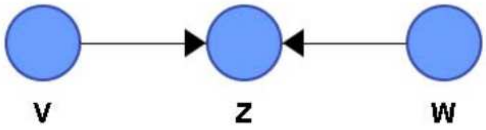

FIG. 3.3 – Connexion convergente

Ainsi, à partir de ces trois types de connexions, la notion d'indépendance conditionnelle peut être définie comme suit : V et W sont indépendantes sachant l'état de Z si P(V|Z,W)=P(V|Z).
P(V|Z) définit une probabilité conditionnelle, qui s'exprime dans les réseaux bayésiens par une table de probabilité conditionnelle (TPC).

Une table de probabilités conditionnelles, cf. tableau 3.1, se construit de la manière suivante :
– Soit S, un nœud du réseau, définit par les états $[s_1, s_2, ..., s_k]$.
– Soit T, un nœud parent de S, définit par les états $[t_1, t_2, ..., t_l]$.

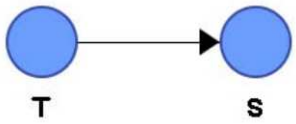

FIG. 3.4 – Réseau bayésien contenant deux variables

– La TPC de la variable S est définie par la probabilités conditionnelles $P(S|T)$ pour chaque état de S sachant l'état du parent T.

TPC P(S|T)		**S**			
		s_1	s_2	...	s_k
T	t_1	$P(S = s_1 \| T = t_1)$	$P(S = s_2 \| T = t_1)$	...	$P(S = s_k \| T = t_1)$
	t_2	$P(S = s_1 \| T = t_2)$	$P(S = s_2 \| T = t_2)$	...	$P(S = s_k \| T = t_2)$
	...	...	...	...	...
	t_l	$P(S = s_1 \| T = t_l)$	$P(S = s_2 \| T = t_l)$	...	$P(S = s_k \| T = t_l)$

TAB. 3.1 – Table de probabilités conditionnelles de la variable S

Enfin, comme le souligne [Weber et Jouffe, 2006], la notion d'inférence dans les réseaux bayésiens permet de considérer toute observation sur l'état d'une variable pour mettre à jour les probabilités associées aux autres variables du réseau.
Ainsi, si aucune observation (sur les variables du réseau) n'est disponible, l'inférence se fait à partir des probabilités définies *a priori*. Si à présent, il existe des observations (ou évidences), alors cette connaissance est intégrée dans le réseau, qui procède alors à une mise à jour de l'ensemble des probabilités de ses variables.
Cette inférence peut être réalisée avec différents niveaux de connaissances : des données certaines (lorsque l'état de la variable concernée est parfaitement connu), et/ou des données entâchées d'incertitudes (lorsqu'il existe une distribution de probabilités entre certains états de la variable concernée).

Ainsi, le tableau 3.2 présente les principales caractéristiques des réseaux bayésiens (RB) pouvant intéresser notre problématique d'analyse de risques.

Outil	Raisonnement	Quantification	Evolutions temporelles
RB	Inductif et Déductif	Oui	Non
RB Dynamique			Oui

TAB. 3.2 – Caractéristiques des réseaux bayésiens

3.2 Construction du modèle de risque

Dans cette partie, nous abordons les étapes de la modélisation qui permettent de représenter les variables du modèle et leurs influences, *i.e.* qui permettent de construire l'ossature du modèle de risque. Afin de structurer notre démarche, nous traitons distinctement les éléments du système ayant des caractéristiques similaires. Ces éléments s'organisent de la manière suivante : les nœuds-papillons (représentant les scénarios incidentels/accidentels), les barrières de défense (prévenant ou limitant l'occurrence de l'événement redouté du scénario) et les aspects humains et organisationnels (influençant ces barrières de défense).

3.2.1 Traduction d'un nœud-papillon en réseau bayésien

La traduction d'un nœud-papillon en un réseau bayésien se formalise par la traduction d'un arbre de défaillances puis par celle d'un arbre d'événements. La démarche de construction de ces arbres se base sur des mécanismes déterministes, qui peuvent être traduits et/ou complétés par des mécanismes probabilistes propres aux réseaux bayésiens.

3.2.1.1 Modélisation de la structure

Nous nous basons sur la méthode, proposée dans [Portinale et Bobbio, 1999] et complétée dans [Bobbio *et al.*, 2001], qui permet de traduire un arbre de défaillances en réseau bayésien pour l'analyse de systèmes fiables.

Cette démarche se base sur les hypothèses utilisées pour les analyses par arbre de défaillances, à savoir :
- les événements considérés sont binaires,
- ces événements sont statistiquement indépendants,
- les influences entre les événements et leurs causes sont représentées par des portes logiques de type ET et OU,
- l'événement indésiré constitue l'événement de base de l'arbre qu'il est nécessaire d'analyser.

L'utilisation des réseaux bayésiens permet de relâcher les trois premières hypothèses.

La méthode de traduction, illustrée dans les figures 3.5, 3.6 et 3.7, est décrite par [Bobbio *et al.*, 2001] en six étapes distinctes :

- Créer, pour chaque nœud feuille de l'arbre de défaillances (composant, événement ...), un nœud racine dans le réseau bayésien, en respectant le fait que les événements identiques

apparaissant plusieurs fois dans l'arbre ne sont modélisés qu'une seule fois dans le réseau bayésien.
- Assigner, à chaque nœud racine du réseau bayésien, les probabilités *a priori* du nœud feuille correspondant de l'arbre.
- Créer, pour chaque porte logique de l'arbre, un nœud dans le réseau bayésien.
- Associer un nom à ce nœud qui correspond à la variable de sortie de la porte logique considérée dans l'arbre.
- Connecter les nœuds dans le réseau bayésien à partir des connexions définies au niveau des portes logiques de l'arbre de défaillances. - Associer une table de probabilités conditionnelles à chaque nœud intermédiaire du réseau bayésien, et qui correspond à la porte (ET, OU, $k : n$) considérée dans l'arbre de défaillances.

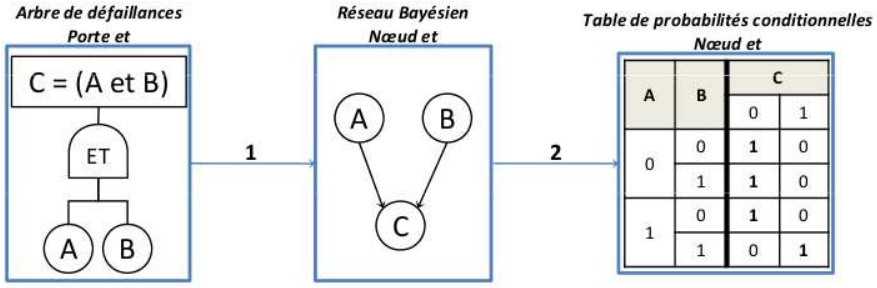

FIG. 3.5 – Traduction d'une porte ET

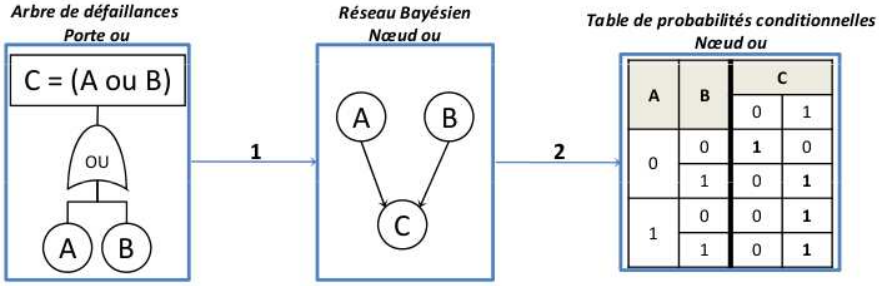

FIG. 3.6 – Traduction d'une porte OU

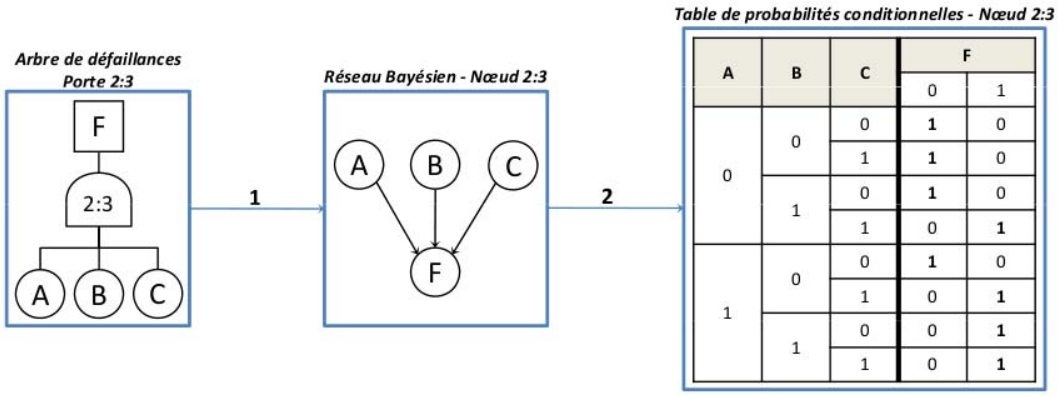

FIG. 3.7 – Traduction d'une porte 2 parmi 3

Dans ces figures, une variable à 1 traduit l'état de fonctionnement normal du composant associé alors que la valeur 0 traduit le dysfonctionnement de ce composant.

3.2.1.2 Quantification du modèle

Trois spécificités des systèmes considérés dans notre problématique impliquent d'utiliser des mécanismes probabilistes : les défaillances de causes communes, la paramétrisation des tables de probabilités conditionnelles pour des variables ayant de nombreux parents, et l'utilisation de variables n-aires.

a - Les défaillances de causes communes

Les portes probabilistes sont utilisées lorsque les connaissances du système sont incomplètes (*i.e.* lorsqu'il subsiste des incertitudes sur le comportement du système), ou lorsque l'analyse ne vise pas l'élaboration d'un modèle détaillé.
Dans le cas des défaillances de causes communes, la modélisation se fait directement dans les tables de probabilités conditionnelles du réseau bayésien en décrivant les dépendances probabilistes existantes entre les variables concernées [Bobbio *et al.*, 2001].

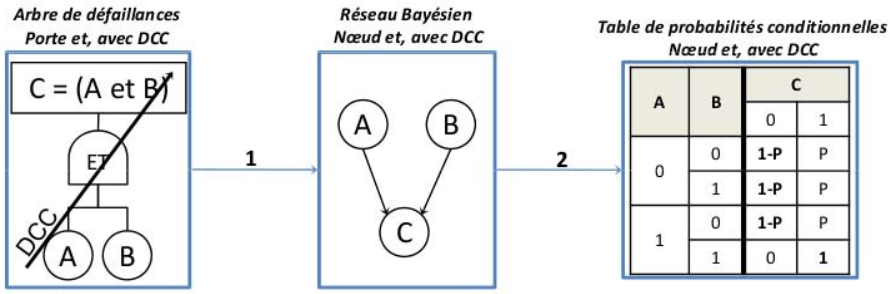

FIG. 3.8 – Traduction d'une porte ET, avec défaillances de causes communes (DCC)

La valeur P, dans la figure 3.8, définit la probabilité de défaillance du système du fait des causes communes (lorsqu'un des composants, ou les deux, sont en état de non fonctionnement).

b - L'utilisation des portes de type « noisy-OR » et « noisy-AND »

Partant du constat que la dimension d'une table de probabilités conditionnelles associée à une variable du modèle (et donc des paramètres à spécifier) croit exponentiellement avec le nombre de ses parents directs, il peut rapidement devenir difficile de paramétrer ces tables de probabilités.
En posant l'hypothèse que l'influence de chacun des parents de la variable considérée se définit de manière indépendante des autres parents, les portes de type « noisy » (OR et AND) réduisent l'effort de paramétrisation ([Jensen, 2001], [Onisko *et al.*, 2001]). En effet, le nombre de paramètres à spécifier pour ces portes devient linéaire au nombre de parents de la variable étudiée. Ainsi, l'utilisation de ces portes permet d'éviter la spécification complète de ces tables de probabilités conditionnelles.

Soit une variable binaire Y, et $X = \cup_{i=1}^{n} X_i$, l'ensemble des parents de Y également binaires. Le modèle « noisy-OR » requiert la définition de n paramètres (p_1, p_2, ..., p_n). Chacun de

ces paramètres représente la probabilité que Y soit vrai sachant que le parent X_k est vrai et que tous les autres parents sont faux (*i.e.* $P_k = P(Y/\bar{X}_1, ...X_k, ..., \bar{X}_n)$). Ainsi en partant de l'hypothèse que chaque X_k influence Y indépendamment des autres parents, le modèle se définit complètement si l'on suppose que Y est faux si aucun de ses parents n'est vrai.

$$P(Y|X) = 1 - \prod_{X_i \in X_t} (1 - p_i) \tag{3.4}$$

Avec $X_t \subseteq X$, l'ensemble des parents de Y étant vrais.

Une extension peut également être proposée, sous le terme de « leaky noisy-OR » [Galàn *et al.*, 2007], si l'on suppose qu'il existe une probabilité pour que Y soit vrai même si tous ses parents sont faux. Cette caractéristique se modélise en considérant que l'influence entre X_k et Y est pondérée par l'ajout d'un parent inconnu L. Ainsi, $P(Y/\bar{X}_1, ..., \bar{X}_n)$ devient $P(Y/\bar{X}_1, ..., \bar{X}_n, L) = l$, et l'équation (3.4) est modifiée comme suit :

$$P(Y|X) = 1 - (1 - l) \prod_{X_i \in X_t} (1 - p_i) \tag{3.5}$$

Un raisonnement similaire peut être mené pour les portes de type « noisy-AND », en considérant les paramètres p_i (définissant la probabilité que Y soit vrai, sachant que le parent X_k est faux et que tous les autres parents sont vrais) tels que $p_i = P(Y|X_1, ..., \bar{X}_i, ..., X_n)$ et aboutit à la formule (3.6).

$$P(Y|X) = \prod_{X_i \notin X_t} p_i \tag{3.6}$$

c - Les variables n-aires (ou multi-états)

L'ensemble des points développés jusqu'à présent s'appliquent à des variables binaires. Or, il peut être nécessaire de définir le comportement d'une variable de manière plus précise que par la dichotomie vrai/faux. C'est le cas, par exemple, pour des composants qui ont plusieurs modes de défaillances pouvant aboutir à différents effets sur le fonctionnement du système.

Cette caractéristique permet de donner différentes valeurs à la variable considérée, et ce par la définition de distributions de probabilités sur l'ensemble des états de cette variable ([Weber *et al.*, 2004], [Weber et Jouffe, 2006]).

Prenons, par exemple, le cas d'un composant (Y) dont le fonctionnement est conditionné par l'état de ses deux composants (cf. figure 3.9). Ce composant Y et le composant X_2 sont soit en fonctionnement soit défaillants, alors que le composant X_1 possède deux états de défaillance.
Ainsi, en fonction de la combinaison des défaillances des composants X_1 et X_2, la défaillance du composant Y sera plus ou moins probable (cf. tableau 3.3).

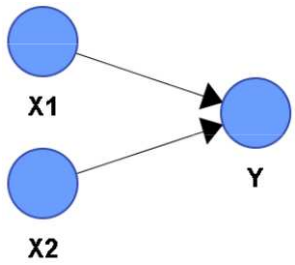

FIG. 3.9 – Réseau bayésien du composant Y

		Y	
X_1	X_2	Non défaillant	Défaillant
Non défaillant	Non défaillant	1	0
	Défaillant	p_1	$\bar{p}_1$
Défaillance 1	Non défaillant	p_2	$\bar{p}_2$
	Défaillant	0	1
Défaillance 2	Non défaillant	p_3	$\bar{p}_3$
	Défaillant	0	1

TAB. 3.3 – Exemple de TPC pour un composant Y

Avec :
- p_1, la probabilité pour que le composant Y fonctionne sachant que X_1 fonctionne et que X_2 est défaillant.
- p_2, la probabilité pour que le composant fonctionne sachant que X_2 fonctionne et que X_1 est dans l'état défaillant 1.
- p_3, la probabilité pour que le composant fonctionne sachant que X_2 fonctionne et que X_1 est dans l'état défaillant 2.

Cette table de probabilité peut alors être étendue pour des composants Y possèdant plusieurs états de défaillance (cf. tableau 3.4). La probabilité d'occurrence de l'une ou l'autre des défaillances de Y est conditionnée par les défaillances observées sur les composants X_1 et X_2.

		Y		
X_1	X_2	Non défaillant	Défaillance a	Défaillance b
Non défaillant	Non défaillant	1	0	0
	Défaillant	0	p_4	$\bar{p}_4$
Défaillance 1	Non défaillant	0	p_5	$\bar{p}_5$
	Défaillant	0	p_6	$\bar{p}_6$
Défaillance 2	Non défaillant	0	p_7	$\bar{p}_7$
	Défaillant	0	p_8	$\bar{p}_8$

TAB. 3.4 – Exemple de TPC pour un composant Y ayant plusieurs états de défaillance

Ainsi, la probabilité pour que le composant Y soit dans l'état défaillant a, se définit comme suit :
- p_4, en considérant que X_1 fonctionne et que X_2 est défaillant.
- p_5, en considérant que X_1 est dans l'état défaillant 1 et que X_2 fonctionne.
- p_6, en considérant que X_1 est dans l'état défaillant 1 et que X_2 est défaillant.
- p_7, en considérant que X_1 est dans l'état défaillant 2 et que X_2 fonctionne.
- p_8, en considérant que X_1 est dans l'état défaillant 1 et que X_2 est défaillant.

Nous développons par la suite comment obtenir les probabilités définies dans ces deux précédents tableaux.

3.2.2 La modélisation des barrières

Ayant décrit les mécanismes qui permettent de traduire le nœud-papillon d'un scénario incidentel/accidentel en un réseau bayésien, il convient de proposer une modélisation des éléments permettant de prévenir ou limiter l'occurrence de l'événement redouté lié à ce scénario (les barrières de défense). Dans un premier temps, nous rappelons les objectifs de cette partie du modèle. Puis, nous présentons les différents modèles développés (les modèles globaux, les modèles liés aux composants et les modèles partiels). Enfin, nous proposons un ensemble de modalités génériques pour chacun des groupes de variables concernés dans cette phase de modélisation.

3.2.2.1 Les objectifs de la modélisation

Dans cette partie du modèle de risque, l'objectif principal est d'estimer la disponibilité des composants techniques de sûreté en prenant en compte leur contexte humain et organisationnel, afin de pouvoir analyser les impacts du comportement de ces composants sur le système (occurrence des événements du scénario, impacts sur la sûreté, impacts sur l'environnement, impacts sur les biens ...).
En ce sens, les modèles proposés doivent permettre, dans le cas de simulations [5], de représenter les influences directes et indirectes des actions humaines (de maintenance et de conduite) sur la disponibilité du composant étudié.
Ces modèles doivent également permettre, dans le cas de diagnostics [6] de situations critiques, d'identifier les variables les plus influentes.
Enfin, les informations concernant un composant technique de sûreté peuvent être obtenues par le biais de données constructeur, d'analyses du retour d'expérience et/ou de jugements d'experts.

3.2.2.2 Les modèles globaux

Comme nous l'avons abordé dans le chapitre 2, deux types de barrières de défense ont été définies : les barrières de type Système Instrumenté de Sécurité (SIS), composées de trois sous-systèmes (détection, traitement et action) et les barrières de type Composant de Sûreté (CS), composées d'un seul sous-système (comme, par exemple, une soupape de sûreté ou un

5. Les analyses par simulation partent de la connaissance de l'état des variables parents pour identifier leurs influences sur les variables filles du modèle.

6. Les analyses par diagnostic partent de la connaissance de l'état de certaines variables filles afin d'identifier les parents les plus influents dans la situation analysée.

mur coupe-feu).
Nous avons également précisé que l'occurrence d'un scénario accidentel peut être évitée (ou limitée) par la présence de barrières disponibles dans le système analysé. Cette disponibilité est, par hypothèse, fonction de données intrinsèques au composant et de données contextuelles provenant de la situation dans laquelle se trouve ce composant (environnement physique, humain et organisationnel).
Ces spécificités permettent de proposer deux modèles globaux de barrières, l'un pour les barrières de type SIS (cf. figure 3.10) et l'autre pour les barrières de type CS (cf. figure 3.11, qui est une simplification du modèle précédent).

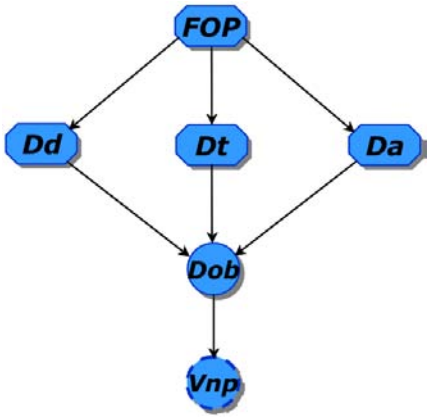

FIG. 3.10 – Modèle global d'une barrière de type SIS

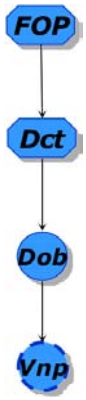

FIG. 3.11 – Modèle global d'une barrière de type CS

Dans ces figures, certains éléments modélisés sont des objets, tels qu'ils sont définis dans [Weber et Jouffe, 2006], et contiennent eux-mêmes plusieurs variables pouvant être connectées en réseaux. Nous reprenons ici la même symbolique pour formaliser les modèles présentés dans les figures 3.10 et 3.11 :

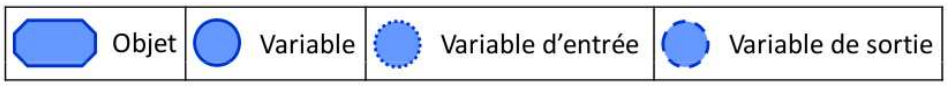

FIG. 3.12 – Symbolique utilisée dans les modèles

Les variables d'entrées sont des variables influençant les objets considérés [7] alors que celles de sortie sont les variables influencées par ces objets [8].

Les objets et variables modélisés décrivent alors les éléments suivants :
- FOP, un objet représentant les facteurs organisationnels pathogènes,
- Dd, un objet représentant la disponibilité du composant de diagnostic,
- Dt, un objet représentant la disponibilité du composant de traitement,
- Da, un objet représentant la disponibilité du composant d'action,
- Dct, un objet représentant la disponibilité du composant technique,
- Dob, une variable modélisant la disponibilité opérationnelle de la barrière (agrègeant les disponibilités des différents composants la constituant),

7. Ces variables d'entrées peuvent influencer tout ou partie des variables contenues dans l'objet considéré.
8. Ces variables de sorties peuvent être influencées par tout ou partie des variables de cet objet.

– Vnp, la variable du nœud-papillon qui représente l'événement sur lequel la barrière agit directement. En effet, dans une représentation par nœud-papillon (cf. partie 2.2.1.2), les barrières de défense sont directement implantées dans le scénario de risque. Lorsque l'on utilise les réseaux bayésiens, la représentation diffère, la barrière est intégrée en tant que parent direct de l'événement qu'elle prévient/protège.

3.2.2.3 Les modèles liés aux composants

Considérant, d'une part, le fait que la disponibilité opérationnelle d'un composant dépend des actions humaines (maintenance et/ou conduite) qui lui sont associées (cf. partie 2.2.2.2) et, d'autre part, le fait qu'une action de maintenance agit de manière indirecte sur cette disponibilité opérationnelle [9] (cf. partie 2.3.2.1), nous proposons un premier modèle générique représentant le comportement d'un composant d'une barrière. Ainsi, dans la figure 3.13, nous définissons le contenu des objet Dd, Dt, et Da. Ces trois objets ont une structure identique et font le lien entre les facteurs organisationnels pathogènes et la disponibilité opérationnelle de la barrière.

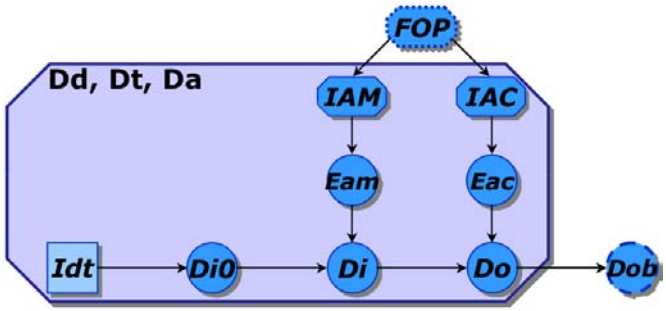

FIG. 3.13 – Modèle générique de composant d'une barrière

Les objets et variables définies dans cette figure ont la signification suivante :
– IAM, un objet regroupant les items caractéristiques de l'action de maintenance étudiée,
– IAC, un objet regroupant les items caractéristiques de l'action de conduite étudiée,
– Eam, l'efficacité de l'action de maintenance [10],
– Eac, l'efficacité de l'action de conduite [11],
– Idt, l'Installation du dispositif technique (qui est une variable de décision [12] modélisant la présence physique du composant dans le système),
– Di0, la disponibilité intrinsèque du composant (qui décrit la disponibilité constructeur compte-tenu de sa présence physique),
– Di, la disponibilité initiale du composant (qui décrit la disponibilité du composant compte-tenu de sa disponibilité intrinsèque et des actions de maintenance réalisées),
– Do, la disponibilité opérationnelle du composant (qui décrit la disponibilité du composant compte-tenu de sa disponibilité initiale et des actions de conduite spécifiques).

9. Alors que l'action de conduite agit directement sur cette disponibilité.
10. Cette efficacité se définit comme la probabilité pour que cette action de maintenance soit réalisée correctement compte tenu de son contexte humain et organisationnel.
11. Cette efficacité se définit comme la probabilité pour que cette action de conduite soit réalisée correctement compte tenu de son contexte humain et organisationnel.
12. Une variable de décision est un nœud représentant une évidence obligatoirement définie (*i.e.* sans distribution *a priori*). Dans notre cas, cette variable permet d'activer ou non l'utilisation de la barrière.

Ce modèle n'est applicable que pour les composants des barrières de type SIS (possédant des composants de diagnostic, traitement et action). En effet, la présence d'actions de conduite ne permet pas de modéliser les composants des barrières de type CS.

Pour pouvoir modéliser les composants des barrières de type CS, *i.e.* modéliser le comportement d'un composant ne nécessitant que des actions de maintenance (cf. partie 2.3.2.2), le modèle à utiliser est le suivant :

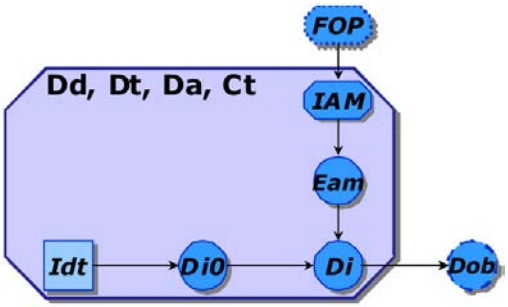

FIG. 3.14 – Modèle simplifié (composants ne nécessitant que des actions de maintenance)

Ainsi, ce modèle est applicable non seulement à l'ensemble des composants des barrières de type SIS, mais également (et par simplification) aux composants des barrières de type CS.

3.2.2.4 Les modèles partiels

Les modèles globaux proposés pour les barrières (cf. figures 3.10 et 3.11), peuvent être raffinés en trois types de modèles partiels. Ces modèles partiels de barrières sont proposés et organisés en fonction des ressources impliquées : le modèle « technique », le modèle « humain » et le modèle mixte. Ces modèles partiels utilisent les modèles génériques définis pour les composants (cf. figures 3.13 et 3.14).

Le modèle « technique » se définit par le fait que tous les composants de la barrière considérée sont des composants techniques de sûreté, nécessitant uniquement des actions de maintenance pour être en mesure de remplir leur fonction. L'ensemble des composants de ce type de barrières se modélise par la figure 3.14.
Le modèle « humain » se traduit par le fait que tous les composants de la barrière nécessitent, pour pouvoir remplir correctement leur fonction, non seulement des actions de maintenance, mais également des actions de conduite. L'ensemble des composants de ce type de barrières se modélise par la figure 3.13.
Enfin, le modèle mixte permet de représenter une barrière dont chaque composant peut être influencé soit par des actions de maintenance (cf. figure 3.14), soit par des actions de maintenance et des actions de conduite (cf. figure 3.13). Ainsi, pour ce dernier modèle, il n'y a pas unicité dans la représentation des différents composants de la barrière étudiée.

En considèrant les barrières de type SIS, différentes configurations (ou modèles partiels) peuvent être rencontrées. Ces configurations sont présentées dans le tableau 3.5.

Deux configurations ne peuvent être définies (signalées par « / » dans le tableau 3.5) du fait des spécificités des barrières de type SIS. En effet, une détection humaine implique un

traitement humain.
Considérons, par exemple, une barrière permettant d'éviter le surremplissage d'une cuve. Le fait de surveiller visuellement le niveau de produit dans la cuve implique une action humaine en cas de surremplissage, comme l'appui sur un bouton d'arrêt d'urgence pour stopper le transfert de produit.

Composant de			Type de barrière
Détection	**Traitement**	**Action**	
Composant technique	Composant technique	Composant technique	Technique
		Action humaine	Mixte (a)
	Action humaine	Composant technique	Mixte (b)
		Action humaine	Mixte (c)
Action humaine	Composant technique	Composant technique	/
		Action humaine	/
	Action humaine	Composant technique	Mixte (d)
		Action humaine	Humaine

TAB. 3.5 – Nature des barrières de type SIS

Les autres configurations sont illustrées, pour cet exemple, de la manière suivante :

Type de barrière	Composant de Détection	Composant de Traitement	Composant de Action
Technique	Capteur de niveau	Ordre automatique de fermeture d'une vanne	Fermeture automatique de la vanne
Mixte (a)		Activation automatique d'une alarme	Fermeture manuelle de la vanne
Mixte (b)		Appui sur un bouton pour fermer la vanne	Fermeture automatique de la vanne
Mixte (c)		Activation manuelle d'une alarme	Fermeture manuelle de la vanne
Mixte (d)	Surveillance visuelle du niveau	Appui sur un bouton pour fermer la vanne	Fermeture automatique de la vanne
Humaine		Activation manuelle d'une alarme	Fermeture manuelle de la vanne

TAB. 3.6 – Exemples de barrières

3.2.2.5 Les modalités associées aux variables des modèles proposés

Ayant présenté la structure graphique des différents modèles de barrières, nous pouvons aborder la définition des modalités des variables propres aux composants techniques de ces barrières (cf. tableau 3.7). Les modalités des autres variables présentes dans ces modèles seront précisées dans les parties suivantes.

Variables	Modalités	Définition
Idt	Présent	Cette modalité permet de préciser que le composant considéré est présent physiquement dans le système étudié.
	Absent	Cette modalité définit l'absence physique du composant.
Di0, Di, Do, Dob	Disponible	C'est l'aptitude du composant à être en état d'accomplir sa fonction dans des conditions données, à un instant donné ou durant un intervalle de temps donné, en supposant que la fourniture des moyens extérieurs nécessaires est assurée [AFNOR, 2001].
	Indisponible	C'est l'inaptitude du composant à être en état d'accomplir cette fonction.
	Absent	Cette modalité définit l'absence physique du composant.
Vnp	Absent	Cette modalité permet de définir l'absence de dysfonctionnement d'un composant ou l'absence de l'événement.
	Présent	Cette modalité permet de définir la présence du dysfonctionnement ou de l'événement.

TAB. 3.7 – Modalités et définitions associées aux variables d'un composant technique

Concernant les modalités associées aux variables du nœud-papillon (Vnp), deux modalités ont été définies de manière générique (Absent, Présent) mais le nombre et l'intitulé de ces modalités peuvent être étendus (*i.e.* pour passer de la représentation d'un comportement binaire à la représentation d'un comportement n-aire) en fonction des particularités de l'événement considéré.
Précisons également que l'état de la variable « Idt », représentant les hypothèses de départ de l'analyse en ce qui concerne la présence physique des composants des barrières, doit être fixé avant toute inférence (simulation ou diagnostic).

3.2.3 La modélisation des aspects humains et organisationnels

Dans la description des modèles des barrières présentés ci-avant, nous n'avons pas abordé la modélisation des aspects humains et organisationnels les influençant. Ces points vont à présent être discutés. En premier lieu, nous rappelons les objectifs de cette partie du modèle. Puis, nous présentons différentes structures d'influences pouvant être utilisées pour représenter ces dimensions. Ensuite, nous proposons un ensemble de modalités génériques pour chacun des groupes de variables concernés dans cette phase de modélisation. Enfin, nous analysons, de manière plus précise, les spécificités de chacune des structures proposées (informations à recueillir lors des enquêtes faites sur le terrain, comportements en fonction des connaissances disponibles, dimensions des tables de probabilités).

3.2.3.1 Les objectifs de la modélisation

Dans cette partie du modèle (allant des caractéristiques de l'organisation à l'efficacité de l'action humaine), nous cherchons à évaluer l'efficacité d'une action humaine compte-tenu de son contexte (collectif de travail et/ou organisation).
La connaissance de cette efficacité permet par la suite d'estimer la disponibilité des barrières de défense.

Le modèle doit permettre d'étudier, en fonction de l'information à disposition (qui est, elle-même, fonction du sujet central des investigations sur site et des objectifs de ces enquêtes [13]) :
- les impacts de l'organisation sur le collectif de travail,
- les impacts du collectif de travail sur l'efficacité de l'action,
- les impacts combinés organisation/collectif de travail sur l'efficacité de l'action.

Ce modèle doit également permettre le diagnostic de situations critiques (organisation/collectif de travail) dans le cas où une (ou plusieurs) action(s) humaine(s) s'est (se sont) avérée(s) inefficace(s).

Les différentes connaissances recherchées peuvent ainsi être obtenues :
- pour une action existante, via une analyse du retour d'expérience et des avis d'experts,
- pour une nouvelle action (dont on a aucun historique), par un impact de l'organisation et/ou des collectifs de travail spécifiques à d'autres actions déjà en place.

Nous formalisons l'ensemble de ces finalités par une structure générique adaptée (liens, paramètres, comportements ...), qui sera plus compliquée qu'une structure spécifique issue d'un cas particulier ne considérant pas l'ensemble de ces finalités (mais étant un sous-ensemble de ce modèle générique).

3.2.3.2 Présentation des différentes structures d'influences

Différentes structures, cf. figures 3.15, 3.16, et 3.17, peuvent être utilisées pour modéliser les influences présentes entre les facteurs organisationnels pathogènes, les caractéristiques des actions humaines (items et phases), et l'efficacité de ces dernières. L'utilisation d'une de ces structures dépend, d'une part, des connaissances à disposition pour renseigner le modèle et, d'autre part, des objectifs de l'analyse.

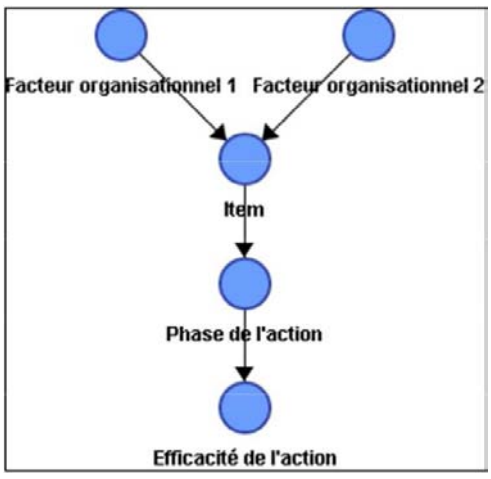

FIG. 3.15 – Structure n°1

La première structure (cf. figure 3.15) reprend la configuration développée dans l'approche System-Action-Management [Paté-Cornell et Murphy, 1996] et repose, de ce fait, sur

13. En effet, les informations recueillies n'auront pas le même niveau de granularité si l'analyse est réalisée par des experts en fiabilité humaine ou par des experts en analyse organisationnelle.

l'hypothèse que l'organisation influence les opérateurs qui, eux-mêmes, ont une influence sur le système technique. Ainsi les facteurs organisationnels pathogènes influencent l'état des items caractéristiques de l'action, qui influencent à leur tour l'efficacité de cette action au travers de ses phases.

La deuxième structure (cf. figure 3.16) diffère de la précédente car les influences entre les facteurs organisationnels et les items ne sont plus explicitement représentées. Les items sont placés au niveau organisationnel et le processus de changement lié à l'action est considéré à un niveau local (celui du collectif en charge de l'action).

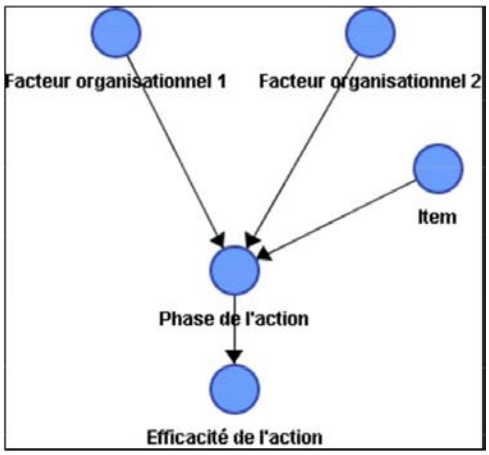

FIG. 3.16 – Structure n°2

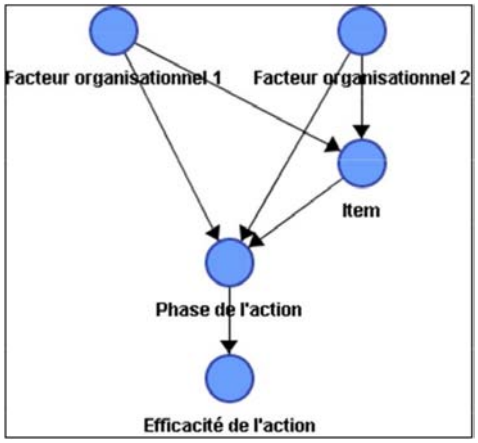

FIG. 3.17 – Structure n°3

Enfin, la dernière configuration (cf. figure 3.17) est la plus complète et la plus générique mais aussi la plus compliquée. Dans cette configuration, nous replaçons les items au niveau du collectif de travail, ce qui permet une modélisation explicite des influences entre les facteurs organisationnels et les items, tout en conservant un lien direct entre les facteurs organisationnels et les phases de l'action (comme le souligne le « chemin des conditions latentes » de la figure 1.8 du chapitre 1 de ce mémoire).

Nous proposons de discuter, dans les paragraphes suivants, de l'intérêt de chacune de ces structures. Avant cela, il est nécessaire de définir les modalités retenues pour les différentes variables du modèle.

3.2.3.3 Les modalités associées aux variables représentatives de ces dimensions

Ayant présenté les différentes structures d'influence permettant de modéliser ces dimensions, nous pouvons définir les modalités des variables repésentatives de ces dimensions (cf. tableau 3.8).

Variables	Modalités	Définition
FOP	Absent	Signifie que le caractère pathogène du facteur organisationnel n'est pas avéré.
	Présent	Signifie que le caractère pathogène du facteur organisationnel est avéré.
Items	Présent	Modalité générique, qui signifie que l'item considéré est effectif, *i.e.* il répond aux exigences de l'action.
	Dégradé	Modalité générique, qui signifie que l'item considéré est non effectif, *i.e.* il ne répond pas (ou que partiellement) aux exigences de l'action.
Phases	Efficace	Signifie que la phase de l'action considérée est efficace, *i.e.* elle remplit la fonction pour laquelle elle a été mise en place.
	Inefficace	Signifie que cette phase est inefficace, *i.e.* elle ne remplit pas ou que partiellement la fonction pour laquelle elle a été mise en place.
Efficacité	Efficace	Signifie que l'action réalisée est efficace, *i.e.* elle remplit la fonction pour laquelle elle a été mise en place.
	Inefficace	Signifie que cette action est inefficace, *i.e.* elle ne remplit pas ou que partiellement la fonction pour laquelle elle a été mise en place.

TAB. 3.8 – Modalités et définitions associées aux FOP et aux variables représentatives d'une action humaine

Les modalités associées aux items ont été définies de manière générique mais le nombre et l'intitulé de ces modalités peut être étendu (*i.e.* passer de la représentation d'un comportement binaire à la représentation d'un comportement n-aire) en fonction des particularités de l'item considéré, alors que les facteurs organisationnels pathogènes sont, par définition, des variables booléennes.

3.2.3.4 Analyse des caractéristiques des différentes structures d'influences

Les spécificités de chacune des trois structures présentées ci-avant (cf. figures 3.15, 3.16 et 3.17) sont liées d'une part, au(x) groupe(s) de variables defini(s) comme nœuds racines du réseau, et d'autre part aux influences existantes entre les différents groupes de variables du modèle proposé.

a - Caractéristiques des variables racines du réseau pour les trois structures
Les informations relatives aux variables racines du réseau bayésien et celles nécessaires pour la construction du modèle sont des données *a priori* qui sont spécifiées par jugements d'experts et à l'aide du retour d'expérience disponible.

Structures	Groupe(s) de variables racines		
n°1	Facteurs Organisationnels Pathogènes	*ET*	/
n°2			Items
n°3			/

TAB. 3.9 – Nœuds racines du modèle pour chacune des structures étudiées

b - Caractéristiques des variables filles du réseau pour la structure n°1
Différents groupes de variables filles sont à considérer dans cette structure : les items, les phases et l'efficacité de l'action humaine.

Concernant les items, l'information recherchée se traduit par l'interrogation suivante : sachant l'état des facteurs organisationnels (Absent ou Présent), quelle est la probabilité pour que chaque item soit Présent ?
Ainsi, partant d'une configuration initiale [14] et en considérant le type d'action et le type de composant, on obtient une distribution de probabilités *a priori* pour l'item concerné.
Si, à présent, un facteur organisationnel prend un caractère pathogène, alors cette distribution se trouve dégradée par la présence de ce facteur pathogène. Plus il y a de facteurs organisationnels pathogènes, plus cette dégradation doit être importante. Nous verrons par la suite comment implanter, dans le modèle, ce principe de dégradation (ou d'aggravation).

Concernant les phases de l'action, deux points sont à aborder :
- Sachant l'état des items (Présent ou Dégradé), quelle est la probabilité pour que la phase concernée (Préparation, Réalisation, Clôture) soit Efficace ?
- Dans combien de cas où l'action (de maintenance/conduite sur un équipement donné) a été inefficace, un problème lié à la préparation (et/ou à la réalisation, et/ou à la clôture) a été identifié ?

Le premier point permet d'analyser les influences entre les items et les phases de l'action de manière descendante [15] ; le second point analyse les influences entre les phases et l'efficacité de l'action de manière ascendante [16].

Enfin, la concaténation de l'efficacité de chacune des phases de l'action permet de définir le niveau d'efficacité de l'action. Cette concaténation est fonction de la complexité de l'action étudiée (équipement concerné, outils à utiliser, personnel nécessaire ...), et peut se traduire dans le réseau bayésien :
- soit par une règle logique simple [17], si les trois phases de l'action sont considérées comme ayant le même facteur d'influence sur l'efficacité de l'action analysée,
- soit par une règle logique pondérée, si chacune de ces phases à un facteur d'influence spécifique sur l'efficacité de cette action.

Cette première configuration devient limitative lorsque l'on connaît l'état de tous les items (si, par exemple, l'analyse a été menée par des experts en fiabilité humaine). Les facteurs organisationnels deviennent alors indépendants des phases de l'action et donc de son efficacité. En d'autre termes, il est possible de découpler la dimension organisationnelle des autres dimensions du modèle.

14. Cette configuration initiale est obtenue par jugements d'experts et par une analyse du retour d'expérience disponible.
15. Il s'agit ici de se poser la question : « Que se passerait-il si ... ? ».
16. Dans ce cas, il est courant d'utiliser le retour d'expérience disponible.
17. Cette règle logique est traduite par un ET si l'efficacité de l'action est conditionnée par l'efficacité de l'ensemble de ses phases, ou un OU si l'efficacité de cette action est conditionnée par l'efficacité d'une de ses phases.

c - Caractéristiques des variables filles du réseau pour la structure n°2

Deux groupes de variables doivent également être considérés dans cette structure : les phases et l'efficacité de l'action humaine.

L'efficacité des phases de l'action est conditionnée par l'état des facteurs organisationnels et l'état des items. Comme précédemment, la définition d'une configuration initiale permet de spécifier une distribution *a priori* pour ces variables. Puis, différentes dégradations sont à considérer :

- si un facteur organisationnel prend un caractère pathogène,
- si un item est mal (ou non) réalisé [18],
- si une combinaison des deux dégradations est observée (facteurs organisationnels et items).

La méthode de quantification devra donc permettre de montrer pour chacune des phases de l'action, l'influence :

- du caractère pathogène de chacun des facteurs organisationnels,
- du caractère dégradé de chaque item. Ceci se traduit, dans la table de probabilité, par une dégradation de la distribution initiale pour une situation organisationnelle « optimale » mais dont l'item étudié est dégradé,
- de l'effet cumulé de plusieurs facteurs organisationnels pathogènes (alors que les items sont présents),
- de l'effet cumulé de plusieurs items dégradés (alors que le contexte organisationnel n'a pas de caractère pathogène),
- de l'effet cumulé de la combinaison facteur(s) organisationnel(s) pathogène(s) et items dégradés.

Concernant l'efficacité de l'action, l'information est obtenue de la même manière que ce que nous avons proposé pour la structure n°1.

Dans cette structure, il n'y a pas de liens directs entre les facteurs organisationnels et les items (cf. figure 3.16, partie 3.2.3.2), il faut alors connaître l'état des phases de l'action pour que les facteurs organisationnels et les items deviennent dépendants. Or, l'efficacité de ces phases, qui contribuent directement à l'efficacité de l'action, est une variable dont nous cherchons à estimer l'état à partir d'une situation observée (au travers des facteurs organisationnels pathogènes et/ou des items).

d - Caractéristiques des variables filles du réseau pour la structure n°3

Trois groupes de variables sont à considérer dans cette dernière structure : les items, les phases et l'efficacité de l'action humaine.

Concernant les items et l'efficacité de l'action humaine, les informations sont obtenues de la même manière que ce que nous avons proposé pour la structure n°1.

Concernant les phases de l'action, l'information est obtenue de la même manière que ce que nous avons proposé dans la structure n°2.

18. Plus le nombre d'items négatifs augmente, plus cette dégradation sera importante.

D'un point de vue comportemental, la structure n°3 est celle qui répond à l'ensemble des objectifs de la modélisation (cf. partie 3.2.3.1). En effet, du fait des influences présentes dans cette structure, il est possible de représenter les impacts de l'organisation sur le collectif de travail mais également ceux de ce collectif sur l'efficacité de l'action et, enfin, les impacts combinés organisation/collectifs de travail sur cette efficacité.

Cette structure permet ainsi de s'adapter aux informations disponibles suite aux recueils effectués sur site[19], et de ne pas limiter la circulation de ces informations dans le modèle proposé. Ce que ne permettent pas les autres structures.

Afin d'assurer le caractère générique de notre démarche d'intégration, nous proposons d'utiliser la structure n°3 pour les développements qui vont suivre.
Notons que cette structure générique peut être simplifiée, en fonction des informations à disposition, lors de l'application à des cas particuliers. Certaines influences peuvent disparaître et on se retrouve alors dans des structures de type 1 ou 2. La mise en œuvre de telles simplifications dans le modèle entraînent ainsi la considération des limites inhérentes à la structure simplifiée obtenue.

e - Comparaison des caractéristiques paramétriques de chaque structure
Dans ce paragraphe, nous présentons les dimensions des tables et le nombre des paramètres à définir dans les situations extrêmes, *i.e.* lorsqu'il n'y a qu'une variable parent qui influence la variable fille étudiée et lorsque l'ensemble des variables parents d'un même type influencent cette variable fille. Lors de l'application à une situation concrète, les dimensions des tables et le nombre de paramètres à spécifier se situeront donc dans cet intervalle.

Le premier tableau (cf. tableau 3.10) présente la dimension des tables de probabilités conditionnelles associées à chacune des variables du modèle. Le second tableau (cf. tableau 3.11) précise le nombre de paramètres à faire spécifier (en théorie) par le groupe d'experts.

	Structure n°1	**Structure n°2**	**Structure n°3**
Facteurs organisationnels	$1 \cdot 2$	$1 \cdot 2$	$1 \cdot 2$
Items	$2^1 \cdot 2$ à $2^7 \cdot 2$	$1 \cdot 2$	$2^1 \cdot 2$ à $2^7 \cdot 2$
Préparation	$2^3 \cdot 2$	$2^4 \cdot 2$ à $2^{10} \cdot 2$	$2^4 \cdot 2$ à $2^{10} \cdot 2$
Réalisation	$2^4 \cdot 2$	$2^5 \cdot 2$ à $2^{11} \cdot 2$	$2^5 \cdot 2$ à $2^{11} \cdot 2$
Clôture	$2^2 \cdot 2$	$2^3 \cdot 2$ à $2^9 \cdot 2$	$2^3 \cdot 2$ à $2^9 \cdot 2$
Efficacité de l'action	$2^3 \cdot 2$	$2^3 \cdot 2$	$2^3 \cdot 2$

TAB. 3.10 – Dimensions des TPC pour une variable ($ligne \cdot colonne$)

Ce premier tableau montre que, pour certaines structures (notamment les structures n°2 et n°3), la dimension des tables de probabilités conditionnelles peut devenir importante, et augmenter la complexité du modèle. En ce sens, il est nécessaire de développer une méthode

19. Ces informations peuvent être d'un niveau organisationnel macroscopique et/ou d'un niveau humain plus local, du fait, d'une part, des experts en charge de l'analyse (appartenant soit à la discipline des facteurs humains, soit à celle des analyses organisationnelles) et, d'autre part, de l'implication de l'organisation dans cette analyse.

permettant de structurer la construction de ces tables de probabilités. Nous abordons cette structuration dans la partie 3.3.2 de ce chapitre.

	Structure n°1	**Structure n°2**	**Structure n°3**
Facteurs organisationnels	7	7	7
Items	18 à 1152	9	18 à 1152
Préparation	8	16 à 1024	16 à 1024
Réalisation	16	32 à 2048	32 à 2048
Clôture	4	8 à 512	8 à 512
Efficacité de l'action	8	8	8
Total	**61** à **1195**	**80** à **3608**	**89** à **4751**

TAB. 3.11 – Nombre de paramètres à spécifier (en théorie)

Le second tableau met en évidence le fait que plus la structure d'influences se complique, plus le nombre de paramètres nécessaires à la construction théorique du modèle augmente. En l'état, les paramètres sont trop nombreux pour que les experts puissent les discerner et donc les quantifier. C'est pourquoi il est nécessaire de développer une méthode de quantification qui permette de réduire le nombre de paramètres à expliciter.

3.3 Quantification du modèle de risque

Dans cette partie, nous abordons les étapes de la modélisation relatives à la quantification des variables du modèle de risque influençant (directement ou indirectement) le scénario incidentel/accidentel : les éléments techniques des barrières de défense et les aspects humains et organisationnels pouvant les impacter.
Partant du constat fait par [Gregoriades et Sutcliffe, 2008], qui soulignent que la performance d'un réseau bayésien dépend directement des connaissances *a priori* que l'utilisateur lui fournit, il s'avère nécessaire de développer des méthodes permettant de modéliser le plus finement possible ces connaissances *a priori* et la manière de les implémenter dans les tables de probabilités conditionnelles associées.

3.3.1 Le niveau technique de la barrière

Au niveau des modèles de barrières de défense, les variables concernées sont, d'une part, les disponibilités des composants (que nous avons formalisé par trois niveaux : la disponibilité intrinsèque, la disponibilité initiale et la disponibilité opérationnelle) et, d'autre part, la disponibilité opérationnelle de la barrière (cf. figure 3.13 de la partie 3.2.2.3).

a - La disponibilité intrinsèque du composant

La table de probabilité associée à cette variable, cf. tableau 3.12, se définit en fonction de la présence (ou de l'absence) physique du composant dans le système.

- **SI** le composant est **absent** physiquement du système, **ALORS** ses valeurs de disponibilité et d'indisponibilité ne peuvent être estimées. Le composant prend alors l'état **absent**.
- **SI** le composant est **présent** dans le système, **ALORS** il est possible de définir une distribution de probabilités sur ses états de **disponibilité** et d'**indisponibilité** (la probabilité de l'état absent prend alors obligatoirement une valeur nulle). Cette distribution de probabilités s'obtient par le biais de données contructeurs (comme les taux de défaillance ou de réparation ...), du retour d'expérience à disposition et/ou de jugements d'experts.

Installation du dispositif technique	**Disponibilité intrinsèque**		
	Disponible	Indisponible	Absent
Présent	x_1	$1 - x_1$	0
Absent	0	0	1

TAB. 3.12 – TPC associée à la disponibilité intrinsèque d'un composant ($x_1 \in [0, 1]$)

b - La disponibilité initiale du composant

Concernant la variable représentant la disponibilité initiale du composant, *i.e.* la disponibilité du composant impactée par l'efficacité de la maintenance, nous proposons d'appliquer un principe d'aggravation uniquement sur les états de disponibilité et d'indisponibilité du composant (cf. tableau 3.13). Ce principe d'aggravation permet de dégrader la probabilité de la variable d'être dans l'état influencé par cette aggravation. Si le composant est absent, il restera dans cet état quel que soit l'état de l'action de maintenance (efficace ou non).

SI le composant est **intrinsèquement disponible ET** :
- que l'action de maintenance est **efficace**, **ALORS** le composant conserve le **même niveau de disponibilité**,
- que cette action de maintenance est **inefficace**, **ALORS** le niveau de disponibilité du composant se trouve **dégradé** d'un facteur $\alpha_1 \in [0, 1]$.

SINON
SI le composant est **intrinsèquement indisponible ET** :
- que l'action de maintenance est **efficace**, **ALORS** le niveau d'indisponibilité du composant se trouve **dégradé** d'un facteur $\alpha_2 \in [0, 1]$ (par complémentarité, cette caractéristique a pour effet d'augmenter la disponibilité du composant),
- que cette action de maintenance est **inefficace**, **ALORS** le composant conserve le **même niveau d'indisponibilité**.

SINON Le composant est **absent**.

Ainsi, si le composant est intrinsèquement disponible, le principe d'aggravation s'applique sur la modalité « Disponible » de la variable fille, alors que si le composant est intrinsèquement indisponible, le principe d'aggravation s'applique sur la modalité « Indisponible » de cette variable fille.

Disponibilité intrinsèque	**Efficacité de l'action de maintenance**	**Disponibilité initiale**		
		Disponible	Indisponible	Absent
Disponible	Efficace	1	0	0
	Inefficace	α_1	$1-\alpha_1$	0
Indisponible	Efficace	$1-\alpha_2$	α_2	0
	Inefficace	0	1	0
Absent	Efficace	0	0	1
	Inefficace	0	0	1

Tab. 3.13 – TPC associée à la disponibilité initiale d'un composant

Avec : α_1, le facteur de dégradation de la disponibilité initiale du composant dû à l'inefficacité de l'action de maintenance ; α_2, le facteur d'amélioration de cette disponibilité initiale dû à l'efficacité de l'action de maintenance.

c - La disponibilité opérationnelle du composant

La même approche est utilisée pour la variable représentant la disponibilité opérationnelle du composant, *i.e.* la disponibilité du composant impacté par l'efficacité de la conduite (cf. tableau 3.14).

SI le composant est **initialement disponible ET** :
- que l'action de conduite est **efficace**, **ALORS** le composant conserve le **même niveau de disponibilité**,
- que cette action de conduite est **inefficace**, **ALORS** le niveau de disponibilité du composant se trouve **dégradé** d'un facteur $\alpha_3 \in [0,1]$.

SINON
SI le composant est **initialement indisponible ET** :
- que l'action de conduite est **efficace**, **ALORS** le niveau d'indisponibilité du composant se trouve **dégradé** d'un facteur $\alpha_4 \in [0,1]$,
- que cette action de conduite est **inefficace**, **ALORS** le composant conserve le **même niveau** d'indisponibilité.

SINON Le composant est **absent**.

Disponibilité initale	**Efficacité de l'action de conduite**	**Disponibilité opérationnelle**		
		Disponible	Indisponible	Absent
Disponible	Efficace	1	0	0
	Inefficace	α_3	$1-\alpha_3$	0
Indisponible	Efficace	$1-\alpha_4$	α_4	0
	Inefficace	0	1	0
Absent	Efficace	0	0	1
	Inefficace	0	0	1

Tab. 3.14 – TPC associée à la disponibilité opérationnelle d'un composant

Avec : α_3, le facteur de dégradation de la disponibilité opérationnelle du composant dû à l'inefficacité de l'action de conduite ; α_4, le facteur d'amélioration de cette disponibilité

opérationnelle dû à l'efficacité de l'action de conduite.

Les facteurs de dégradation, α_i (pour $i = [1, 2, 3, 4]$), sont établis par jugements d'experts et par une analyse du retour d'expérience à disposition, à partir d'une table d'estimation semi-quantitative. Cette échelle peut, par exemple, se définir de la manière suivante :

Modalités	α_i (en %)
Pas d'impact	100
Faible impact	95
Impact moyen	75
Impact important	50
Impact fort	1

TAB. 3.15 – Exemple de table permettant d'estimer les α_i

La construction d'une telle échelle doit suivre un certain nombre de règles afin de pouvoir être plus facilement appréhendée par les experts. Ces régles permettent de définir le nombre de modalités de l'échelle, leur signification, les valeurs numériques associées et les conclusions admissibles. Nous proposons ainsi, en annexe G, un ensemble de règles pour la construction de l'échelle d'élicitation associée au cas d'application de ces travaux de thèse.

Avant de poursuivre sur la méthode utilisée pour quantifier la disponibilité opérationnelle d'une barrière, nous proposons d'illustrer notre démarche au travers d'un exemple.

d - Exemple de calcul de la disponibilité d'un composant

Nous considérons une vanne manuelle qui nécessite une action de maintenance (surveillance) et une action de conduite (fermeture/ouverture manuelle). Le modèle permettant de calculer la disponibilité de cette vanne est donné par la figure 3.18.

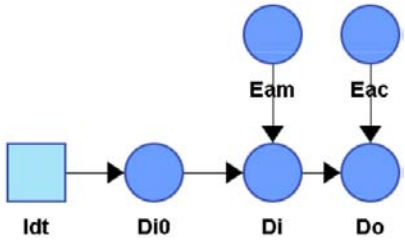

FIG. 3.18 – Modèle du composant étudié

Avec les variables suivantes :
- **Idt**, l'installation du dispositif technique (la vanne),
- **Di0**, la disponibilité intrinsèque de la vanne,
- **Di**, la disponibilité initiale de la vanne,
- **Do**, la disponibilité opérationnelle de la vanne,
- **Eam**, l'efficacité de l'action de surveillance,
- **Eac**, l'efficacité de l'action de fermeture/ouverture manuelle.

Les données à renseigner avant toute inférence sont précisées dans le tableau 3.16 et sont obtenues par jugements d'experts.

Variable	**Valeur** (en%)
Disponibilité intrinsèque de la vanne (Di0)	99
Efficacité de l'action de maintenance (Eam)	90
Efficacité de l'action de conduite (Eac)	99
Influence de l'efficacité de la maintenance (α_1)	50
Influence de l'inefficacité de la maintenance (α_2)	75
Influence de l'efficacité de la conduite (α_3)	25
Influence de l'inefficacité de la conduite (α_4)	75

TAB. 3.16 – Données du modèle à renseigner avant inférence

Les résultats observés [20] avec cette quantification sont définis ci-après :

- Si la variable « Idt » est fixée à l'état « absent », alors le modèle aboutit à une évidence sur l'absence (des disponibilités Di0, Di et Do) du composant.

- Si la variable « Idt » est fixée à l'état « présent » (sans ajouter d'autre évidence), alors la disponibilité intrinsèque du composant (Di0) vaut 99%, sa disponibilité initiale (Di) vaut 94.27%, et sa disponibilité opérationnelle (Do) vaut 94.98%.
  Illustrons le calcul pour la variable Di0 :

$$P(Di0 = disponible|Idt = present) = \frac{P(Idt=present|Di0=disponible).P(Di0=disponible)}{P(Idt=present)}$$

$$P(Di0 = disponible|Idt = present) = \frac{100\times99}{100} = 99\%$$

- Si la variable « Idt » est fixée à l'état « présent » et que l'action de maintenance (Eam) est efficace (sans connaître l'état de l'action de conduite), alors Di vaut 99.25% et Do vaut 98.69%.
  Par contre si l'action de maintenance est inefficace, alors Di prend la valeur 49.50% et Do prend la valeur 61.63%.

- Si la variable « Idt » est fixée à l'état « présent » et que l'action de conduite (Eac) est efficace (sans connaître l'état de l'action de maintenance), alors Di vaut 94.27% et Do vaut 95.71%.
  Par contre si l'action de conduite est inefficace, alors Do prend la valeur 23.57%.

- Si la variable « Idt » est fixée à l'état « présent » et que les actions de maintenance et de conduite sont efficaces, alors Di vaut 99.25% et Do vaut 99.44%.

- Si la variable « Idt » est fixée à l'état « présent » et que l'action de maintenance est inefficace et celle de conduite est efficace, alors Di prend la valeur 49.50% et Do prend la valeur 62.12%.

20. Ces résultats sont obtenus automatiquement par inférence dans le réseau bayésien modélisant le composant (cf. figure 3.18).

– Si la variable « Idt » est fixée à l'état « présent » et que l'action de maintenance est efficace et celle de conduite est inefficace, alors Di prend la valeur 99.25% et Do prend la valeur 24.81%.

Nous pouvons remarquer que l'efficacité de l'action de conduite a une influence plus importante sur la disponibilité opérationnelle du composant que l'efficacité de l'action de maintenance.

Ce cas permet d'illustrer que l'efficacité de chaque action peut avoir une influence spécifique sur la disponibilité du composant concerné et que l'inefficacité de plusieurs actions conduit à une situation plus dégradée que si une seule de ces actions est inefficace.
Le modèle ainsi construit permet également de pouvoir conclure sur la disponibilité du composant même si l'information concernant l'efficacité des actions est partielle.

e - La disponibilité opérationnelle de la barrière

Enfin, la table de probabilités conditionnelles relative à la variable représentant la disponibilité opérationnelle de la barrière, *i.e.* la variable qui aggrége les disponibilités des différents composants de cette barrière, est formalisée selon la règle logique précisée ci-après.

SI tous les composants de la barrière sont **disponibles**, **ALORS** cette barrière est **disponible**.
SINON
SI un ou plusieurs de ses composants est **absent**, **ALORS** cette barrière est **absente**.
SINON cette barrière est **indisponible**.

Prenons, par exemple, le cas d'une barrière de défense dont la fonction est d'empêcher la propagation d'un incendie. Cette barrière, de type SIS, se compose d'un détecteur de fumée, d'une unité de traitement, et d'un sprinkler. Si l'un de ces composants est absent ou indisponible, alors la barrière ne peut remplir sa fonction et prend alors respectivement l'état « absent » ou l'état « indisponible » (cf. partie 3.2.2.5) :
– Sans détection de fumée, l'unité de traitement ne peut analyser un dépassement de seuil et actionner le sprinklage.
– Sans unité de traitement, la détection de fumée ne suffit pas à déclencher un sprinklage de la zone incendiée.
– Sans sprinklers, la zone incendiée ne peut être arrosée (même s'il y a eu détection de fumées).

3.3.2 Les niveaux humain et organisationnel

La construction des tables de probabilités conditionnelles associées aux variables représentatives de la dimension humaine (les items, les phases et l'efficacité d'une action de maintenance ou de conduite) dépend de la méthode d'aggravation utilisée pour qualifier les influences présentes entre ces variables et les facteurs organisationnels pathogènes (qui sont les variables représentatives de la dimension organisationnelle).

3.3.2.1 Présentation des différentes méthodes d'aggravation

Les différentes méthodes que nous proposons se basent sur la règle suivante : si une variable parent A est dans un état dégradé, alors l'état non dégradé de la variable fille B passe d'un niveau de probabilité N à un niveau de probabilité (N-x).
Le paramètre « x » représente l'importance de l'influence de la variable parent sur sa variable fille, et peut s'exprimer de différentes manières selon la méthode utilisée. Ce paramètre peut entraîner, pour la variable fille, un seul ou plusieurs niveaux de dégradations simultanés.

a - La méthode d'aggravation par niveau de vraisemblance
La première déclinaison de cette méthode, (a), est basée sur la règle suivante : Si m variables parents de type A (sur n variables du même type) sont dans un état dégradé alors le niveau de probabilité de la variable fille B passe d'un niveau N à un niveau (N-p).
Avec :
- m allant de 1 à n, n étant le nombre total des variables de type A.
- p, un paramètre qui représente l'influence du nombre de variables parents de type A sur la variable fille étudiée.

Nous illustrons cette déclinaison de la méthode par l'exemple qui suit :
- Si tous les facteurs organisationnels pathogènes sont absents, alors la probabilité de l'état « présent » de l'item Formation (relatif au remplacement d'une sonde de température) est fixée à $P_{pf} = 99\%$.
- Si un de ces sept facteurs est présent, alors cette probabilité est multipliée par un facteur $f_1 = 10^{-1/8}$.
- Si deux de ces sept facteurs sont présents, alors cette probabilité est multipliée par un facteur $f_2 = 10^{-1/4}$.
- Si trois de ces sept facteurs sont présents, alors cette probabilité est multipliée par un facteur $f_3 = 10^{-1/2}$.
- Si quatre (ou plus) de ces sept facteurs sont présents, alors cette probabilité est multipliée par un facteur $f_4 = 10^{-1}$.

La deuxième déclinaison de cette méthode, (b), nécessite de considèrer l'ensemble de la combinatoire associée aux différents états des parents, et de proposer une distribution de probabilités (ou une règle logique) pour chaque ligne de la table de probabilités conditionnelles.

Nous illustrons cette déclinaison de la méthode par l'exemple suivant :
- Si aucun facteur organisationnel n'est présent, alors la probabilité de l'état « présent » de l'item Formation prend la valeur $P_{pf} = 99\%$.
- Si le facteur organisationnel « Pressions de Production » est présent, alors cette probabilité prend la valeur $P_{pf} = 50\%$.
- Si le facteur organisationnel « Mauvais traitement de la complexité organisationnelle » est présent, alors cette probabilité prend la valeur $P_{pf} = 75\%$.
- Si les facteurs organisationnels « Pressions de Production » et « Mauvais traitement de la complexité organisationnelle » sont présents, alors cette probabilité prend la valeur $P_{pf} = 35\%$ ...

b - La méthode d'aggravation par facteur de dégradation

Dans cette approche, la probabilité de l'état non dégradé d'une variable B donnée est fonction de l'influence spécifique de l'état dégradé de chacun de ses parents. De manière plus précise, partant d'un contexte complétement favorable (*i.e.* lorsque l'ensemble de variables parents de la variable B sont dans un état non-dégradé), la probabilité initiale de l'état non dégradé de la variable B peut être fixée à $b_0 \in [0, 1]$.
Soit A_1, un des parents de B. Si ce parent passe dans un état dégradé, alors la probabilité de l'état non dégradé de la variable B devient $b_0 \times \alpha_{A1-B}$,
avec $\alpha_{A1-B} \in [0, 1]$, le facteur de dégradation représentatif de l'influence négative de cette variable parent sur B.
Si à présent, un second parent (A_2) passe également dans un état dégradé, alors la probabilité de la variable B devient $b_0 \times f(\alpha_{A1-B}, \alpha_{A2-B})$, avec :

- $\alpha_{A2-B} \in [0, 1]$, le facteur de dégradation représentatif de l'influence négative de la variable A_2 sur B.
- $f(\alpha_{A1-B}, \alpha_{A2-B})$, une fonction permettant de cumuler les influences négatives des variables A_1 et A_2 sur la variable B.

En ce sens, nous proposons de définir la fonction $f(\alpha_{A1-B}, \alpha_{A2-B})$ comme le produit des α_{Ai-B} (avec $i = 1, 2$).
L'utilisation de l'opérateur multiplicatif est ici utilisé pour traduire l'effet cumulé de l'état dégradé de plusieurs variables parents sur la variable fille concernée. Cet effet cumulé se traduit de la manière suivante : si une seule variable parent est dans un état dégradé, alors la situation observée sur la variable fille doit être moins critique que si deux variables parents sont dans cet état dégradé.

Ainsi la probabilité que la variable B soit dans son état non dégradé, sachant l'état dégradé de ses parents A_1 et A_2, se définit comme suit :

$$P(\bar{b}|a_1, a_2) = b_0 \times f(\alpha_{A1-B}, \alpha_{A2-B}) = b_0 \times \alpha_{A1-B} \times \alpha_{A2-B} \tag{3.7}$$

Nous pouvons remarquer, à ce stade, que la déclinaison (a) de la méthode d'aggravation par niveau de vraisemblance est plus restrictive que la méthode utilisant les facteurs de dégradation. En effet, la première démarche ne permet pas de définir l'impact d'une variable parent particulière sur une variable fille particulière, mais modélise l'impact d'un nombre de variables parents (étant dans un état dégradé) d'un même type sur l'état d'une variable fille.

3.3.2.2 Etude paramétrique des différentes méthodes d'aggravation

Afin de pouvoir opter pour l'une ou l'autre de ces méthodes, en rationalisant la paramétrisation, il s'avère nécessaire de conduire une étude comparative sur la quantité de paramètres nécessaire à la quantification de chacune des structures définies dans la partie 3.2.3.2. En effet, comme nous l'avons vu dans la partie 3.2.3.4, il est important d'utiliser une méthode de quantification qui permette, d'une part de structurer les tables de probabilités conditionnelles et, d'autre part de réduire le nombre de paramètres à évaluer.
En ce sens, une analyse du nombre de paramètres à définir (cf. tableaux 3.17 à 3.19) a été menée pour chacune de ces méthodes de quantification et pour chacune des structures d'influences présentées dans la partie 3.2.3.2.

	Structure n°1	Structure n°2	Structure n°3
Facteurs organisationnels	7	7	7
Items	18 à 72	9	18 à 72
Préparation	4	8 à 32	8 à 32
Réalisation	5	10 à 40	10 à 40
Clôture	3	6 à 24	6 à 24
Efficacité de l'action	4	4	4
Total	**41** à **95**	**44** à **116**	**53** à **179**

TAB. 3.17 – Nombre de paramètres à spécifier (méthode des niveaux de vraisemblance - type a)

Dans ces tableaux, nous précisons les nombres minimaux et maximaux de paramètres à définir pour la variable considérée.

Prenons, dans le tableau 3.17, l'exemple des items de la structure n°1 :

- Au minimum, chaque variable se quantifie par le biais d'une distribution initiale pouvant être influencée par un seul des sept facteurs organisationnels pathogènes. Il y a donc deux règles à définir pour chaque item (soit 18 règles pour l'ensemble des items) : l'une représentant l'état de l'item dans un contexte favorable, et l'autre représentant l'état de cet item sachant la présence d'un facteur organisationnel pathogène.
- Au maximum, chaque variable se quantifie par le biais d'une distribution initiale pouvant être influencée par les sept facteurs organisationnels pathogènes. Il y a donc huit règles à définir pour chaque item (soit 72 règles pour l'ensemble des items) : l'une représentant l'état de l'item dans un contexte favorable, et l'autre représentant l'état de cet item sachant la présence des sept facteurs organisationnels pathogènes.

	Structure n°1	Structure n°2	Structure n°3
Facteurs organisationnels	7	7	7
Items	18 à 1152	9	18 à 1152
Préparation	8	16 à 1024	16 à 1024
Réalisation	16	32 à 2048	32 à 2048
Clôturee	4	8 à 512	8 à 512
Efficacité de l'action	8	8	8
Total	**61** à **1195**	**80** à **3608**	**89** à **4751**

TAB. 3.18 – Nombre de paramètres à spécifier (méthode des niveaux de vraisemblance - type b)

Nous pouvons conclure, au regard des résultats de cette analyse, que la méthode de quantification par facteur de dégradation est celle qui s'adapte le mieux à notre problématique. Elle permet de limiter le nombre de paramètres à définir (cf. tableau 3.19) tout en donnant la possibilité de particulariser l'importance de l'influence de chaque parent sur la variable fille concernée (cf. partie 3.3.2.1).

	Structure n°1	**Structure n°2**	**Structure n°3**
Facteurs organisationnels	7	7	7
Items	18 à 72	9	18 à 72
Préparation	4	5 à 11	5 à 11
Réalisation	5	6 à 12	6 à 12
Clôture	3	4 à 10	4 à 10
Efficacité de l'action	4	4	4
Total	**41** à **95**	**35** à **53**	**44** à **116**

TAB. 3.19 – Nombre de paramètres à spécifier (méthode des facteurs de dégradation)

La limitation de la méthode de quantification par niveau de vraisemblance de type (a)[21] ne vient pas du nombre de paramètres à définir (qui est quasiment identique à celui nécessaire dans l'approche par facteur de dégradation), mais de l'impossibilité de pouvoir spécifier l'influence particulière d'un parent sur la variable fille concernée.
La limitation de la méthode de quantification par niveau de vraisemblance de type (b) vient du nombre accru (voire ingérable) de paramètres à définir[22].

3.3.2.3 Implantation des tables de probabilités conditionnelles

Les premières variables à définir dans cette partie du modèle, en considèrant la structure n°3, sont les facteurs organisationnels pathogènes. Ces variables constituent les nœuds racines du réseau qui, comme nous l'avons précisé dans la partie 3.2.3.4, sont spécifiées à l'aide de jugements d'experts et du retour d'expérience à disposition.

La distribution *a priori* sur ces variables racines peut prendre une des formes suivantes :
- Une distribution uniforme sur les différentes modalités de la variable, si aucune connaissance n'est disponible *a priori*.
- Une distribution quelconque, s'il existe une certaine connaissance *a priori* (exemple de question à aborder : Dans la configuration organisationnelle étudiée, quelle est la probabilité d'apparition du caractère dégradé de cette variable racine ?).
- Une quasi-certitude sur l'état dégradé (ou non dégradé) de la variable, si l'on considére qu'*a priori* la situation est critique (ou satisfaisante).

L'évolution de l'état des autres variables de cette partie du modèle (les items, les phases, et l'efficacité de l'action humaine) est définie par la combinaison de facteurs de dégradation (dont le principe a été présenté précédemment).

Nous allons à présent aborder la manière de construire les tables de probabilités conditionnelles associées à ces variables.

21. Cette démarche conditionne l'aggravation de l'état de la variable fille au nombre de parents étant dans un état dégradé.

22. Notons que cette méthode est la moins restrictive des trois en ce qui concerne la particularisation de l'importance de chaque influence. En effet, elle permet de définir une règle particulière pour chaque combinaison de l'état des parents.

En ce sens, nous proposons de généraliser, pour une variable influencée par n variables parents, la formulation particulière présentée dans la partie 3.3.2.1, et ce à partir des principes généraux énoncés dans la partie 3.2.1.2 concernant les portes de type « noisy-OR » et « noisy-AND ».
L'intérêt de ces portes est qu'elles permettent de traduire le fait que même si l'un des parents de la variable étudiée se trouve en état de non fonctionnement, alors il existe une probabilité pour que le composant associé fonctionne correctement. Cela correspond au fait que le système est en mesure de maintenir un certain niveau de fonctionnement, ou de se reconfigurer, et ce en présence de défauts particuliers.

Soit Y une variable, et $X = \cup X_i$, l'ensemble des parents de Y (avec $i = 1, 2, 3, ..., n$).
On définit par :
- $\bar{y}$, la modalité non dégradée de la variable Y (et par y, sa modalité dégradée).
- $\bar{x_i}$, la modalité non dégradée du parent X_i (et par x_i, sa modalité dégradée).
- $X_k \subseteq X$, le sous-ensemble des parents de Y qui sont dans un état dégradé.
- $\alpha_{i-Y} \in [0, 1]$, l'influence de l'état dégradé du parent X_i sur l'état non dégradé de la variable Y.

Concernant la probabilité initiale de l'état non dégradé de la variable Y (*i.e.* sachant l'état non dégradé de l'ensemble des parents X), au lieu de la fixer à la valeur 1, nous proposons d'introduire une incertitude. La présence de cette incertitude se justifie car les variables concernées dans cette partie du modèle représentent des caractéristiques des comportements humain et organisationnel.

Nous nous basons donc sur les spécificités des portes du type « leaky noisy-OR (ou AND) » (cf. partie 3.2.1.2) pour définir cette probabilité initiale :

$$P(\bar{y}|\bar{x_1}, \bar{x_2}, ..., \bar{x_n}) = a_0 \quad (avec\ a_0 \in [0, 1]) \tag{3.8}$$

La probabilité de l'état non dégradé de la variable Y, sachant l'état dégradé du i^{ime} parent, se définit de la manière suivante :

$$p_i = P(\bar{y}|\bar{x_1}, \bar{x_2}, ..., \mathbf{x_i}, ..., \bar{x_n}) = a_0 \times \alpha_{i-Y} \quad (avec\ \alpha_{i-Y} \in [0, 1]) \tag{3.9}$$

Enfin, à partir de [Onisko *et al.*, 2001], il est possible de définir la probabilité de l'état non dégradé de la variable Y sachant $X_k \subseteq X$:

$$P(\bar{y}|X_k) = a_0 \prod_{i:X_i \in X_k} (\frac{p_i}{a_0}) = a_0 \times \prod_{i:X_i \in X_k} \alpha_{i-Y} \tag{3.10}$$

La construction de la table de probabilités conditionnelles de la variable Y est automatisée par l'utilisation de la structure « leaky noisy », et se base sur le principe suivant : pour les n variables parents de la variable fille Y, toute la combinatoire précédente est multipliée par le facteur d'aggravation correspondant (cf. figures 3.19 et 3.20).

Cette règle permet la représentation de toutes les règles de dégradations relatives à ce parent, tout en limitant le nombre de paramètres nécessaires à la quantification [23].
Nous illustrons la construction d'une telle table au travers du tableau 3.20 et de la figure 3.21.

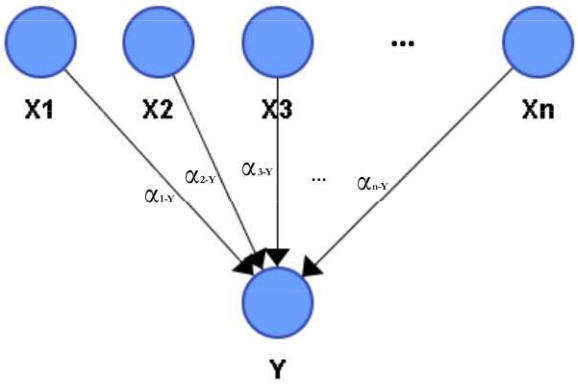

FIG. 3.19 – Modèle général d'une porte de type « noisy-OR »

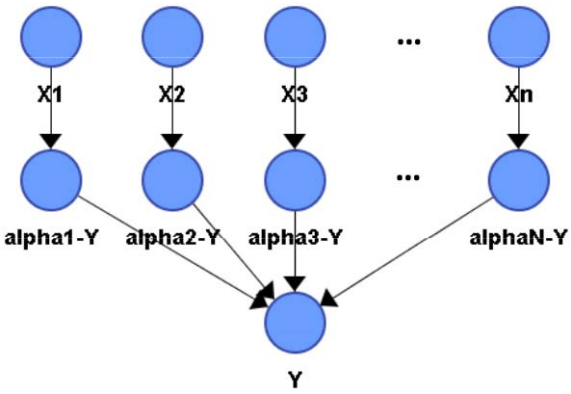

FIG. 3.20 – Modélisation directe d'une porte de type « noisy-OR »

Du fait de la complexité des modèles proposés dans notre approche, nous utilisons la modélisation décrite dans la figure 3.19. En effet, la modélisation proposée dans la figure 3.20, est certes plus intuitive, mais ne peut être implantée pour des modèles de grandes tailles où les interactions entre variables sont nombreuses.

Xn	**...**	**X3**	**X2**	**X1**	**Y**	
					Non Dégradé (ND)	**Dégradé (De)**
ND	ND	ND	ND	ND	a_0	1-a_0
ND	ND	ND	ND	**De**	a_1	1-a_1
ND	ND	ND	**De**	ND	a_2	1-a_2
ND	ND	ND	**De**	**De**	a_3	1-a_3
ND	ND	**De**	ND	ND	a_4	1-a_4
ND	ND	**De**	ND	**De**	a_5	1-a_5
ND	ND	**De**	**De**	ND	a_6	1-a_6
ND	ND	**De**	**De**	**De**	a_7	1-a_7
...	...	...	...	...	...	...
De	ND	ND	ND	ND	a_p	1-a_p
De	ND	ND	ND	**De**	a_{p+1}	1-a_{p+1}
...	...	...	...	...	...	...
De	**De**	**De**	**De**	**De**	a_{2^n-1}	1-a_{2^n-1}

TAB. 3.20 – TPC d'une variable caractéristique d'une action humaine (item, phase, efficacité)

23. En effet, le nombre de paramètres nécessaires à la quantification est linéaire au nombre de parents de la variable concernée.

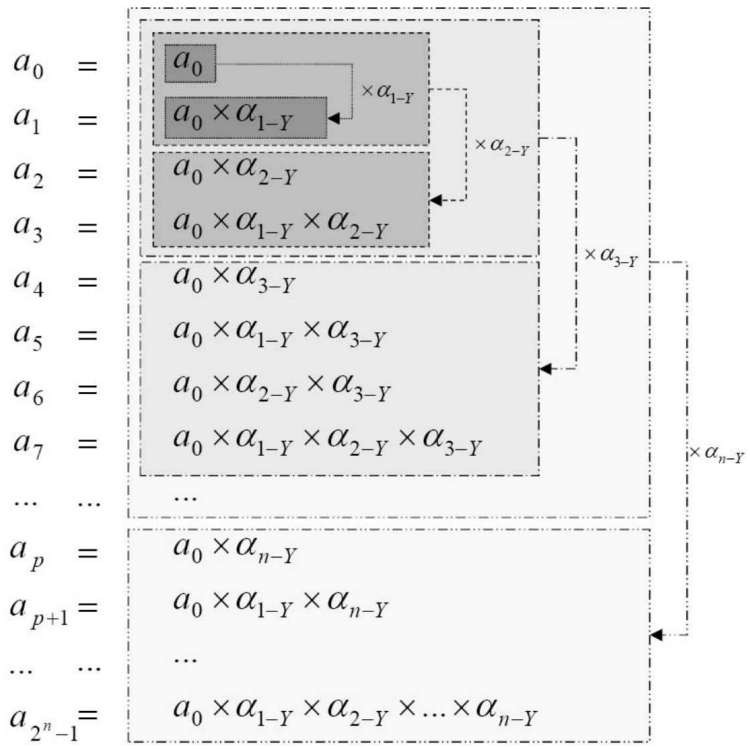

FIG. 3.21 – Structuration du principe de dégradation

3.4 Conclusions

Dans ce chapitre, nous avons abordé les aspects relatifs à la modélisation des principes de structuration des connaissances développés dans le deuxième chapitre de ce mémoire.
Notre méthodoloqie se base sur l'hypothèse que toute démarche de modélisation nécessite l'utilisation d'outils supports qui soient adaptés aux spécificités des systèmes considérés, et qui permettent de répondre aux finalités de la problématique dans laquelle s'inscrit cette démarche.
Ainsi, du fait de la complexité des systèmes considérés dans notre approche (nombre de variables, structures d'influences, connaissances de nature différentes à intégrer ...), et de la nécessité d'estimer quantitativement les risques associés aux scénarios étudiés, nous avons opté pour l'utilisation des réseaux bayésiens.
Notre choix se base, notamment, sur une récente analyse bibliographique ([Medina Oliva *et al.*, 2009]) qui a permis de montrer que les réseaux bayésiens, du fait de leurs spécificités, sont de plus en plus utilisés dans les problématiques d'analyses de risques de systèmes complexes. En effet, ce formalisme permet :
- de s'abstraire de certaines hypothèses ne pouvant pas toujours être respectées pour des systèmes complexes,
- de simuler et diagnostiquer des situations particulières sans utiliser d'outils supplémentaires et sans induire des temps de calculs importants,
- de représenter, par ajout de la variable « temps », des chaînes de Markov.

Connaissant les spécificités de l'outil support à notre démarche de modélisation, nous proposons une approche qui se décompose en deux principales étapes : la construction qualitative du modèle de risque, et la construction quantitative de ce modèle. Ces deux étapes sont

elles-mêmes scindées en sous-étapes, afin de pouvoir se focaliser sur la modélisation des parties du système ayant des caractéristiques similaires : les nœuds-papillons, les barrières de défense, et les aspects humains et organisationnels.
La construction qualitative du modèle de risque s'attache à développer la structure des différentes dimensions du système représentées dans ce modèle. Cette structure porte d'une part sur l'identification et la modélisation des influences existantes (de manière générique) entre les variables du modèle, et d'autre part sur les modalités (également génériques) nécessaires à la description des différents états de chacune de ces variables.
La construction quantitative du modèle de risque permet, quant à elle, de se focaliser sur les méthodes utilisées pour renseigner l'ensemble des tables de probabilités présentes dans le modèle. Ces méthodes permettent ainsi de définir, de manière générique, la forme des distributions de probabilités (*a priori*) associées à chaque nœud du modèle.
Différents travaux, portant sur la traduction d'arbres de défaillances en réseaux bayésiens ([Portinale et Bobbio, 1999], [Bobbio *et al.*, 2001]), sont utilisés comme base pour la traduction de la partie du modèle représentant les scénarios incidentels/accidentels (qui sont initialement modélisés sous forme de nœuds-papillons). Plusieurs phases successives permettent cette traduction : la construction de la structure du scénario (*i.e.* définir les nœuds du réseau bayésien et les influences présentes entre ces nœuds), la traduction des mécanismes déterministes (*i.e.* renseigner les tables de probabilités des nœuds dont l'état est obtenu par des fonctions logiques simples de type ET, OU), et la traduction des mécanismes probabilistes (*i.e.* renseigner les tables de probabilités des nœuds pour lesquels il existe une incertitude sur leur état).
Concernant la modélisation des barrières de défense, dont nous cherchons à estimer la disponibilité, plusieurs niveaux de granularité sont proposés : les modèles globaux, les modèles liés aux composants, et les modèles partiels.
Les modèles globaux décrivent les caractéristiques générales associées au deux types de barrières identifiées dans le deuxième chapitre de ce mémoire (les barrières de type SIS et les barrières de type CS).
Les modèles liés aux composants permettent de spécifier les influences des actions humaines de maintenance et/ou de conduite sur la disponibilité d'un composant.
Les modèles partiels permettent, pour des barrières multi-composants, de proposer une classification (technique, humaine, mixte) qui est fonction des modèles (liés aux composants) utilisés.
Les méthodes de quantification sont, à ce niveau, décrites pour les variables représentant la disponibilité des composants des barrières :

- La disponibilité intrinsèque du composant est fonction de données constructeurs et issue du retour d'expérience.
- La disponibilité du composant maintenu est l'actualisation de la disponibilité intrinsèque connaissant l'efficacité de l'action de maintenance considérée.
- La disponibilité du composant maintenu et conduit se définit comme l'actualisation de la disponibilité du composant maintenu connaissant l'efficacité de l'action de conduite.
- La disponibilité de la barrière représente l'agrégation des disponibilités des différents composants (maintenus et conduits) la constituant.

Enfin, pour la modélisation des aspects humains (les items, et les phases d'une action) et organisationnels (les facteurs organisationnels pathogènes), qui vise l'évaluation de l'efficacité des actions humaines (de maintenance et de conduite), nous proposons différentes structures d'influences. Le choix de l'une ou l'autre de ces structures dépend des données

à disposition pour renseigner le modèle, et des objectifs de l'analyse. La méthode de quantification proposée, pour renseigner les tables de probabilités associées aux variables de ces structures, se base sur les portes de type « noisy-OR » et « noisy-AND ». L'utilisation de ce type de portes permet, par la définition de facteurs spécifiques (de dégradation dans notre cas), de particulariser chacune des influences du modèle et de cumuler ces influences, tout en limitant le nombre de paramètres à spécifier.

L'application de cette démarche de modélisation permet de construire un modèle de risque global pouvant être utilisé pour décrire et comprendre une situation observée (analyse de la structure d'influences des variables du modèle), et/ou pour probabiliser les risques (inférence à partir des tables de probabilités conditionnelles) associés à cette situation [Léger *et al.*, 2009].
Comme tout modèle, il offre une vision partielle de la réalité au sens ou certains aspects ne sont pas représentés (comme par exemple les aspects résilients des organisations). Mais, en l'état, il se base sur un ensemble de représentations exhaustives et partagées (actuellement) dans chacune des disciplines concernées. Ces représentations pourront évoluer, et être complétées par de futurs travaux[24]. Les résultats de ces travaux pourront alors enrichir notre démarche méthodologique en permettant la représentation de nouveaux pans de la réalité.

Notons également que, pour l'analyse de cas particuliers, les méthodes et modèles développés peuvent être adaptés en fonction des objectifs de l'analyse, et des moyens à disposition.
Ainsi, différentes déclinaisons opérationnelles de la démarche générique proposée dans ce chapitre ont été développées par EDF et par l'INERIS en fonction des particularités des systèmes analysés.
Ces adaptations portent principalement sur la réduction du nombre de variables (ou niveaux) à considérer dans la modélisation, et/ou sur le choix des facteurs multiplicatifs de l'échelle d'élicitation d'avis d'experts (modification des valeurs quantifiées de l'échelle) et/ou sur la simplification de cette échelle (réduction du nombre de modalités).

A ce stade, la faisabilité de la démarche et la validité des méthodes et modèles associés n'ont pas encore été montrées. Afin d'étudier ces différents points, nous proposons, dans le chapitre suivant, une application complète de notre méthodologie à un cas industriel réel. Cette mise en pratique permettra, d'une part de proposer une particularisation des mécanismes et modèles développés de manière générique, et d'autre part d'identifier les limites potentielles actuelles de notre approche.

24. Ces travaux sont actuellement, ou seront, réalisés par des experts de la discipline concernée.

Chapitre 4

Application de la méthodologie à un cas industriel

Dans les deux précédents chapitres, nous avons développé une méthodologie permettant l'intégration et la modélisation des dimensions technique, humaine et organisationnelle d'un système dans une démarche d'analyse de risques.
Afin de démontrer la faisabilité de cette méthodologie et de valider les modèles associés, nous proposons d'appliquer ces développements à un cas industriel réel. En ce sens, le présent chapitre décrit la mise en œuvre de cette approche d'analyse de risques intégrée sur un scénario critique d'une installation classée.
Nous proposons d'appliquer notre démarche d'intégration sur ce scénario en suivant les étapes développées dans les chapitres précédents, à savoir :

- L'extraction et la formalisation des connaissances (techniques, humaines et organisationnelles) relatives au scénario considéré. Cette première phase se traduit par un positionnement du système dans son contexte industriel, puis par une présentation de l'installation technique étudiée, et enfin par une restitution des informations obtenues sur site concernant la situation humaine et organisationnelle spécifique à cette installation.
- La structuration de l'ensemble de ces connaissances. Cette étape se traduit par la représentation du scénario étudié sous forme de nœud-papillon [Andersen *et al.*, 2004], et par la particularisation de la configuration humaine et organisationnelle pour certaines actions de maintenance (réalisées sur des composants techniques de barrières).
- Et enfin, l'unification de ces dernières via le modèle de risque. Cette dernière phase vise à modéliser ces connaissances (nœud-papillon, barrières, configurations humaines et organisationnelles associées) dans un réseau bayésien, et à proposer une quantification du modèle ainsi obtenu à partir des informations à disposition.

La dernière partie de ce chapitre est consacrée à l'analyse des résultats fournis par le modèle, et ce dans différentes configurations. Le premier cas proposé a pour objectif de présenter les résultats obtenus en utilisant les données récoltées lors des analyses sur site ; alors que les autres cas permettent d'identifier les comportements et de tester la robustesse du modèle lorsque l'on modifie certaines distributions initiales (notamment celles associées aux actions humaines et à l'organisation) ou les valeurs quantifiées des modalités de l'échelle d'élicitation d'avis d'experts.
Ces mises en application permettent d'apporter un ensemble de conclusions quant aux actions prioritaires à mener sur le système (dans un objectif de sûreté), et sur les possibilités, la validité et les limites du modèle de risque ainsi construit.

4.1 Présentation du contexte industriel

Pour comprendre les spécificités de l'installation étudiée, il est tout d'abord nécessaire de présenter le contexte dans lequel évolue le système de production. En effet, la présentation de ce contexte permet de donner des précisions concernant le métier de l'industriel, les particularités du process de production et les dangers majeurs identifiés. Ces précisions sont importantes pour pouvoir positionner le sous-système considéré dans la chaîne de production et identifier son importance au regard de la sûreté.

4.1.1 Informations générales sur le contexte industriel du cas d'étude

Le site industriel étudié, que nous nommerons « site industriel X » (dans un souci de confidentialité), dont les activités se positionnent dans l'industrie chimique, appartient à un groupe de dimension mondiale, et emploie environ 80 personnes.
Il produit des granulés [1], à hauteur de 90 kilotonnes par an, et à partir de trois matières premières principales :
- Le produit « a », qui est un produit stable aux températures usuelles de stockage, de manipulation et d'emploi, mais qui reste malgré tout très volatil, et doit donc être manipulé en atmosphère ventilée exempte de flamme ou point chaud.
- Le produit « b », qui est un composé au pouvoir réactif élevé et qui réagit facilement.
- Les produits « c » [2], qui sont des composés utilisés comme accélérateurs, activateurs, catalyseurs de réactions chimiques.

Du fait de cette activité, l'installation considérée est classée et soumise à autorisation avec servitude (SEVESO seuil haut, [European Council, 1997]).
Par ailleurs ce site a obtenu les certifications suivantes (du fait d'une culture de sûreté partagée par les différents acteurs impliqués) :
- ISO 9001 [ISO, 2000], pour la gestion de la qualité,
- ISO 14001 [ISO, 2004], pour la protection de l'environnement,
- OHSAS 18001 [OHSAS, 1999], pour la gestion de la santé et la sécurité dans le monde du travail.

Et en ce qui concerne la prévention des risques majeurs, il met en œuvre un Système de Gestion de la Sécurité (SGS), conformément à l'arrêté du 10 mai 2000 [MEDD, 2000].

4.1.2 Le process de production

La fabrication se déroule en trois phases : la réaction chimique, le traitement intermédiaire, et le traitement de surface [3] (cf. figure 4.1), qui sont présentées dans les parties suivantes.

1. Dans ce secteur d'activité, le diamètre du produit fini peut varier de 0,2 à 1 mm selon l'application de destination.
2. La présence de ces produits peut créer de graves dangers d'incendie et d'explosion.
3. Pour aboutir à la forme finale, le produit doit être calibré pour obtenir les granulométries requises, et traité pour lui donner des caractéristiques et qualités spécifiques.

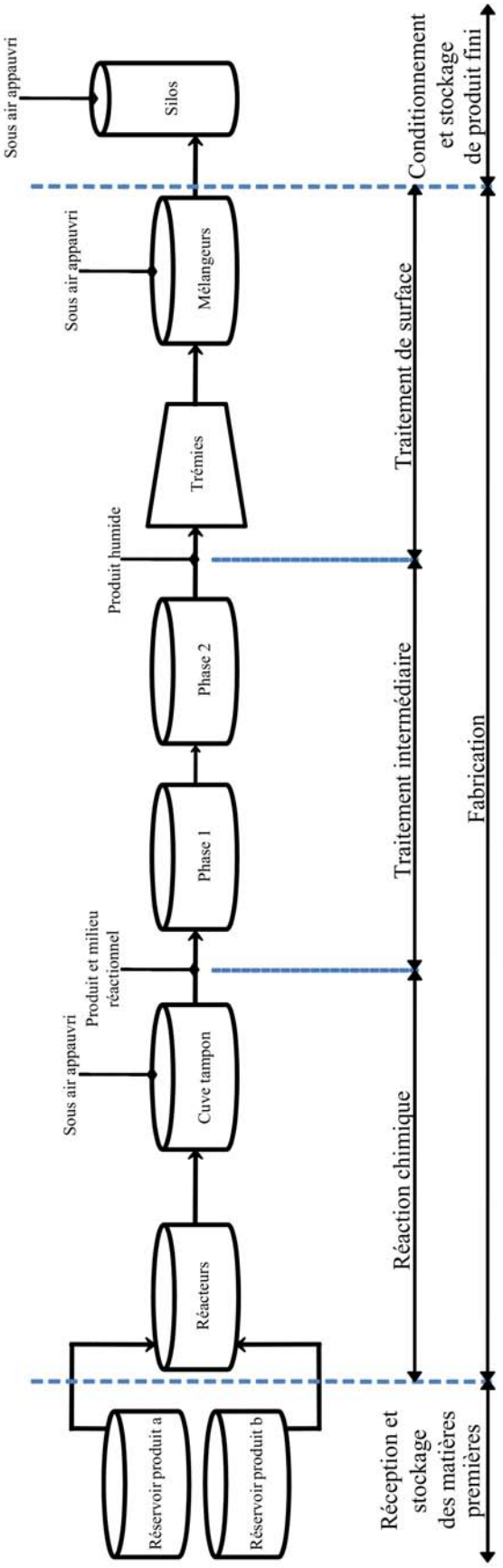

FIG. 4.1 – Les étapes de fabrication des granulés

4.1.2.1 La réaction chimique

De manière générale, la réaction de chimique considérée est lente à température ambiante. C'est pourquoi, elle est très souvent accélérée par action directe de la lumière, de la chaleur ou d'agents chimiques divers. Ce type de réaction est fortement exothermique et peut être la cause d'une élévation dangereuse de pression, lorsqu'elle se produit dans des récipients fermés.

En phase préliminaire, avant chauffage, les principaux réactifs sont chargés dans le réacteur, après avoir été préalablement pesés, dans l'ordre suivant :
(1) Les produits réactifs : le produit « b » (principal réactif), le milieu réactionnel qui permet de contrôler la réaction et d'obtenir le produit sous forme de granulés, les initiateurs (produits « c ») pour démarrer la réaction, l'additif de réaction.
(2) Les autres composés réactifs sont introduits en quantité relativement infime.
(3) Les autres matières premières.
Le réacteur est ensuite chauffé à la vapeur pour faire réagir le produit « b ».
Pendant la réaction chimique, la température est contrôlée. La réaction est effectuée dans un milieu réactionnel spécifique pour permettre un meilleur contrôle et limiter le risque d'emballement thermique.
Lorsque la réaction chimique est terminée, le produit « a » est introduit en direct après avoir été préalablement pesé. Cette phase ne présente pas de risque d'emballement thermique.
Lorsque cette phase est achevée, le réacteur est refroidi puis vidangé (par gravité) vers des cuves tampons sous pression d'air appauvri en oxygène.
Ces cuves tampons, contenant les granulés dans le milieu réactionnel, sont agitées et alimentent en continu les chaînes de finition. Les granulés humides passent ensuite dans un filtre ou tamis où les grosses particules sont stoppées et éliminées.

4.1.2.2 Le traitement intermédiaire

La phase 1 de ce traitement a pour objectif de séparer le milieu réactionnel des granulés. Le principe est le suivant : les granulés humides sont introduits dans un cylindre, puis ils sont soumis à un courant d'air à température ambiante. Les granulés les plus fins passent ensuite dans un cyclone ou ils vont être séparés de l'air transporteur. Les plus fins sont séparés par un filtre et récupérés par décolmatage puis vendus ou recyclés.

Les granulés sont ensuite dirigés, par vis sans fin puis par voie pneumatique, vers la phase 2 dont l'objectif est de séparer physiquement les produits afin de les sélectionner selon leur granulométrie. Sur le circuit de vis sans fin, il est introduit un produit antistatique permettant d'augmenter le pouvoir isolant du produit fini.

4.1.2.3 Le traitement de surface et le conditionnement

En sortie de la phase 2, les granulés sont introduits gravitairement dans un mélangeur où ils sont mis en contact avec des produits solides. Le mélange est ensuite vidangé gravitairement dans une trémie qui alimente une ligne de conditionnement ou les silos de stockage.

Le produit fini est livré chez les clients en octabin [4]. Ce conditionnement est réalisé depuis un local spécifique renfermant six silos de stockage qui alimentent par gravité six postes de

4. Emballage carton à forme octogonale avec à l'intérieur une sache plastique.

conditionnement. Le stockage des produits finis est réalisé dans trois magasins de stockage où ils sont acheminés ou repris pour expédition par chariot élévateur.

4.1.3 Le risque Explosion

Au cours des opérations industrielles conduisant à l'évaporation de liquides inflammables ou à la mise en suspension de produits combustibles à l'état pulvérulent[5], une explosion a lieu dès lors que six conditions sont réunies simultanément (cf. figure 4.2, [INERIS-MEDD, 2008]) : trois concernent le produit (l'évaporation ou mise en suspension, le domaine d'explosivité, et la présence de produit combustible) et trois autres sont relatives au milieu et à l'environnement (la source d'inflammation, la présence d'oxygène, et le confinement).

Lorsqu'une condition manque parmi celles-ci, hormis celles du triangle du feu (présence simultanée d'un combustible, d'un comburant et d'une source d'inflammation), l'explosion n'a pas lieu, toutefois l'inflammation et l'incendie qui en résultent ne seront pas évités.

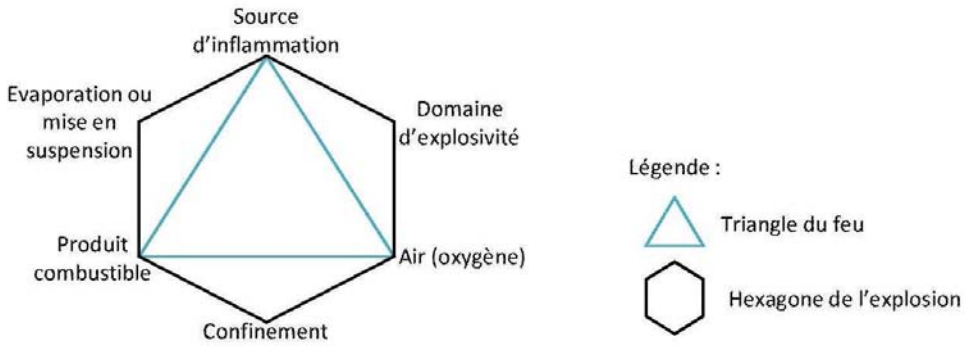

FIG. 4.2 – Hexagone de l'explosion et triangle du feu

Ces caractéristiques sont décrites dans les parties suivantes.

4.1.3.1 Présence d'un produit combustible

Il est admis que les explosions de poussières intéressent les solides finement divisés, de dimension inférieure à 300 μm. On peut aussi souligner la présence, dans certaines conditions de température et de pression, de vapeurs inflammables issues de l'évaporation de liquides inflammables. Lorsque ces deux types de produits combustibles sont présents simultanément dans un mélange air-poussière-vapeur, il en résulte un mélange hybride poussière-vapeur. Cette situation existe chez l'industriel X, qui manipule de fines particules de produit fini en présence de produit « a » émanant du produit fini.

5. État d'un produit, composé ou matériau sous forme de poudre.

4.1.3.2 Source d'inflammation

Les sources d'inflammation à considérer, internes ou externes au procédé, peuvent être classées en deux catégories :
- Les sources d'inflammation continues, comme les surfaces chaudes, qui peuvent provenir de surfaces de moteurs ou de pièces en mouvement s'échauffant par friction.
- Les sources d'inflammation instantanées, c'est le cas par exemple des étincelles électriques, électrostatiques ou mécaniques.

En ce qui concerne les vapeurs des produits « a » et « b », dont les énergies minimales d'inflammation sont inférieures à 1mJ, les étincelles électrostatiques, électriques et mécaniques sont susceptibles d'enflammer les atmosphères explosives (ATEX[6]) résultant de leur mélange avec l'air. L'inertage du process, qui consiste à éliminer l'oxygène présent dans une installation et à le remplacer par de l'azote, est la solution préconisée par les DRIRE[7] pour prévenir la formation de telles ATEX.

4.1.3.3 Domaine d'explosivité, Présence de comburant et Confinement

Le domaine d'explosivité d'un produit combustible est caractérisé par la concentration de ce produit pouvant donner lieu à une explosion. Il est défini par ses limites inférieure (LIE[8]) et supérieure (LES[9]) d'explosivité du produit dans l'air.

Le comburant, nécessaire à l'incendie ou à l'explosion, est souvent représenté (dans le cas des procédés fonctionnant sous air) par l'oxygène présent dans l'installation.

Le confinement est présent dans les procédés complètement ou partiellement fermés (capacités, silos ...).

4.2 Présentation du scénario étudié

Du fait de la présence dans une zone confinée d'une grande quantité de produit à l'état pulvérulent, de produit facilement inflammable (le produit « a ») et d'opérateurs intervenant sur l'installation (pour conditionner le produit fini), le stockage de granulés à l'état alvéolaire fait partie des installations classées de ce site industriel.
Cette partie vise ainsi à présenter ces installations de stockage, les risques associés à leur exploitation et les éléments implémentés pour prévenir l'occurrence de ces risques (ou en limiter les conséquences). Ces points permettent, en considérant également les aspects présentés dans la partie précédente concernant le risque Explosion, de proposer une modélisation des scénarios étudiés sous la forme d'un nœud-papillon (comme développé dans [Andersen *et al.*, 2004]).

6. Une atmosphère explosive est un mélange avec l'air, dans les conditions atmosphériques, de substances inflammables sous forme de gaz, vapeurs, brouillards ou poussières, dans lequel, après inflammation, la combustion se propage à l'ensemble du mélange non brûlé [Parlement européen et Conseil, 2000].

7. DRIRE : Directions Régionales de l'Industrie, de la Recherche et de l'Environnement

8. Limite inférieure du domaine de concentration d'une substance inflammable dans l'air à l'intérieur duquel une explosion peut se produire [AFNOR, 1997].

9. Limite supérieure du domaine de concentration d'une substance inflammable dans l'air à l'intérieur duquel une explosion peut se produire [AFNOR, 1997].

4.2.1 Présentation de l'installation étudiée

L'installation étudiée fait partie de l'atelier de conditionnement de produit fini qui comporte six silos de stockage métalliques avec une capacité unitaire de 200 m^3 (cf. figure 4.3).

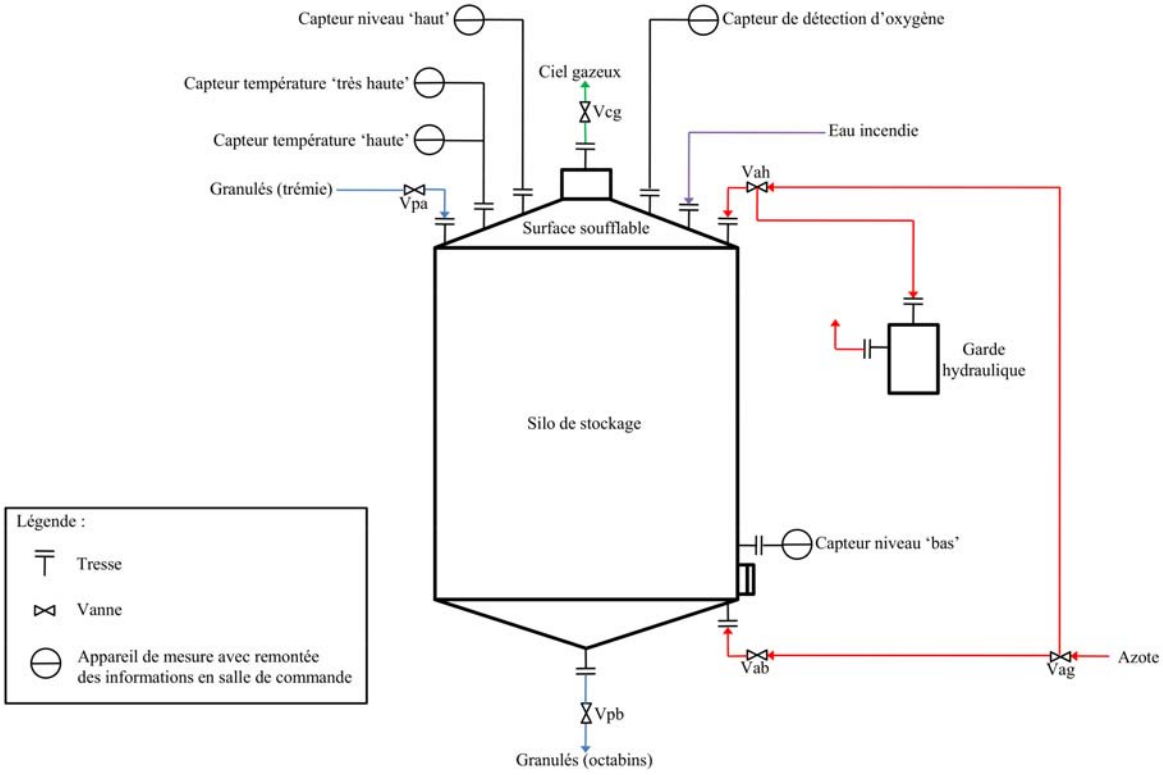

FIG. 4.3 – Schéma de l'installation étudiée : le silo de stockage de produit fini

Chaque silo est inerté par appauvrissement en oxygène, pour prévenir tout risque de formation d'ATEX par présence de produit « a » dans les silos de stockage (« azote » et « capteur de détection d'oxygène » dans la figure 4.3), et protégé par des aspersions d'eau à l'intérieur (« eau incendie ») et à l'extérieur commandées manuellement depuis le local de conditionnement (rez-de-chaussée sous le silo).

Les autres composants de cette installation ont comme fonction :
- d'éviter l'épandage de produit par débordement (le capteur de niveau haut),
- d'éviter le sous-remplissage du silo (le capteur de niveau bas),
- d'éviter les montées brutales en pression (la surface soufflable),
- d'éviter la présence de source d'inflammation électrostatique (les tresses de continuité électrique),
- de protéger le silo contre les surpressions faibles (la garde hydraulique, qui joue le rôle de soupape),
- de détecter une augmentation anormale de la température dans le silo (les capteurs de température haute et très haute).

L'ensemble des équipements présents à l'intérieur des silos sont conçus et installés de façon à ne pas constituer de source d'inflammation.

Le transport du produit fini, entre les trémies situées en aval des mélangeurs et les silos de stockage, est pris en charge par un système de transport pneumatique inerté par de l'air appauvri en oxygène. Les postes de conditionnement, en fûts ou en octabins, sont munis de systèmes d'aspiration du produit « a » (issu de l'accumulation de produit fini dans les silos).

4.2.2 Risques et phénomènes dangereux liés à l'installation étudiée

4.2.2.1 Identification des potentiels de dangers liés au procédé

L'événement redouté majeur pour l'installation de stockage de produit fini est une explosion, suivie ou non d'un départ de feu, dans le magasin et dans les silos voisins du silo étudié.

Plusieurs scénarios possibles peuvent aboutir à cette situation critique :
- En cas de défaillance d'air appauvri et avec la présence d'une source d'inflammation, les risques d'explosion de produit « a » ne sont pas à exclure. L'explosion provoquerait alors l'incendie du silo concerné.
  De plus, le ciel gazeux des silos étant commun, en cas de dysfonctionnement de cette inertage non détecté par la chaîne de mesure mise en œuvre, une explosion dans le ciel de l'un des silos est susceptible de se propager aux autres silos.
  Au regard du retour d'expérience interne à l'établissement étudié, les sources d'inflammations les plus à craindre sont les travaux par points chauds (soudure ...), la foudre et les étincelles d'origine électrostatique.
- Les poussières de produit fini peuvent être la source d'explosions si elles sont suffisamment divisées. En effet, dans le cas des produits solides, la formation d'une ATEX résulte de la mise en suspension dans l'air de particules combustibles de dimension inférieure à 300 μm.
  Or, chez l'industriel X, la granulométrie médiane du produit le plus fin présent dans les installations est de l'ordre de 280 μm.
  Ainsi tous ces produits solides sont susceptibles de former une ATEX par accumulation de charges (transport, manutention, défaut de mise à la terre de l'installation), et d'aboutir à son inflammation du fait de la présence de vapeurs dont l'énergie minimale d'inflammation est particulièrement faible.

Des opérateurs étant présents au niveau des postes de conditionnement du produit fini implantés sous ces silos de stockage, les conséquences (effets de pression locaux et effets thermiques) d'une telle explosion sont considérées comme importantes.

La combinaison et la complexité des phénomènes pouvant apparaître dans le système considéré ne permettent pas d'identifier, sans méthode d'analyse, lequel de ces scénarios est le plus probable et/ou critique. Il est par conséquent difficile de proposer, sans cette analyse, des parades permettant de contrer les scénarios les plus critiques (en terme d'occurrence et/ou de criticité).

4.2.2.2 Accidentologie

L'accidentologie, interne au site X (cf. tableau 4.1) et internationale (cf. tableau 4.2), révèle un certain nombre d'événements ayant impactés des silos de stockage de produit fini.

Année	Phénomène observé	Causes	Conséquences
1984	Incendie dans un magasin de stockage de produit fini	Indéterminées	Le magasin et 1800 tonnes de produits ont été détruits.
1997	Explosion de produit suivie d'un incendie	Électricité statique	/
1998	Début d'incendie propagé à des octabins	Travaux au chalumeau provoquant des particules de métal en fusion	Dégagement de fumées importantes

TAB. 4.1 – Accidents/incidents relatifs au stockage de produit fini du site X

Année	Phénomène observé	Causes	Conséquences
1982-1989 1991-1998 2000	Incendie de stockages de produit fini	Électriques, travaux par points chauds ...	Destruction de bâtiments
1998	Incendie et dégagement de fumées âcres	Indéterminées	Évacuation des maisons, Fermeture des routes voisines, 4h d'intervention des pompiers
2001	Démarrage d'incendie dans un silo, Emission de fumées	Décharge électrostatique (produit fini de faible granulométrie)	7 employés incommodés (avec hospitalistion), Arrêt total de la production du site (pendant une semaine)
2002	Démarrage d'incendie dans un silo	Indéterminées	Pas de victimes, Impact sur l'environnement faible, Perte de 7t de produit fini, Arrêt complet de l'unité de production

TAB. 4.2 – Accidents relatifs au stockage de produit fini dans d'autres entreprises

4.2.2.3 Éléménts Importants Pour la Sécurité (EIPS)

L'étude des phénomènes dangereux et de l'accidentologie a permis d'implémenter des EIPS [10].

La fonction de sécurité de ces derniers, consiste à :
- Prévenir tout point chaud (Matériel ATEX, Mise à la terre, Dispositif de protection contre la foudre).

10. Ces éléments peuvent être des équipements (vannes, lignes de mesures ...), dispositifs de sécurité ou groupes de dispositifs de sécurité, des opérations réalisées par un individu (formation, habilitation, fabrication, intervention ...), ou des paramètres. D'après [Salvi et Bernuchon, 2003], pour être qualifié d'EIPS, un élément doit être choisi parmi les barrières destinées à prévenir l'occurrence ou à limiter les effets d'un événement redouté central susceptible de conduire à un accident majeur.

– Prévenir les risques liés aux travaux (Procédure de permis de pénétrer dans les capacités en espace confiné avec contrôle explosimétrique).
– Maintenir une pression d'air appauvri dans le réseau (Chaîne de détection d'oxygène[11], Procédure de gestion de défaut d'inertage).

Et également des EIPS spécifiques aux silos, dont la fonction consiste à :

– Prévenir l'incendie d'un silo, lié à la formation de charges électrostatiques, et ayant pour origine un mauvais fonctionnement du système d'alimentation de l'atelier en air appauvri (Chaîne de détection d'oxygène sur les chaînes de transfert du produit fini vers les silos et à l'entrée de chaque silo, Basculement air appauvri/azote pur automatique, Prévention des points chauds, Sondes de températures avec colonnes d'arrosage intérieure et extérieure).
– Prévenir tout incendie, du à des effets dominos, dans la zone des silos (Sprinklage de la zone par des colonnes d'arrosage).

Nous allons à présent apporter quelques précisions sur les principaux systèmes importants pour la sécurité : les tresses de continuité électrique (assurant la mise à la terre des installations), les chaînes de détection d'oxygène et le système de production d'azote.

a - L'équipotentialité (ou continuité électrique)

La mise en œuvre de produits sous forme pulvérulente ainsi que des produits inflammables très volatiles rendent particulièrement importantes l'équipotentialité et la mise à la terre de l'ensemble des parties conductrices de l'installation, au moyen par exemple de tresses conductrices solidaires des équipements et démontables uniquement à l'aide d'outils.
Chez l'industriel X, l'inspection est visuelle et réalisée par l'équipe de production. Cette inspection se fait au niveau des brides et des tresses de continuité électrique.

b - Les Chaînes de détection d'oxygène

Il y a six détecteurs d'oxygène (un par silo), qui sont contrôlés et étalonnés tous les ans, et pour lesquels l'information est remontée en salle de commande de manière indépendante afin d'éliminer toute défaillance de cause commune. La redondance est, quant à elle, assurée par le fait que les silos ont un ciel gazeux commun.
Pour contrôler la teneur en oxygène dans ces silos, l'industriel X utilise ces détecteurs de la manière suivante :

– Si la concentration en oxygène est supérieure à 5%, alors l'envoi du produit fini est stoppé, sans arrêt du transport, et un évent est ouvert à l'atmosphère[12].
– Si la concentration en oxygène est supérieure à 7%, alors le système procède à une coupure automatique du traitement intermédiaire et de l'ensemble des équipements en aval (cf. figure 4.1), l'évent est ouvert, et de l'air appauvri[13] est introduit dans le silo.
– Une alarme à chaque seuil est également transmise en salle de commande.

c - Le système de production d'azote

L'azote est produit sur place par *Air Liquide* avec un système de contrôle (qui est maintenu quatre fois par an) : si un problème est détecté au niveau de la concentration en azote (concentration trop faible) alors le système bascule sur de l'azote pur.

11. La chaîne de détection est constituée d'un capteur de détection d'oxygène et d'une alarme.
12. Ceci augmente le débit d'air appauvri pour maintenir l'équilibre des pressions, et a pour effet de diluer les produits détectés.
13. L'air appauvri est produit au niveau d'une centrale qui est télésurveillée par *Air Liquide*, et une réserve d'azote pur est également présente sur le site. Le basculement air appauvri vers azote pur est automatique.

Pour qu'il y ait une perte de l'azote, il faut que le système d'*Air Liquide* soit défaillant ET qu'il n'y ait pas d'azote liquide sur le site. Et en cas de perte de cette ressource, un système d'arrosage se met en fonctionnement dans les installations (réacteurs, silos ...) afin d'éviter toute formation d'ATEX.
La fiabilité de l'ensemble de cette installation a été évalué à 99% par *Air Liquide*.

4.2.3 Modélisation du scénario technique par nœud-papillon

L'ensemble des informations données dans les sections précédentes a permis la proposition d'une modélisation sous la forme d'un nœud-papillon, [Andersen *et al.*, 2004], des scénarios pouvant aboutir à l'explosion d'un silo (et ayant un impact sur la sûreté). Cette modélisation a ensuite été validée par l'ensemble des parties prenantes de l'étude. Ces scénarios sont présentés dans les figures 4.4 et 4.5.
Dans ce modèle, les barrières (représentées par des barres verticales dans les figures 4.4 et 4.5) sont définies dans le tableau 4.3.

Label	Intitulé	Fonction
a	Respect de la maintenance	Assurer le respect des procédures ou modes opératoires de maintenance
b	Détecteur d'oxygène	Détecter une concentration excessive d'oxygène dans le système et mettre en place les mesures de sécurité prévues
c	Respect du matériel ATEX	Assurer le respect de la conformité à la réglementation ATEX pour les composants implémentés dans le système
d	Mise à la terre	Liaisons équipotentielles de masses électriques
e	Permis de feu	S'assurer d'avoir les autorisations avant de débuter tout travaux par points chauds
f	Surface soufflable	Limiter la dangerosité des conséquences en cas d'explosion dans le silo

TAB. 4.3 – Liste et fonctions des barrières

4.3 Analyse de la situation humaine et organisationnelle

Les observations présentées dans cette partie sont relatives à la situation organisationnelle du site et aux activités réalisées sur les silos. Les informations recueillies proviennent d'entretiens réalisés en binômes [14] auprès de quatre opérateurs (plus ou moins expérimentés, et appartenant à des équipes de maintenance ou de production) du site étudié, et sur la base d'un protocole d'analyse spécifique décrit dans [Farret *et al.*, 2007].

14. Ces binômes étaient constitués d'un expert technique et d'un expert organisationnel afin de sonder toutes les dimensions de la situation analysée.

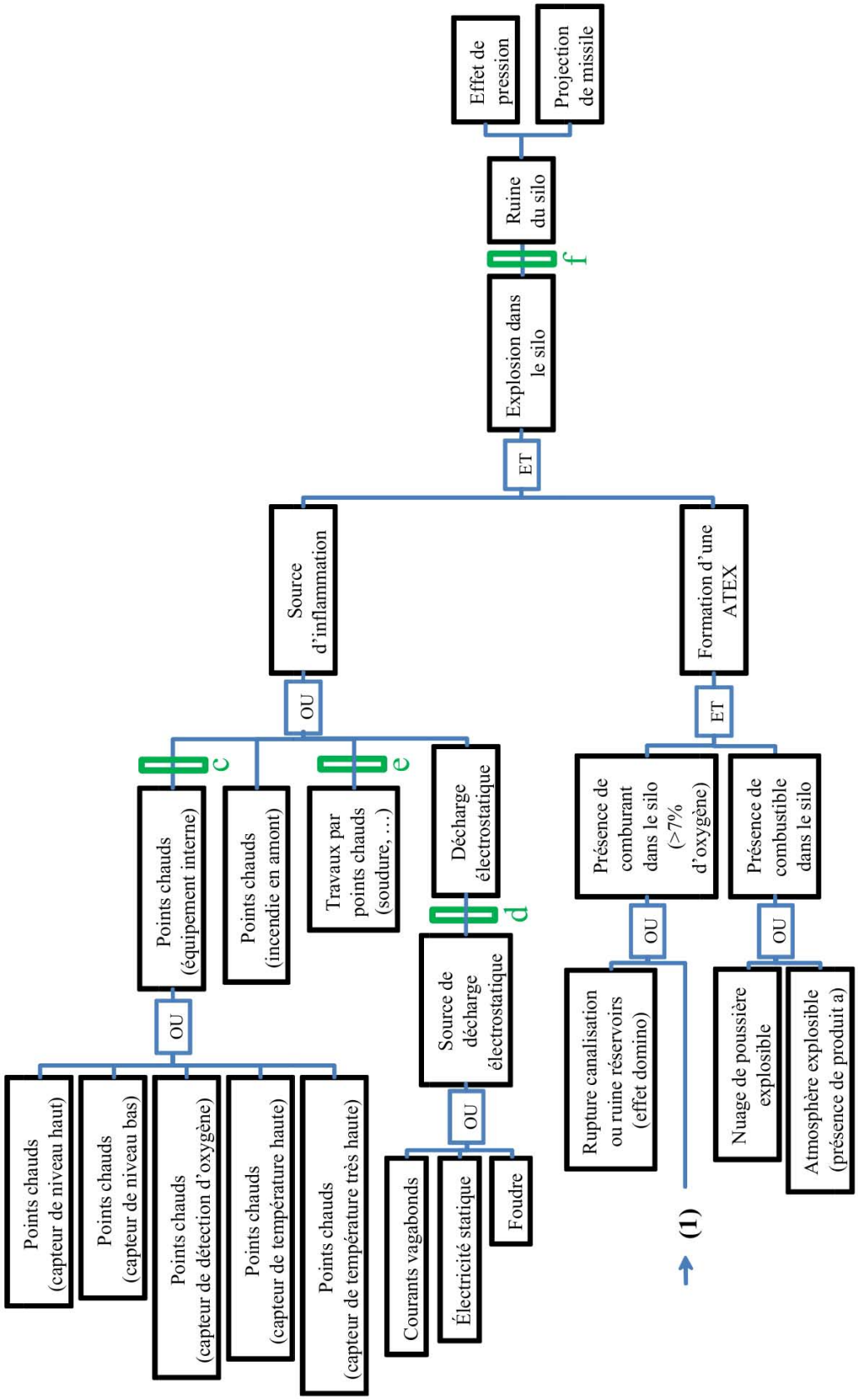

FIG. 4.4 – Représentation par nœud-papillon des scénarios menant à l'explosion d'un silo

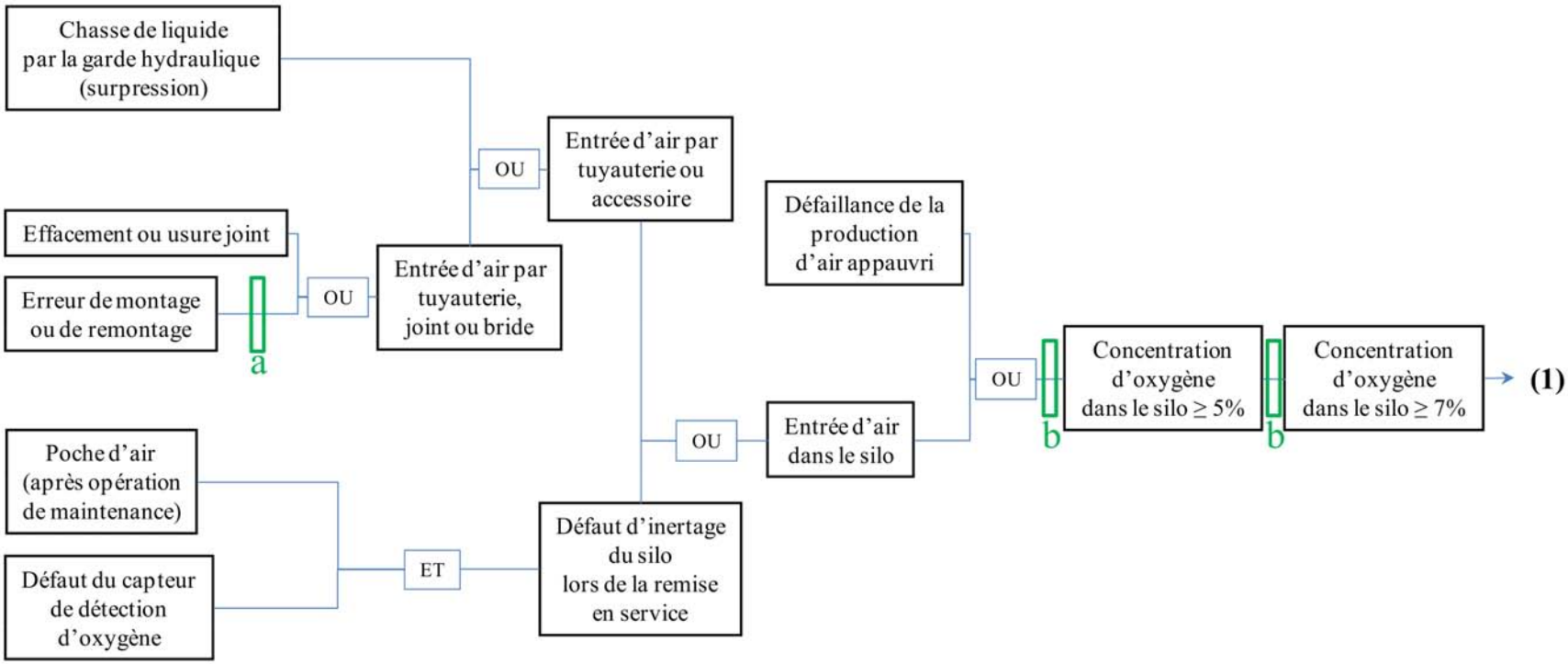

FIG. 4.5 – Représentation par nœud-papillon des scénarios menant à la présence de comburant dans un silo (autres que des effets dominos)

4.3.1 Caractéristiques de l'organisation étudiée

L'industriel a subi, il y a quelques temps, plusieurs restructurations qui ont abouti à une diminution des effectifs et à une décentralisation du management de haut niveau.

Les services concernés, pour cette analyse, sont la maintenance (une dizaine de personnes et des sous-traitants) et la production (cinq équipes travaillant en 5/8).
Le travail, au niveau de l'équipe de maintenance, s'organise de la manière suivante :
- une réunion de planification hebdomadaire permet de planifier au mieux le préventif de la semaine et les arrêts de production,
- une réunion journalière est réalisée avec l'équipe de production pour préciser ce qui va être fait dans la journée (arrêts programmés ...),
- les actions urgentes (définies dans la réunion journalière) sont traitées en priorité puis les opérateurs traitent les actions de maintenance préventive.

En ce qui concerne les équipes de production, les opérateurs sont de plus en plus polyvalents (résultant d'une décision du management visant à diversifier les activités de chaque opérateur). De ce fait, le travail s'organise de la manière suivante :
- Pour l'équipe du matin, les opérateurs participent à la réunion journalière avec l'équipe de maintenance, puis certains sont assignés à des rondes et d'autres reçoivent des consignes spécifiques, puis l'ensemble de l'équipe accueille les entreprises extérieures (signature, suivi), et démarre enfin les réacteurs.
- Pour l'équipe de nuit, les opérateurs doivent suivre un ensemble de consignes qui ont été définies au cours de la journée.

4.3.2 Modifications du fait des restructurations

Au niveau de l'équipe de maintenance, les restructurations ont ajoutées de nouvelles activités (comme les travaux neufs) à cette fonction. De ce fait, la charge de travail étant accrue, cette équipe sous-traite de plus en plus certains travaux préventifs (comme un remplacement de vanne) pour pouvoir faire ces études et cahiers des charges ; par contre la maintenance des matériels EIPS n'est pas sous-traitée.
Un premier constat apparaît alors : les interventions extérieures sont aujourd'hui plus importantes qu'avant les restructurations et ajoutent une charge de travail supplémentaire à l'équipe (en effet, lorsque la sous-traitance n'a pas toute la connaissance nécessaire, elle sollicite de l'aide auprès du personnel interne).
De ce fait, la réalisation de certaines actions préventives, dont le nombre a augmenté depuis la parution de la nouvelle réglementation ATEX ([Parlement européen et Conseil, 2000]), comme l'installation d'un nouveau parc de capteurs, prend du retard.

Au niveau des équipes de production (ou de conduite), le constat est le même (mais avec une pression plus forte) : depuis les restructurations, la charge de travail est plus importante et l'appel à la sous-traitance externe également.

Il a également été observé que certains cadres intermédiaires [15] (comme le contremaître) ont disparus. De ce fait, la communication verticale est rendue plus difficile par le départ récent d'autres cadres, comme le soulignent les opérateurs : « la chasse aux informations est plus

15. Ces cadres permettaient de faire le lien entre les opérateurs sur le terrain et la hiérarchie.

difficile », « les cadres sont beaucoup pris dans les réunions », « il y a moins de présence de l'organisation sur le terrain du fait de la disparition du contremaître », « les cadres ne connaissent pas réellement le travail des opérateurs. En ce qui concerne le travail de chef de poste, vu de l'extérieur, ça n'est pas lourd, alors que de l'intérieur ça l'est ».

4.3.3 Les silos de stockages de produits finis

Les silos ne sont pas sollicités durant la nuit ni le week-end. De ce fait, certaines personnes des équipes de production doivent quitter leur poste pour aller occasionnellement vider ces silos.
De plus, les compétences requises pour travailler aux silos semblent être moins importantes que celles nécessaires aux opérateurs de production : « ils (la direction) demandent moins aux personnes sur les silos (tâches à accomplir) qu'à ceux qui sont dans la production (travail en salle de commande, maintenance de premier niveau ... qui nécessitent des compétences spécifiques) ».

Des précisions concernant les EIPS, présents dans le scénario étudié, ont également été apportées par les opérateurs impliqués dans cette analyse :

- Les tresses de continuité électrique sont vérifiées visuellement, et non de manière métrique, par des opérateurs des équipes de production (maintenance de premier niveau).
- La délivrance des permis de feu est faite par des opérateurs formés à ce sujet. Ces permis de feu sont remplis avec (dans le cas d'une sous-traitance) ou sans l'intervenant en évaluant les risques potentiels dans la zone de travail.
- L'étalonnage des capteurs d'oxygène est annuel et réalisé via une bouteille étalon. Durant cette action, il y a un arrêt des transferts venant de la production vers le silo concerné. Cette opération est réalisée de manière indépendante pour chaque silo car les chaînes de transfert concernées lui sont spécifiques.
  L'opération se fait en binôme : un opérateur (habilité à consigner le matériel électrique) doit monter au niveau du toit du silo et isoler la cellule (par vannes manuelles d'isolement avec fin de course), et l'autre opérateur se trouve en salle de commande (il utilise des abaques de calculs avec un mode opératoire spécifique). La communication entre ces opérateurs se fait par talkie-walkie.
  La cellule est testée puis étalonnée et/ou remplacée (en cas de doute sur son état ou suivant la durée de vie constructeur).
  L'enclenchement de ces capteurs (à 5% ou à 7%) est rare (une à deux foix par an), et a notamment lieu lors du regonflage des silos (injection d'azote dans le silo pour évacuer l'air présent) après des opérations de maintenance spécifiques. En effet, il n'y a pas de vérification de l'état de ces capteurs (du fait de leur contact avec un ciel gazeux autre que l'azote, ou de la présence de poches d'air) lors de ce regonflage (cette vérification se fera lors de la prochaine visite préventive).

Enfin, et de manière générale, les opérations de maintenance sont peu formalisées (peu de modes opératoires), et à chaque action de maintenance est associée une phase de clôture de l'intervention qui est réalisée par l'opérateur (permet de recenser le déroulement de l'intervention et les problèmes éventuels dans une base de données dédiée).

4.3.4 Constats et conclusions

Le constat qui apparaît en premier lieu permet de souligner les efforts fournis par l'organisation pour intégrer la sûreté à tous les niveaux[16] du système (et conserver une culture de sûreté solide) : nombreux investissements techniques de sûreté, système de sûreté vivant, écoute du personnel et réactivité, politique de maintenance préventive en développement, suivi régulier des formations. Ces points sont favorables à la prévention et à une culture de la sûreté, mais doivent faire l'objet d'une attention particulière du fait du contexte actuel dans lequel se trouve cette entreprise.

Le deuxième constat porte sur l'augmentation de la charge de travail du personnel d'encadrement (due notamment à une baisse des effectifs et à une concurrence très présente dans ce domaine). Cette situation amène à une augmentation de l'utilisation de la sous-traitance externe, qui est sollicitée en fonction des besoins des opérateurs internes, et ceci plus particulièrement pour le service maintenance.
Cette baisse dans les effectifs amène à une disparition du personnel d'encadrement intermédiaire et rend la communication verticale plus difficile (et risque de conduire à une rupture entre le management et le personnel de terrain).
L'utilisation accrue de la sous-traitance externe combinée au manque de formalisation des modes opératoires (hormis pour les permis de feu et les habilitations électriques) risque d'aboutir à une perte de la mémoire organisationnelle.

Le troisième constat concerne la vision que portent l'ensemble du personnel du site X sur les silos. Ils sont vus comme une installation maîtrisée et sûre (par rapport à d'autres équipements), au sens où les problèmes identifiés portent plus sur la qualité des produits que sur la sûreté. Ainsi dans certaines situations critiques (pressions externes dues à la concurrence, baisse des effectifs ...), des choix peuvent être fait au détriment du silo, et/ou favoriser des actions réalisées par un personnel n'ayant pas le savoir requis.

Le quatrième constat met en exergue le manque de formalisation dans l'affectation de la fonction contrôle (de fin de chantier par exemple). En effet, il n'y a pas de contrôle explicite des actions (le compte-rendu de l'action est réalisé par l'opérateur lui-même). Cette situation peut mener à un recensement incomplet ou absent (volontaire ou non) de certains défauts apparus dans le système.

Les conclusions du premier expert organisationnel, au regard de cette situation, sont les suivantes : « Le système est encore dans un équilibre assez favorable à la prévention des accidents majeurs (et à la sûreté en général). Si le système était bien dimensionné autrefois (avec des « espaces » pour réfléchir, de la redondance, du personnel ...), il apparaît qu'aujourd'hui ce dimensionnement tend à être réduit. Le risque est d'aboutir à une situation plus dégradée, qui se sera instaurée non de manière brutale mais incrémentale sur les années, et de ce fait, sera acceptée par les uns et les autres (cette nouvelle situation sera alors devenue la norme et non plus une déviance). Ce qu'il est nécessaire de surveiller est, d'une part les petits incidents à venir (il y en aura certainement car le système semble « se tendre »), mais surtout, la mise sous pression potentielle et à venir qui sera peut être acceptée et banalisée suite à tous ces changements incrémentaux. »

16. « La sûreté est l'affaire de tous. »

Les conclusions du deuxième expert organisationnel portent sur « les caractéristiques allant dans le sens d'une fragilisation du système :
- La question de la maintenance réalisée par l'externe qui ne fait pas l'objet d'une doctrine, et est faite au coup par coup et en fonction des besoins (que l'on pourrait qualifier d'improvisation organisée). De ce fait, des personnels non formés, voire non familiarisés avec la culture de sûreté du site X peuvent intervenir.
- Les réorganisations (ou des craintes de réorganisation, ayant les mêmes effets que des réorganisations proprement dites) peuvent créer, quant à elle, une instabilité dans le système (ce qui peut entraîner une perte de vision des interlocuteurs pertinents). Or, la sûreté a besoin de repères et de stabilité. »

Ces remarques soulignent la potentialité de la présence d'une periode d'incubation [17], d'un déplacement de l'équilibre de départ, et d'une fragilisation du système pour l'avenir.

Au regard de ces observations, trois facteurs organisationnels ont été identifiés comme étant pathogènes pour la sûreté du système :
- La présence de Pressions de Productions [18] (malgré la présence d'une culture de production). En effet, la présence du caractère pathogène de ce facteur est identifiée par l'observation d'effectifs en réduction (notamment au niveau des cadres dans notre cas), d'un accroissement de la charge de travail (difficultés à consacrer du temps aux fonctions de contôles), d'objectifs stratégiques portant l'accent sur la production et les performances productives (difficulté d'arbitrer entre différentes tâches) ...
- L'affaiblissement de la Culture Organisationnelle de Sûreté [19] actuellement en place, si les changements actuels se poursuivent au fil du temps. En effet, ce facteur est identifié dans une organisation lorsque les analyses de risques ne sont pas réactualisées ou réexaminées compte-tenu de changements techniques et/ou organisationnels ou de connaissances tirées du REX, les contrôles internes sont insuffisants (voire inadaptés, inexistants, ou non pris en compte), la documentation concernant la sûreté est insuffisante ...
- L'Absence de Réexamen des Hypothèses de Conception [20]. En effet, ce facteur a pour caractéristiques une insuffisance (ou absence) dans l'analyse et l'évaluation de la gravité des défauts, un manque d'analyse globale des effets des défauts sur la sûreté ...

Des suggestions, pour pallier ces manques, ont été proposés par les experts organisationnels :
- Développer un système de veille et d'écoute (en identifiant clairement les signaux faibles, les réseaux de correspondants ...).
- Développer la formalisation des modes opératoires de maintenance et de contrôles (puis veiller à les faire vivre car le système est changeant).

17. Période durant laquelle des signes de dégradations de la sûreté s'accumulent mais restent ignorés [Turner et Pidgeon, 1997].

18. Sont considérées « Pressions de Productions », des injonctions visant à passer outre ou à volontairement ignorer certaines dimensions de la sûreté de manière à favoriser les critères de rentabilité de court terme [Dien *et al.*, 2006].

19. La Culture de Sûreté est un ensemble de connaissances, de pratiques et de valeurs partagées et soutenues de façon volontaire par l'ensemble des membres de l'organisation. Elle vise à assurer que la sûreté des installations bénéficie à tout moment (et en toute circonstance) de toute l'attention requise dans l'atteinte des objectifs de production [Dien *et al.*, 2006].

20. La conception de tout système technologique s'appuie sur la définition et sur la prise en compte d'hypothèses de dimensionnement (technique et social). Ces hypothèses sont basées sur une vision du fonctionnement futur du système. Il peut s'avérer, avec le temps, que certaines hypothèses soit deviennent caduques (*i.e.* inadaptées aux caractéristiques du nouveau mode de fonctionnement nominal), soit se révèlent fausses compte-tenu des caractéristiques réelles du mode de fonctionnement [Dien *et al.*, 2006].

– En ce qui concerne les silos, analyser plus précisément les causes de déclenchements d'alarmes à 5% (voire 7%) et les actions entreprises dans ce cas.

Ces aspects doivent à présent être analysés afin d'étudier leurs influences sur les autres dimensions du système (les opérateurs humains, et le système technique), et donc sur la probabilité d'occurrence de l'événement redouté. Cette étude vise à identifier l'ensemble des causes possibles à l'occurrence de cet événement, afin de conforter et compléter l'ensemble des solutions proposées pour pallier les faiblesses de la situation actuelle.

4.4 Modélisation du scénario sous BayesiaLab

La modélisation du scénario sous BayesiaLab[21], à partir des informations présentées dans les parties 4.2 et 4.3, se fait en plusieurs étapes. La première permet de construire la structure du modèle, et consiste à traduire le nœud-papillon du scénario en un réseau bayésien, puis à modéliser les barrières de défense, et enfin modéliser la configuration humaine et organisationnelle associée[22]. Ayant la structure du modèle, il devient alors possible de quantifier les variables de ce modèle. La quantification de ces variables consiste à définir leur distribution initiale, puis à spécifier l'importance des influences présentes dans le modèle au travers des tables de probabilités conditionnelles. Cette étape de quantification suit les règles génériques développées dans le chapitre 3 de ce mémoire.

4.4.1 Traduction du scénario modélisé par nœud-papillon en réseau bayésien

La traduction du nœud-papillon du scénario en réseau bayésien suit les règles décrites dans la partie 3.2.1 et est présenté dans la figure 4.6 (les objets présents dans cette figure sont explicités dans les figures 4.8 et 4.9). Cette modélisation par réseau bayésien a été approuvée par l'ensemble des parties prenantes de l'étude.

Les barrières **a** (respect des procédures ou modes opératoires de maintenance), **c** (respect du matériel ATEX) et **e** (permis de feu) n'apparaissent plus dans la représentation par réseau bayésien. En effet, ces barrières représentent des barrières humaines et organisationnelles. Or dans notre démarche, il est nécessaire d'identifier clairement le composant technique influencé par cette action humaine[23] (cf. partie 2.3.1).

Ces barrières (**a**, **c** et **e**) se retrouveront indirectement dans les aspects humains et organisationnels relatifs aux barrières **b** (détection d'oxygène), **d** (tresses de continuité électrique) et **f** (surface soufflable), qui sont directement représentées dans la représentation du scénario par réseau bayésien.

21. BayesiaLab est un logiciel sous licence qui permet de construire des réseaux bayésiens statiques ou dynamiques, et qui est de plus en plus utilisé en milieu industriel pour des problématiques diverses (marketing, finance, santé, automobile, gestion des risques ...).

22. Cette configuration est une particularisation justifiée de la configuration générique proposée dans le chapitre 2.

23. Une telle action ne peut pas influencer directement un phénomène physique (comme par exemple l'explosion d'un réservoir). S'il est nécessaire de modéliser une telle influence, il faudra modéliser la disponibilité du composant technique (ici le réservoir) et ensuite, ajouter les impacts des actions humaines et de l'organisation.

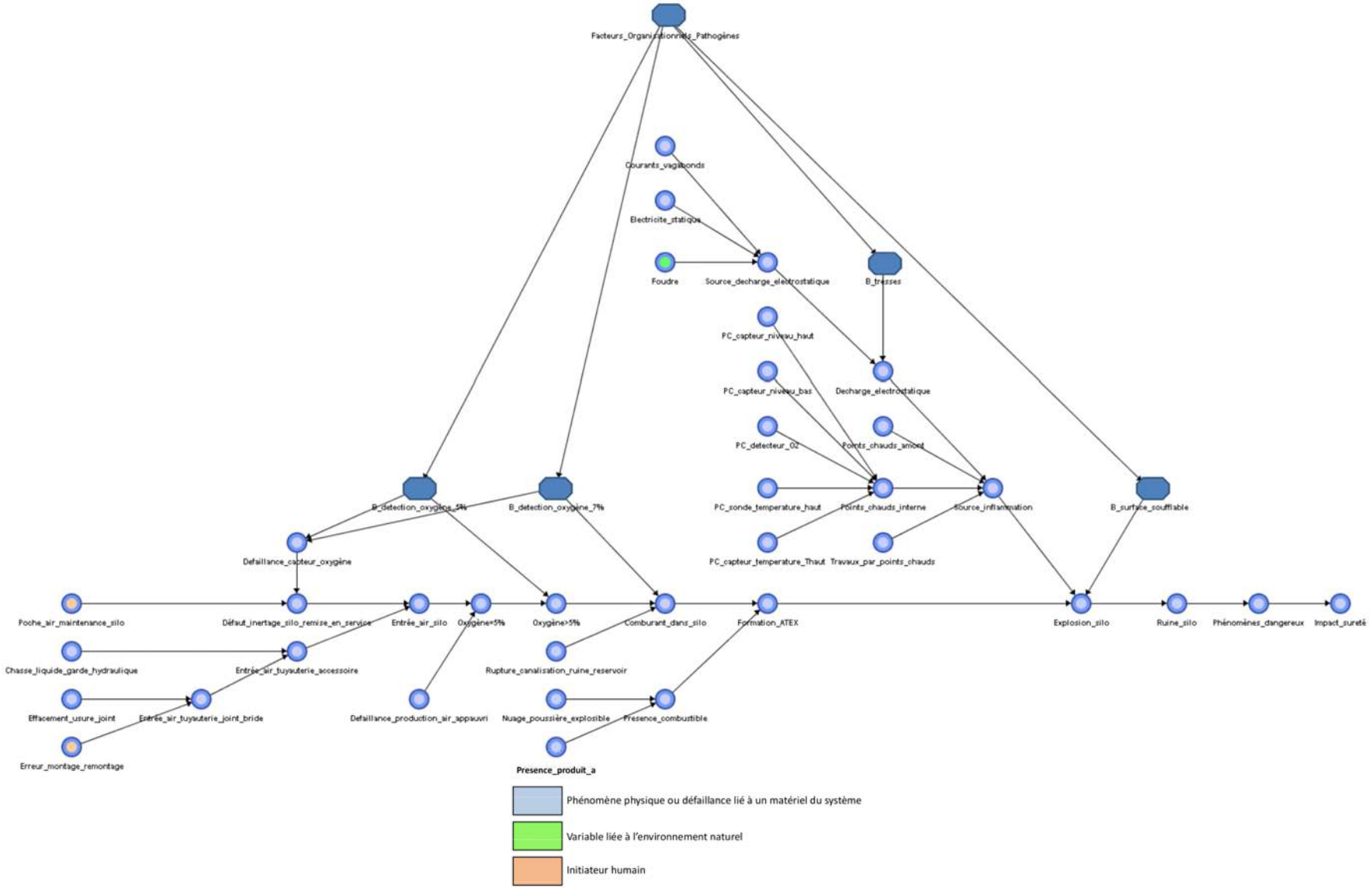

FIG. 4.6 – Représentation par réseau bayésien du nœud-papillon du scénario étudié

4.4.2 Modélisation des barrières étudiées

4.4.2.1 Les barrières

Les barrières modélisées explicitement dans le modèle réseau bayésien (**b**, **d** et **f**) sont de natures différentes (et les modèles utilisés pour les représenter le seront donc également, cf. partie 3.2.2). En effet, la barrière **b** (détection d'oxygène) est une barrière de type SIS [24], alors que les barrières **d** (tresses de continuité électrique) et **f** (surface soufflable) sont des barrières passives de type CS [25].

Ainsi, la barrière de détection d'oxygène est constituée d'un capteur de concentration (qui est étalonné pour deux seuils, l'un à 5% d'oxygène et l'autre à 7%), d'un processus de traitement (spécifique à chaque seuil, il permet d'émettre une alarme et de mettre automatiquement le système en sécurité), et d'une action finale (qui est l'ouverture d'un évent à l'atmosphère pour le seuil à 5%, complétée par l'introduction d'air appauvri dans le ciel gazeux du silo pour le seuil à 7%).

Les informations recueillies, lors des analyses sur site, pour le capteur de concentration portent sur sa disponibilité intrinsèque [26], une action de maintenance importante pour la sécurité (l'étalonnage) et les impacts organisationnels spécifiques à cette action.

Celles concernant les processus de traitement et les actions finales sont relatives à leur disponibilité opérationnelle [27].

Les informations recueillies sur site pour la barrière tresses (de continuité électrique) portent sur sa disponibilité intrinsèque, une action de maintenance importante pour la sûreté (la surveillance de la continuité électrique) et les impacts organisationnels spécifiques à cette action.

Enfin, l'information recueillie pour la barrière surface soufflable est relative uniquement à sa présence physique dans le système [28].

4.4.2.2 La configuration humaine et organisationnelle

L'information recueillie par les experts (lors des analyses sur site) se situe au niveau organisationnel du système. La configuration retenue pour modéliser ces aspects humains et organisationnels est donc une simplification de la configuration générique (présentée dans la partie 3.2.4). En effet, n'ayant pas de connaissance à apporter au niveau des items des actions humaines (mais uniquement au niveau des facteurs organisationnels), il n'y a pas de risque de découplage entre les connaissances du niveau organisationnel et celles du niveau technique (cf. figure 4.7).

24. SIS : Safety Instrumented System, constitué de trois éléments (Détection, Traitement, Action).
25. CS : Composant de Sûreté, constitué d'un seul élément.
26. C'est la disponibilité fournie par le constructeur ou issue du retour d'expérience disponible.
27. En effet, la durée limitée des analyses sur site nous a obligé à orienter nos études sur certains équipements importants pour la sûreté avec des activités de maintenance à la charge soit de l'équipe de maintenance, soit des équipes de production.
28. Les analyses sur site ne nous ont pas permis d'obtenir les informations nécessaire à l'élaboration de la configuration humaine et organisationnelle pour la barrière « surface soufflable », si ce n'est la confirmation de sa présence physique dans le système.

Rappel :
- *Les facteurs organisationnels pathogènes (**FOP**) sont les suivants : Faiblesse de la culture organisationnelles de sûreté (**COS**), Défaillance dans la gestion quotidienne de la sûreté (**GQS**), Faiblesse des organismes de contrôle (**OC**), Mauvais traitement de la complexité organisationnelle (**MT**), Difficulté à faire vivre un retour d'expérience (**REX**), Pressions de production (**PP**), Absence de réexamen des hypothèses de conception (**AR**).*
- *Les items sont les suivants : Délégation (**De**), Aides (**Ai**), Formation (**Fo**), Expérience (**Ex**), Respect du cahier des charges (**Rcc**), Facteurs d'environnement (**Fe**), Gestion collective et dynamique de groupe (**Gcdg**), Contrôle et atteinte des objectifs (**Cao**), Retour d'expérience (**Rex**).*

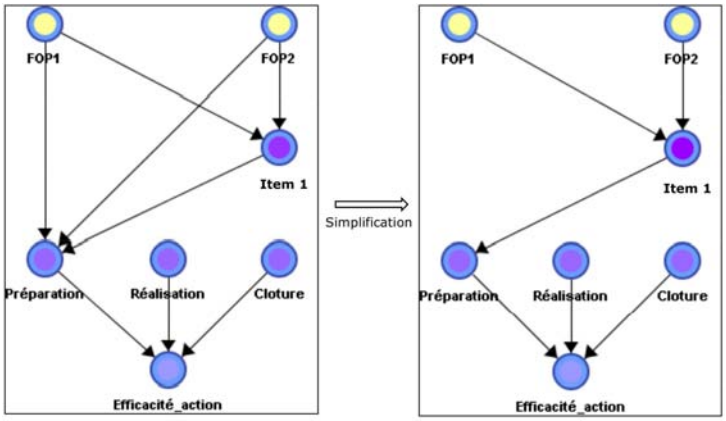

FIG. 4.7 – Configurations (générique et simplifiée) permettant de représenter les aspects humains et organisationnels du système

Les influences entre les facteurs organisationnels et les caractéristiques des actions humaines à identifier et à justifier se situent donc uniquement au niveau des items de ces actions.

Les configurations particulières relatives aux actions d'étalonnage du capteur et de surveillance des tresses, et obtenues par simplification de la configuration générique présentée dans la partie 2.3.3, sont décrites dans les tableaux 4.4 et 4.5[29].
La justification des simplifications apportées à ces configurations est présentée dans l'annexe E de ce mémoire.

4.4.2.3 Les modèles associés

Les justifications données dans la partie précédente permettent de construire les influences présentes entre les objets « Facteurs_organisationnels_ pathogènes », « Caractéristiques_ étalonnage_capteur » et « Caractéristiques_surveillance_tresses » de la figure 4.8, et sont explicitement représentées dans la figure 4.9.

29. Les cellules grisées dans ces tableaux représentent la configuration générique telle qu'elle est décrite dans la partie 2.3.3. Les signes « X » représentent la configuration particulière obtenue avec les experts organisationnels.

	COS	GQS	OC	MT	REX	PP	AR
De							
Ai	X		X		X	X	X
Fo		X			X	X	
Ex							
Rcc	X					X	
Fe					X		X
Gcdg	X	X			X	X	
Cao					X	X	
Rex	X	X			X	X	

TAB. 4.4 – Configuration humaine et organisationnelle pour l'action d'étalonnage du capteur de détection d'oxygène

	COS	GQS	OC	MT	REX	PP	AR
De							
Ai							
Fo		X			X	X	
Ex						X	
Rcc		X				X	
Fe					X	X	X
Gcdg							
Cao					X	X	X
Rex		X			X	X	

TAB. 4.5 – Configuration humaine et organisationnelle pour l'action de surveillance de l'état des tresses de continuité électrique

4.4.3 Vue globale du scénario sous BayesiaLab

La mise en commun de ces modèles partiels permet d'aboutir à un modèle global du scénario prenant en compte ses aspects techniques, humains et organisationnels, qui est représenté par la figure 4.10, et qui a été approuvée par les différents experts impliqués dans l'analyse.

4.4.4 Quantification du modèle obtenu

La quantification du modèle se fait en deux étapes principales[30] : la quantification des variables (qui consiste à en fixer les distributions initiales), puis la quantification des influences présentes dans ce modèle (qui consiste à définir des règles logiques ou opérations mathématiques permettant de faire évoluer, via les TPC[31], ces distributions initiales en fonction de l'état des parents des variables considérées).

30. Cette quantification se fait via un tableau Excel dont l'utilisation est décrite dans l'annexe F de ce mémoire.

31. TPC : Tables de Probabilités Conditionnelles

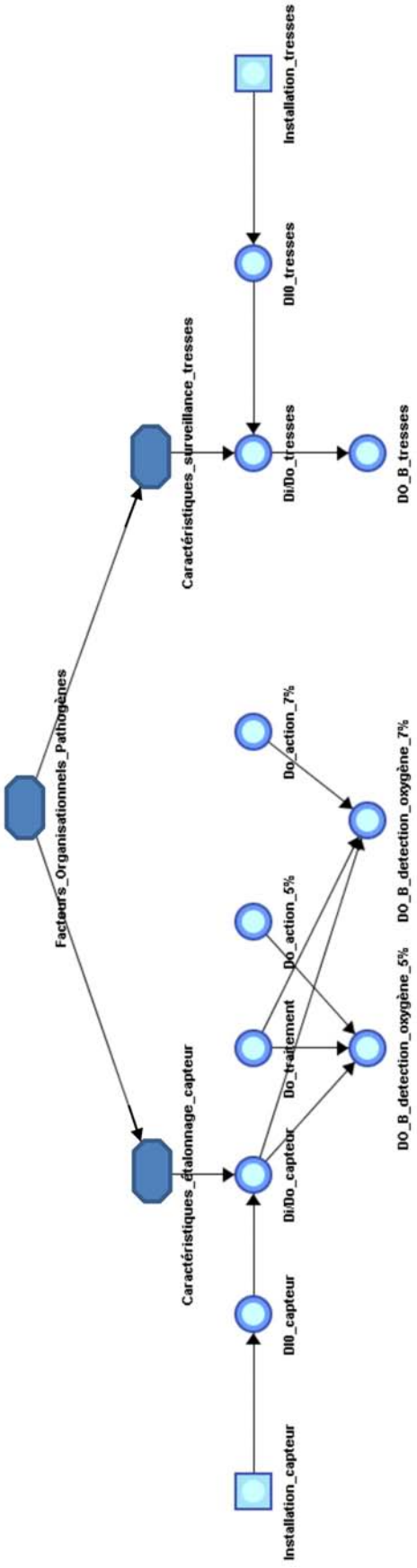

FIG. 4.8 – Modèles des barrières « détection d'oxygène » et « tresses de continuité électrique »

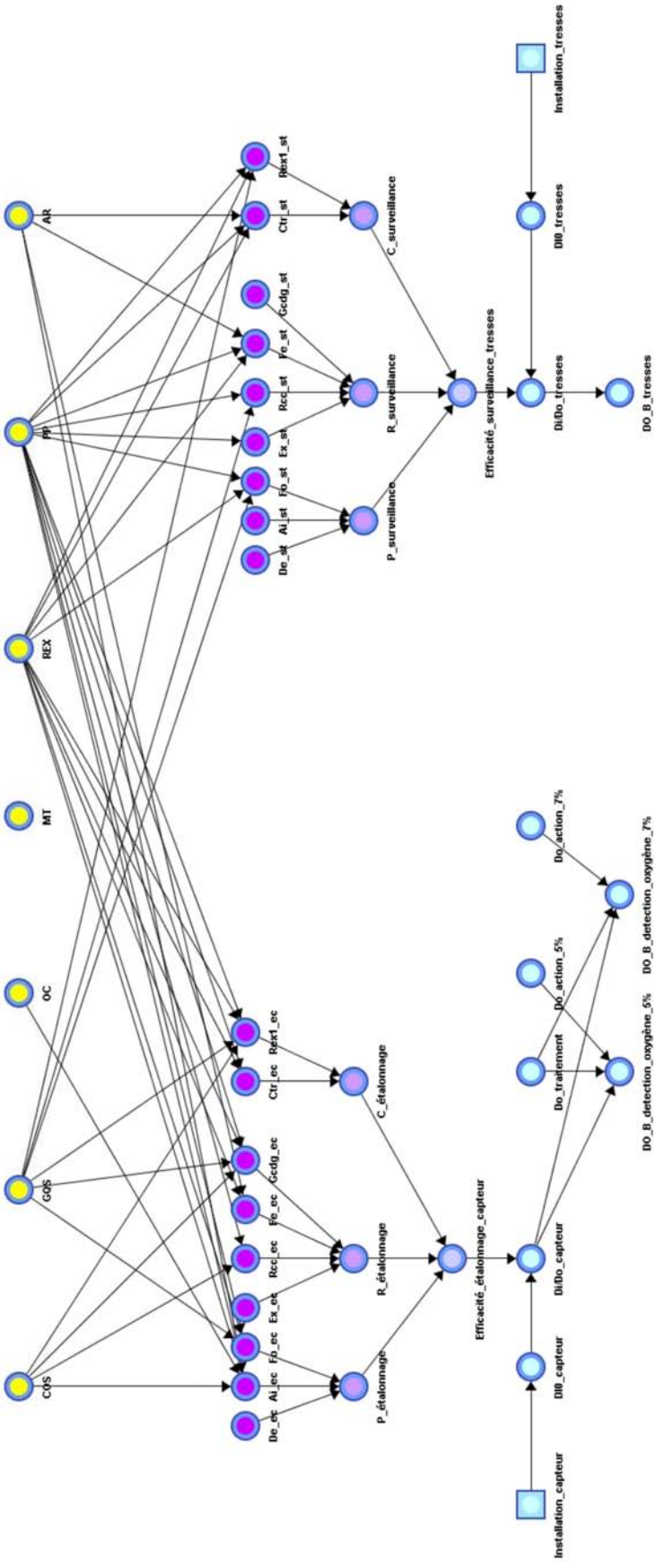

FIG. 4.9 – Configurations humaine et organisationnelle pour les barrières « détection d'oxygène » et « tresses de continuité électrique »

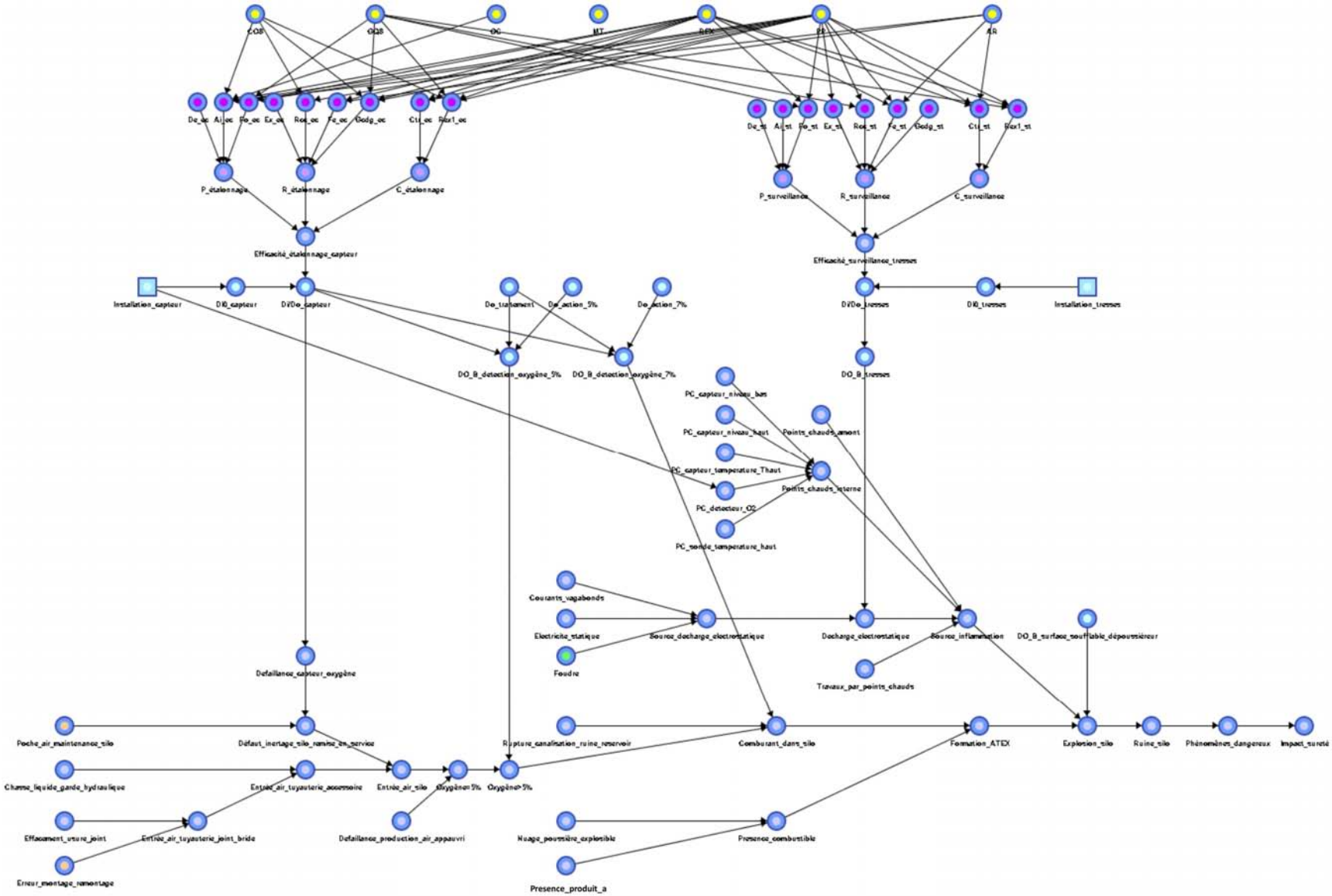

FIG. 4.10 – Représentation par réseau bayésien du scénario complet

4.4.4.1 Quantification des variables du modèle

La quantification proposée à été obtenue, lors des séances d'analyse de risques (pour le scénario technique) et lors des analyses d'activités (pour les aspects humains et organisationnels), par avis d'experts, par l'analyse du retour d'expérience disponible, et par l'analyse de la documentation à notre disposition.

Les distributions initiales données pour les initiateurs du scénario sont précisées dans le tableau 4.6.

Initiateur	**Modalité *Absent***	**Modalité *Présent***
Poche_air_maintenance_silo	99	1
Chasse_liquide_garde_hydraulique	99	1
Effacement_usure_joint	99	1
Erreur_montage_remontage	90	10
Defaillance_production_air_appauvri	99	1
Nuage_poussiere_explosible	99	1
Presence_produit_a	0.1	99.9
Rupture_canalisation_ruine_reservoir	99.99	0.01
Foudre	99.969	0.031
Electricite_statique	1	99
Courants_vagabonds	0	100
PC_capteur_niveau_bas	99	1
PC_capteur_niveau_haut	99	1
PC_capteur_temperature_haut	99	1
PC_capteur_température_Thaut	99	1
PC_capteur_detecteur_O2	99	1
Points_chauds_amont	99.9	0.1
Travaux_par_points_chauds	99.9	0.1

TAB. 4.6 – Distributions initiales des initiateurs techniques du scénario étudié (en %)

Concernant les disponibilités des composants des barrières étudiées, les valeurs sont précisées dans le tableau 4.7.

Composant de la barrière	**Type de disponibilité**	**Modalité « Disponible »**	**Modalité « Indisponible »**
Capteur de détection d'oxygène	Intrinsèque	98	2
Traitement	Opérationnelle	99	1
Action_5%	Opérationnelle	99.9	0.1
Action_7%	Opérationnelle	99	1
Tresses	Intrinsèque	99.9	0.1
Surface soufflable	Opérationnelle	50	50

TAB. 4.7 – Disponibilités des barrières étudiées (en %)

Les disponibilités initiales des variables relatives aux aspects humains [32] et organisationnels [33] ont été fixées à 99% pour leur modalité non dégradée (« Efficace » pour les variables représentant l'efficacité et les phases de l'action, « Présent » pour les items, et « Absent » pour les facteurs organisationnels), et à 1% pour leur modalité dégradée (« Inefficace » pour les variables représentant l'efficacité et les phases de l'action, « Degradé » pour les items, et « Présent » pour les facteurs organisationnels). Cette configuration initiale s'explique par le fait que le système étudié est supposé être en « bonne santé » (du fait de ses activités actuelles, et du retour d'expérience disponible qui ne recense aucun accident majeur pour le site étudié).
Les valeurs attribuées à la surface soufflable témoignent de la méconnaissance de l'état de cet élément par les acteurs du site. Dans le cas où ce composant ne serait pas critique, cette estimation s'avérera suffisante. Dans le cas contraire, il faudra envisager de renforcer la caractérisation de cet élément.

4.4.4.2 Quantification des influences présentes dans le modèle

La quantification proposée a été obtenue par l'analyse des relations logiques présentes dans la représentation nœud-papillon du scénario, et des avis d'experts (pour les impacts humains et organisationnels).

Dans un premier temps, nous décrivons les relations existantes entre les variables du scénario technique. Puis nous quantifions les influences identifiées pour les niveaux humains et organisationnels. Enfin, nous proposons une quantification de la disponibilité opérationnelle de chacun des composants des barrières impactés par des actions humaines (pour le capteur de détection d'oxygène et pour les tresses de continuité électrique).

a - Variables du scénario technique
Ces relations se définissent à partir des portes logiques identifiées dans les figures 4.4 et 4.5. Nous pouvons citer, à titre d'exemples, les règles logiques existantes pour les variables « Entree_air_tuyauterie_accessoire », « Explosion_silo », « Phenomenes_dangereux » et « Impact_surete ».

Règle logique liée à la variable « Entree_air_tuyauterie_accessoire » :
SI (Chasse_liquide_garde_hydraulique == Présent) **OU** (Entrée_air_tuyauterie_joint_bride == Présent),
ALORS (Entree_air_tuyauterie_accessoire == Présent),
SINON(Entree_air_tuyauterie_accessoire == Absent)

Règle logique liée à la variable « Explosion_silo » :
SI (Source_inflammation == Présent) **ET** (Formation_ATEX == Présent) **ET** ((DO_B_surface_soufflable_dépoussiéreur == Indisponible) **OU** (DO_B_surface_soufflable_dépoussiéreur == Absent)),
ALORS (Explosion_silo == Présent),
SINON (Explosion_silo == Absent)

32. Efficacité de l'action, Phases de l'action (Préparation, Réalisation, Clôture) et Items
33. Facteurs Organisationnels Pathogènes

	Phenomenes_dangereux			
Ruine_silo	Absent	Effet_pression	Projection_missile	Combinaison (Pression et Missile)
Absent	100	0	0	0
Présent	0	2	3	95

TAB. 4.8 – TPC de la variable « Phenomenes_dangereux »

	Impact_sureté	
Phenomenes_dangereux	Absent	Présent
Absent	100	0
Effet_pression	30	70
Projection_missile	20	80
Combinaison	0.01	99.99

TAB. 4.9 – TPC de la variable « Impact_sureté »

b - Configuration humaine et organisationnelle

Pour qualifier ces influences, nous proposons d'utiliser une échelle semi-quantitative à cinq niveaux définie dans le tableau suivant [34].

Modalité	**Valeur**	**Définition**
Pas d'Impact (**PI**)	100%	Signifie que l'efficacité de la variable fille n'est pas impactée par le caractère dégradé de la variable parent considérée [35]. Cette modalité est utilisée par les experts lors de la simplification de la configuration générique.
Impact Faible (**IF**)	95%	Signifie que l'efficacité de la variable fille est faiblement impactée par le caractère dégradé de la variable parent considérée.
Impact (**I**)	75%	Signifie que l'efficacité de la variable fille est significativement impactée par le caractère dégradé de la variable parent considérée.
Impact Important (**II**)	50%	Signifie que l'efficacité de la variable fille est fortement impactée par le caractère dégradé de la variable parent considérée.
Impact Total (**IT**)	1%	Signifie que l'efficacité de la variable fille est totalement impactée par le caractère dégradé de la variable parent considérée.

TAB. 4.10 – Échelle semi-quantitative proposée

Ainsi, en considérant les configurations particulières définies dans la partie 4.4.2.2 et l'échelle semi-quantitative proposée dans le tableau précédent, les experts ont proposé les quantifications présentées dans les tableaux 4.11 à 4.13 pour l'action d'étalonnage du capteur, et celles présentées dans les tableaux 4.14 à 4.16 pour les tresses de continuité électrique.

34. La construction de cette échelle suit les règles définies dans l'annexe G de ce mémoire.

35. Dans le cas des influences entre items et facteurs organisationnels, cette définition précise que l'état de l'item concerné n'est pas dégradé par le caractère pathogène du facteur organisationnel.

	COS	GQS	OC	MT	REX	PP	AR
De							
Ai	IF		I		IF	IF	I
Fo		IF			IF	IF	
Ex							
Rcc	IF					I	
Fe					IF		II
Gcdg	IF	IF			IF	IF	
Cao					I	IF	
Rex	II	I			II	IF	

TAB. 4.11 – Qualification des influences entre FOP et items pour l'action d'étalonnage du capteur

	Items (étalonnage du capteur)								
Phase	**De**	**Ai**	**Fo**	**Ex**	**Rcc**	**Fe**	**Gcdg**	**Cao**	**Rex**
P	I	II	I						
R				II	I	II	IT		
C								I	II

TAB. 4.12 – Qualification des influences entre items et phases (étalonnage du capteur)

	Phase de l'action		
	P	**R**	**C**
Efficacité	II	IT	I

TAB. 4.13 – Qualification des influences entre phases et efficacité (étalonnage du capteur)

	COS	GQS	OC	MT	REX	PP	AR
De							
Ai							
Fo		IF			I	IF	
Ex						I	
Rcc		II				I	
Fe					IF	II	IF
Gcdg							
Cao					IF	I	I
Rex		I			II	I	

TAB. 4.14 – Qualification des influences entre FOP et items pour l'action de surveillance des tresses

	Items (surveillance des tresses)								
Phase	**De**	**Ai**	**Fo**	**Ex**	**Rcc**	**Fe**	**Gcdg**	**Cao**	**Rex**
P	IF	IF	IF						
R				I	I	II	IF		
C								II	II

TAB. 4.15 – Qualification des influences entre items et phases (surveillance des tresses)

	Phase de l'action		
	P	**R**	**C**
Efficacité	IF	II	I

TAB. 4.16 – Qualification des influences entre phases et efficacité (surveillance des tresses)

c - Disponibilité opérationnelle des composants des barrières
De la même manière que précèdemment, la quantification de l'influence (de l'action de maintenance sur la disponibilité opérationnelle du composant) est réalisée par l'intermédiaire de l'échelle semi-quantitative présentée dans le tableau 4.10.

La quantification proposée par les experts, à partir de la méthode présentée dans la partie 3.3.1 est alors la suivante :
– $\alpha 1$ = II et $\alpha 2$ = I, pour la disponibilité opérationnelle du capteur d'oxygène.
– $\alpha 1$ = IF et $\alpha 2$ = II, pour la disponibilité opérationnelle des tresses de continuité électrique.

Les disponibilités opérationnelles des barrières de detection d'oxygène à 5% (et à 7%) sont, quant à elles, exprimées au travers de la règle définie ci-après.

SI ((Di/Do_capteur == Disponible) **ET** (Do_traitement == Disponible) **ET** (Do_action_5% == Disponible)),
ALORS (B_detection_oxygene_5% == Disponible),
SINON SI ((Di/Do_capteur == Absent) **OU** (Do_traitement == Absent) **OU** (Do_action_5% == Absent)),
ALORS (B_detection_oxygene_5% == Absent),
SINON (B_detection_oxygene_5% == Indisponible)

4.5 Exploitation du modèle

Cette partie vise à étudier les comportements du modèle face à des configurations de données différentes. Dans un premier temps, nous utilisons la quantification telle qu'elle est présentée dans les parties précédentes. Puis nous modifions certaines valeurs (distributions initiales, valeurs de l'échelle semi-quantitative) afin de tester la robustesse de ce modèle. Nous terminons enfin sur l'interprétation des résultats et les conclusions qui en résultent.
Pour chacune de ces configurations, les situations suivantes sont étudiées : cas *a priori*, cas de simulation et cas de diagnostic (présence d'un impact sur la sûreté, puis l'inefficacité de l'action d'étalonnage du capteur).

Le cas *a priori* consiste à étudier les résultats fournis par le modèle sans apporter de connaissance supplémentaire à la quantification faite lors de la construction de ce modèle (passage du mode Modélisation au mode Validation dans BayesiaLab) ; alors que les cas de simulation et de diagnostic consistent à fixer l'état de certaines variables du réseau pour pouvoir observer le comportement du modèle dans ces configurations particulières.

4.5.1 Tests du modèle

4.5.1.1 Cas *a priori*

Dans cette configuration, nous nous intéressons aux éléments importants pour la sécurité (les barrières « détection d'oxygène » et « tresses de continuité électrique ») et à la probabilité d'occurrence d'un impact sur la sûreté.

Variable du modèle	Modalité	Probabilité
Étalonnage du capteur	Inefficace	6.31
Disponiblité opérationnelle de la détection d'oxygène à 5%	Indisponible	5.67
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	6.52
Surveillance des tresses	Inefficace	2.96
Disponibilité opérationnelle des tresses	Indisponible	0.20
Impact sûreté	Présent	0.02

TAB. 4.17 – État de certaines variables du système *a priori* (en%)

Ces résultats *a priori* permettent d'observer que :

- Le modèle donne des valeurs cohérentes avec les données utilisées pour le construire. En effet, il n'y a pas de comportement divergeant par rapport aux données utilisées pour construire le modèle (les probabilités associées aux modalités dégradées des variables observées sont relativement faibles).
- Le capteur de détection d'oxygène semble être un composant plus critique (car ayant des valeurs d'indisponibilités plus fortes) que les tresses de continuité électrique.

4.5.1.2 Cas de simulation

Le cas de simulation est obtenu en précisant dans le modèle la présence du caractère pathogène des facteurs organisationnels identifiés lors des analyses sur site (cf. tableaux 4.18 et 4.19).

Variable du modèle	Modalité	AR, PP et COS présents
Étalonnage du capteur	Inefficace	48.93
Disponiblité opérationnelle de la détection d'oxygène à 5%	Indisponible	26.53
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	27.20
Surveillance des tresses	Inefficace	25.77
Disponibilité opérationnelle des tresses	Indisponible	1.35
Impact sûreté	Présent	0.11

TAB. 4.18 – État de certaines variables du système (en %) en présence des trois FOP

Variable du modèle	Modalité	AR présent	PP présent	COS présent
Étalonnage du capteur	Inefficace	33.51	18.52	18.26
Disponiblité opérationnelle de la détection d'oxygène à 5%	Indisponible	18.99	11.65	11.52
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	19.72	12.45	12.32
Surveillance des tresses	Inefficace	7.03	23.68	2.96
Disponibilité opérationnelle des tresses	Indisponible	0.40	1.24	0.20
Impact sûreté	Présent	0.07	0.05	0.04

TAB. 4.19 – État de certaines variables du système (en %) en présence d'un des FOP

Ce cas de simulation permet de montrer que la présence des trois facteurs organisationnels pathogènes engendrent une situation plus critique que la présence d'un seul de ces trois facteurs. En effet, les variables observées ont une probabilité plus importante d'être dans leur état degradé lorsque les trois facteurs sont présents que lorsqu'un seul l'est.

Ce cas permet également de proposer une première priorisation [36] pour le traitement des facteurs organisationnels, en fonction des variables (représentatives des barrières) considérées :
– Cas du capteur de détection d'oxygène : (1) AR [37], (2) PP [38], (3) COS [39].
– Cas des tresses de continuité électrique : (1) PP, (2) AR, (3) COS.
Cette première priorisation montre que les AR et PP doivent être traités en priorité (sans discrimination d'ordre), puis viennent les COS. Par contre, le faible écart sur l'impact sûreté ne permet pas de conclure sur la priorité à donner pour le traitement de ces facteurs organisationnels pathogènes. C'est dans le cas suivant que nous allons définir cette priorisation.

36. Rappel : La valeur de la probabilité est utilisée en relatif, au sens où elle n'est utilisée que dans un objectif de classification.
37. AR : Absence de réexamen des hypothèses de conception
38. PP : Pressions de production
39. COS : Faiblesse de la culture organisationnelle de sûreté

4.5.1.3 Cas de diagnostic

a - Présence d'un impact sûreté
Ce cas de diagnostic est obtenu en fixant dans le modèle la présence d'un impact sur la sûreté (cf. tableau 4.20).

Initiateur	Modalité « Présent »
Courants_vagabonds	100
Presence_produit_a	100
Electricite_statique	99
Erreur_montage_remontage	74.58
PC_capteur_niveau_bas	18.85
PC_capteur_niveau_haut	18.85
PC_capteur_temperature_haut	18.85
PC_capteur_température_Thaut	18.85
PC_capteur_detecteur_O2	18.85
Chasse_liquide_garde_hydraulique	7.46
Effacement_usure_joint	7.46
Defaillance_production_air_appauvri	7.46
Poche_air_maintenance_silo	6.35
Points_chauds_amont	1.89
Travaux_par_points_chauds	1.89
Nuage_poussiere_explosible	1
Rupture_canalisation_ruine_reservoir	0.09
Foudre	0.03
Barrière	**Modalité « Inefficace »**
B_surface_soufflable	100
B_detection_oxygene_7%	100
B_detection_oxygene_5%	99.99
B_tresses	4.22

TAB. 4.20 – État des initiateurs et des barrières, en présence d'un impact sur la sûreté (en%)

Ce premier cas de diagnostic permet d'identifier les élements prépondérants dans la présence d'un impact sûreté :
- des éléments déjà prépondérants lors de la construction du modèle (les courants vagabonds, la présence de produit « a » et l'électricité statique),
- des barrières (surface soufflable, détection d'oxygène à 5% et à 7%),
- des erreurs humaines dues à des opérations de maintenance (les erreurs de montage ou de remontage),
- des points chauds internes dus à des composants pouvant être inadaptés à leur environnement (composants non ATEX ...).

Ces élements prépondérants nécessitent d'être étudiés plus en détail :
- Concernant les courants vagabonds et l'électricité statique, ces éléments sont inhérents à l'activité du système de production et leur non occurrence dépend de la disponibilité de

la barrière « tresse » (qui semble rester à un niveau de disponibilité acceptable malgré la présence d'un impact sur la sûreté).
- Concernant la présence de produit « a », un système est amenagé dans le local silo pour absorber la quantité de produit qui s'échappent du silo (cf. partie 4.2.1).
- Concernant les points chauds internes, il a été précisé dans la partie 4.2.1 que tous les composants internes respectent la réglementation ATEX, ce point sera donc à vérifier sur place avec l'industriel.
- Par contre, les barrières « surface soufflable » et « detection d'oxygène » semblent être fortement contributrice à la présence d'un impact sûreté. Ceci signifie qu'une investigation supplémentaire est nécessaire pour expliciter l'indisponibilité de ces barrières.

Pour la barrière « surface soufflable », il est nécessaire de faire des études complémentaires (analyse d'activités ...) afin de pouvoir identifier les causes sous-jacentes explicitant son indisponibilité.

Pour les barrières de détection d'oxygène à 5% et à 7%, les informations présentes dans le modèle permettent de faire cette étude.
Dans un premier temps, nous allons identifier les composants de la barrière qui sont les plus critiques :

Variable	Modalité	Probabilité
Di_Do_capteur	Indisponible	83.87
Do_traitement	Indisponible	16.94
Do_action_7%	Indisponible	1.03
Do_action_5%	Indisponible	0.12
Efficacité_étalonnage_capteur	Inefficace	59.04
DI0_capteur	Indisponible	27.73

TAB. 4.21 – État des composants des barrières « détection d'oxygène », en présence d'un impact sur la sûreté (en %)

Au regard des résultats présentés dans le tableau 4.21, il apparait que l'élément prépondérant est le capteur.
Si, à présent, on étudie les causes menant à l'indisponiblité de ce capteur, on observe que l'inefficacité de l'action de maintenance associée à ce composant est plus importante qu'un problème au niveau de sa disponibilité intrinsèque.

Ces observations nous permettent de proposer un deuxième cas de diagnostic, dans le paragraphe suivant, qui explicite les causes menant à l'inefficacité de l'action d'étalonnage de ce capteur.

b - Inefficacité de l'action d'étalonnage du capteur
Les causes les plus directes de cette inefficacité se situent au niveau des phases de l'action (cf. tableau 4.22), puis par des causes sous-jacentes que sont les items (cf. tableau 4.23) et les facteurs organisationnels (cf. tableau 4.24).

Rang	Phase	Modalité « Inefficace »
1	Réalisation	58.47
2	Préparation	19.83
3	Clôture	11.90

TAB. 4.22 – État des phases de l'étalonnage du capteur, en présence d'une inefficacité de l'action (en %)

Ce cas de diagnostic permet de montrer que l'étape de Réalisation de l'action est prépondérante par rapport aux deux autres étapes.

Rang	Item	Modalité « Degradé »
1	Gcdg	18.64
2	Fe	13.09
3	Ai	8.51
4	Ex	8.31
5	Rex	7.73
6	Rcc	6.29
7	Fo	3.46
8	Cao	3.01
9	De	2.82

TAB. 4.23 – État des items de l'étalonnage du capteur, en présence d'une inefficacité de l'action (en %)

Cette analyse permet de prioriser les items, les plus critiques sont : la gestion collective et dynamique de groupe, les facteurs d'environnements et les aides.

Rang	FOP	Modalité « Présent »
1	AR	5.31
2	REX	3.29
3	PP	2.94
4	COS	2.90
5	GQS	2.23
6	OC	1.90
7	MT	1.00

TAB. 4.24 – État des FOP, en présence d'une inefficacité de l'action (en %)

Au niveau des facteurs organisationnels prioritaires, on retrouve l'absence de réexamen des hypothèses de conception (AR) et les pressions de production (PP) (facteurs identifiés comme étant pathogènes lors des analyses sur site), mais également la difficulté de faire vivre un retour d'expérience (REX) (facteur non pathogène au moment de l'analyse mais dont les signes précurseurs doivent être surveillés).

4.5.2 Utilisations du modèle

Différentes configurations vont à présent être réalisées afin d'étudier les comportements du modèle face à des quantifications différentes : les premières configurations proposent d'appliquer différentes valeurs quantifiées pour l'échelle d'élicitation d'avis d'experts, les dernières portent sur l'utilisation de différentes distributions initiales pour les variables des niveaux actions et organisation.

4.5.2.1 Présentation des différentes configurations

a - Modification des valeurs quantifiées de l'échelle de dégradation

Deux configurations (cf. tableau 4.25) vont être étudiées dans cette partie : la première (cas n°1) consiste à considérer une évolution linéaire entre les différents paramètres de l'échelle, alors que la seconde (cas n°2) consiste à dégrader l'échelle utilisée pour le cas traité dans la partie 4.5.1 (que l'on nommera cas n°0) de 10%.

Modalité de l'échelle	Cas n°0	Cas n°1	Cas n°2
Pas d'Impact	1	1	1
Impact Faible	0.95	0.745	0.855
Impact	0.75	0.50	0.675
Impact Important	0.5	0.255	0.45
Impact Total	0.01	0.01	0.009

TAB. 4.25 – Valeurs quantifiées des modalités de l'échelle d'élicitation d'avis d'experts

Les deux configurations proposées permettent d'étudier le comportement du modèle face à des échelles plus discrimantes que celle du cas n°0 (cf. annexe G de ce mémoire), et d'étudier ainsi la robustesse des résultats observés.

b - Modification des distributions initiales pour les aspects humains et organisationnels

Cinq configurations (cf. tableau 4.26) vont être étudiées dans cette partie : les deux premières (cas n°3 et n°4) permettent de vérifier la robustesse des résultats donnés par le modèle (valeurs des distibutions proches), les deux suivantes (cas n°5 et cas n°6) permettent de tester le comportement du modèle face à des distributions de plus en plus dégradées, enfin le dernier (cas n°7) permet d'étudier le comportement du modèle face à une absence de connaissance *a priori* sur l'état des variables (des niveaux actions et organisations).

Modalité de la variable	Cas n°0	Cas n°3	Cas n°4	Cas n°5	Cas n°6	Cas n°7
Non dégradée	99	99.99	99.90	97	89.10	50
Dégradée	1	0.01	0.10	3	10.9	50

TAB. 4.26 – Distributions initiales (en %) proposées pour les cas n°3 à 7

Les situations étudiées dans la partie suivante, pour chacune des configurations proposées (cas n°1 à 7), sont les mêmes que celles traitées pour le cas n°0 : cas *a priori*, cas de simulation et cas de diagnostic (présence d'un impact sur la sûreté, puis inefficacité de l'action d'étalonnage du capteur).

4.5.2.2 Situation *a priori*

a - Modification des valeurs quantifiées de l'échelle de dégradation

Variable du modèle	Modalité	Cas n°0	Cas n°1	Cas n°2
Étalonnage du capteur	Inefficace	6.31	10.79	7.55
Disponiblité opérationnelle de la détection d'oxygène à 5%	Indisponible	5.67	9.98	6.51
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	6.52	10.80	7.35
Surveillance des tresses	Inefficace	2.96	6.54	3.83
Disponibilité opérationnelle des tresses	Indisponible	0.20	1.70	0.60
Impact sûreté	Présent	0.02	0.05	0.02

TAB. 4.27 – État de certaines variables du système *a priori* pour les cas n°0, 1 et 2 (en %)

Ce cas permet de montrer que :
- Quelle que soit l'échelle considérée, le capteur de détection d'oxygène apparaît (*a priori*) comme étant plus critique que les tresses de continuité électrique.
- Les échelles utilisées dans les cas n°1 et 2 sont plus discrimantes que l'échelle utilisée dans le cas n°0. En effet, les probabilités associées aux modalités dégradées des variables observées sont plus importantes pour les cas n°1 et 2.

b - Modification des distributions initiales pour les aspects humains et organisationnels

Ce cas permet d'observer que :
- Comme pour les cas précédents, quelle que soit la distribution initiale considérée, le capteur de détection d'oxygène apparaît comme étant plus critique que les tresses de continuité électrique.
- Plus la distribution initiale est dégradée, plus les états (*a priori*) des variables du modèle sont dégradés (et notamment pour l'efficacité des actions d'étalonnage du capteur et de surveillance des tresses, qui sont plus directement impactées que les autres variables observées).
- Pour des distributions initiales trés proches (cas n°3 et 4), les valeurs des variables observées sont sensiblement similaires. Ces deux cas permettent de montrer, qu'*a priori*, le modèle donne des résultats cohérents et robustes.

Variable du modèle	Modalité	Cas n°0	Cas n°3	Cas n°4	Cas n°5	Cas n°6	Cas n°7
Étalonnage du capteur	Inefficace	6.31	0.07	0.65	7.79	51.25	97.19
Disponiblité opérationnelle de la détection d'oxygène à 5%	Indisponible	5.67	2.61	2.90	11.29	27.67	50.16
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	6.52	3.49	3.77	12.09	28.32	50.61
Surveillance des tresses	Inefficace	2.96	0.03	0.30	8.60	27.48	75.76
Disponibilité opérationnelle des tresses	Indisponible	0.20	0.05	0.07	0.48	1.44	3.87
Impact sûreté	Présent	0.02	0.01	0.01	0.04	0.12	0.29

TAB. 4.28 – État de certaines variables du système *a priori* pour les cas n°0, et 3 à 7 (en %)

4.5.2.3 Cas de simulation

Pour les différentes configurations étudiées, modification des valeurs quantifiées de l'échelle de dégradation ou des distributions initiales (pour les aspects humains et organisationnels), les classifications observées sont similaires (cf. annexe H de ce mémoire) :

- La présence des trois facteurs organisationnels pathogènes engendrent une situation plus critique que lorsqu'un seul de ces trois facteurs est présent.
- La classification reste la même, quel que soit le cas considéré, pour les variables en lien avec le capteur (AR puis PP puis COS) ou avec les tresses de continuité électrique (PP puis AR puis COS). Par contre au regard de l'impact sûreté, la classification est différente : AR puis PP puis COS (pour les cas n°0, 3, 4 et 5), PP puis AR puis COS (pour les cas n°1, 2 et 6), enfin PP et AR et COS (pour le cas n°7, il n'y a pas de priorisation). Pour le dernier cas, cette classification s'explique par la dimension du modèle. En effet le nombre de variables, entre les facteurs organisationnels (variables racines du réseau) et l'impact sûreté (variable finale du réseau), est important et engendre un phénomène de « filtrage » qui diminue l'importance de ces impacts lors de la simulation.

4.5.2.4 Cas de diagnostic : Présence d'un impact sur la sûreté

Initiateur	Cas n°1	Cas n°2	Cas n°3	Cas n°4	Cas n°5	Cas n°6	Cas n°7
Courants_vagabonds	100	100	100	100	100	100	100
Presence_produit_a	100	100	100	100	100	100	100
Electricite_statique	99	99	99	99	99	99	99
Erreur_montage_remontage	74.11	74.45	75.66	75.46	74.15	73.90	73.82
PC_capteur_niveau_bas	11.95	16.97	19.45	19.39	17.93	15.46	11.41
PC_capteur_niveau_haut	11.95	16.97	19.45	19.39	17.93	15.46	11.41
PC_capteur_temperature_haut	11.95	16.97	19.45	19.39	17.93	15.46	11.41
PC_capteur_température_Thaut	11.95	16.97	19.45	19.39	17.93	15.46	11.41
PC_capteur_detecteur_O2	11.95	16.97	19.45	19.39	17.93	15.46	11.41
Chasse_liquide_garde_hydraulique	7.41	7.44	7.54	7.55	7.42	7.39	7.38
Effacement_usure_joint	7.41	7.44	7.57	7.55	7.42	7.39	7.38
Defaillance_production_air_appauvri	7.41	7.44	7.57	7.55	7.42	7.39	7.38
Poche_air_maintenance_silo	6.95	6.53	4.98	5.24	6.90	7.22	7.32
Points_chauds_amont	1.19	1.70	1.95	1.94	1.79	1.55	1.14
Travaux_par_points_chauds	1.19	1.70	1.95	1.94	1.79	1.55	1.14
Nuage_poussiere_explosible	1	1	1	1	1	1	1
Rupture_canalisation_ruine_reservoir	0.08	0.08	0.10	0.10	0.08	0.08	0.07
Foudre	0.03	0.03	0.03	0.03	0.03	0.03	0.03
Barrière	**Cas n°1**	**Cas n°2**	**Cas n°3**	**Cas n°4**	**Cas n°5**	**Cas n°6**	**Cas n°7**
B_surface_soufflable	100	100	100	100	100	100	100
B_detection_oxygene_7%	100	100	100	100	100	100	100
B_detection_oxygene_5%	99.99	99.99	99.97	99.97	99.99	100	100
B_tresses	41.28	14.33	1.01	1.37	9.17	22.42	44.17

TAB. 4.29 – Présence des initiateurs et indisponibilité des barrières, en présence d'un impact sur la sûreté, cas n°1 à 7 (en %)

Les résultats obtenus sont similaires à ceux du cas n°0. En effet, quelle que soit l'échelle ou la distribution initiale utilisée, on retrouve les mêmes éléments prépondérants, à savoir :
- des éléments déjà prépondérants lors de la construction du modèle (les courants vagabonds, la désorption de pentane et l'électricité statique),
- des barrières (surface soufflable, détection d'oxygène à 5% et à 7%),
- des erreurs humaines dues à des opérations de maintenance (les erreurs de montage ou de remontage),
- des points chauds internes dus à des composants pouvant être inadaptés à leur environnement (composants non ATEX ...).

Composant	Cas n°1	Cas n°2	Cas n°3	Cas n°4	Cas n°5	Cas n°6	Cas n°7
Di_Do_capteur	93.25	86.64	62.41	66.47	92.50	97.52	99.06
Do_traitement	7.67	14.20	38.14	34.14	8.41	3.45	1.93
Do_action_7%	1.01	1.02	1.07	1.06	1.01	1.00	1.00
Do_action_5%	0.11	0.11	0.14	0.13	0.11	0.10	0.10
Efficacité_étalonnage_capteur	86.53	68.36	1.38	12.27	82.23	95.73	99.86
Di0_capteur	9.35	21.29	61.29	54.95	14.23	6.37	3.97

TAB. 4.30 – État (indisponible, inefficace) des composants de la barrière « détection d'oxygène », en présence d'un impact sur la sûreté, cas n°1 à 7 (en %)

Les cas n°3 et 4 montrent que l'aspect technique devient prépondérant par rapport à l'aspect humain. Ces résultats, cohérents avec les données utilisées pour construire le modèle, s'expliquent par le fait que les distributions initales (des variables des dimensions actions et organisations) utilisées pour ces cas sont trés proches de la valeur 100% alors que la disponibilité intrinsèque du capteur est fixée à 98%.

Nous allons donc procéder de la même manière que pour le cas n°0 et étudier plus en détail, dans la partie suivante, les causes de l'indisponibilité de l'action d'étalonnage du capteur.

4.5.2.5 Cas de diagnostic : Inefficacité de l'étalonnage du capteur de détection d'oxygène

Rang	Phase	Cas n°1	Cas n°2	Cas n°3	Cas n°4	Cas n°5	Cas n°6	Cas n°7
1	Réalisation	53.41	57.85	57.57	57.65	60.28	67.25	92.32
2	Préparation	31.96	22.94	18.50	18.62	22.51	32.92	74.78
3	Clôture	24.04	15.66	10.11	10.28	15.45	28.61	73.59

TAB. 4.31 – Inefficacité des phases de l'étalonnage du capteur, en présence d'une inefficacité de l'action, cas n°1 à 7 (en %)

Ce cas de diagnostic permet de montrer que, quelle que soit l'échelle ou la distribution initiale utilisée, l'étape de réalisation de l'action est prépondérante par rapport aux deux autres étapes.

Par contre on observe des classifications différentes au niveau des items. Ces résulats s'expliquent par le fait que les items sont les variables les plus connectées du modèle et donc plus sensibles face aux variations des données du modèle (ici, ce sont les valeurs quantifiées de l'échelle d'élicitation d'avis d'experts ou les distributions initiales des variables des niveaux actions et organisation).

Rang	Cas n°0	Cas n°1	Cas n°2	Cas n°3	Cas n°4	Cas n°5	Cas n°6	Cas n°7
1	Gcdg	Gcdg	Gcdg	Gcdg	Fe	Gcdg	Rex	Rex
2	Fe	Rex	Fe	Fe	Gcdg	Fe	Gcdg	Ai
3	Ai	Ai	Rex	Ex	Ex	Rex	Fe	Fe
4	Ex	Fe	Ai	Ai	Ai	Ai	Ai	Rcc
5	Rex	Rcc	Rcc	Rex	Rex	Ex	Rcc	Rcc
6	Rcc	Fo	Ex	Rcc	Rcc	Rcc	Ex	Gcdg
7	Fo	Cao	Fo	Fo	Fo	Fo	Cao	Fo
8	Cao	Ex	Cao	De	De	Cao	Fo	Ex
9	De	De	De	Cao	Cao	De	De	De

TAB. 4.32 – Classification des items pour les cas n°0 à 7

Rang	Cas n°0	Cas n°1	Cas n°2	Cas n°3	Cas n°4	Cas n°5	Cas n°6	Cas n°7
1	AR	REX	AR	AR	AR	AR	AR	AR
2	REX	AR	REX	REX	REX	REX	REX	PP
3	PP	PP	PP	PP	PP	PP	PP	REX
4	COS	COS	COS	COS	COS	COS	COS	COS
5	GQS	GQS	GQS	GQS	GQS	GQS	GQS	GQS
6	OC	OC	OC	OC	OC	OC	OC	OC
7	MT	MT	MT	MT	MT	MT	MT	MT

TAB. 4.33 – Classification des facteurs organisationnels pour les cas n°0 à 7

Concernant les facteurs organisationnels, on retrouve la même classification (sauf pour le cas n°1, où il y a une inversion des facteurs AR et du REX ; et pour le cas n°7, où il y a une inversion des facteurs REX et PP) ; et les mêmes facteurs prioritaires, à savoir : l'absence de réexamen des hypothèses de conception (AR) et les pressions de production (PP) (facteurs identifiés comme étant pathogènes lors des analyses sur site), mais également la difficulté de faire vivre un retour d'expérience (REX) (facteur non pathogène au moment de l'analyse mais dont les signes précurseurs doivent être surveillés).

4.6 Synthèse et interprétation des résultats

L'ensemble de ces mises en application montre que le modèle donne des résultats cohérents :
- Les analyses *a priori* ont permis d'identifier la criticité de certains composants (les capteurs de détection d'oxygène).
- Le cas de simulation a permis de prioriser les facteurs organisationnels identifiés lors des analyses sur site : les pressions de production (PP) (prioritaire pour l'action de surveillance des tresses de continuité électrique, réalisée par des opérateurs des équipes de production) et l'absence de réexamen des hypothèses de conception (AR) (prioritaire pour l'action d'étalonnage du capteur de détection d'oxgène, réalisée par des opérateurs de l'équipe de maintenance), et la faiblesse de la culture organisationnelle de sûreté (COS).

- Le premier cas de diagnostic (présence d'un impact sur la sûreté) a permis, quant à lui, de prioriser les différents initiateurs du scénario, mais également de confirmer le fait que le capteur de détection d'oxygène est plus critique que les tresses de continuité électrique (priorisation des barrières).
- Le deuxième cas de diagnostic (inefficacité de l'action d'étalonnage du capteur) permet de classer les variables caractéristiques (phases et items) de cette action, ainsi que les facteurs organisationnels : la phase de réalisation de l'action (du fait de la complexité de l'action qui nécessite l'utilisation d'outils spécifiques, d'abaques de calcul, de démonter le matériel ...) ; les items Gcdg [40] (du fait de l'importance de la communication entre les opérateurs), Fe [41] (du fait de l'importance du contexte dans lequel est réalisée l'action : salle de commande, toit des silos ...) et Ai [42] (du fait de l'utilisation d'outils spécifiques : talkie walkie, bouteille étalon, consignation électrique, abaques de calculs ...) ; et les facteurs organisationnels AR, PP (en cohérence avec les observations des analyses sur site) et REX [43].

Ces observations permettent de proposer un ensemble de solutions [44] pour le système « silos de stockage » :

- Concernant les pressions de production, veiller à conserver une équipe de maintenance dédiée et non sous-traitée, et mener une politique de sensibilisation auprès des opérateurs (du site et des sous-traitants) sur les dangers potentiels liés aux silos de stockage.
- Concernant l'absence de réexamen des hypothèses de conception, formaliser l'ensemble des procédures de maintenance et de conduite (pour ne pas perdre la connaissance du système), remettre à jour l'ensemble des documentations permettant d'identifier les interlocuteurs adéquats (les restructurations ayant fait disparaître certains cadres intermédiaires), et veiller à ce que les analyses de risques soient régulièrement réalisées (notamment lorsqu'une modification dans l'installation est réalisée).
- Concernant la difficulté à faire vivre un retour d'expérience, ce facteur n'a pas été identifié comme pathogène au moment des analyses sur site, mais apparaît comme étant prioritaire lors de l'utilisation du modèle. Ceci signifie qu'il faut surveiller les signes précurseurs de sa présence (comme par exemple : un système de REX lacunaire ou insuffisamment détaillé, des méthodes d'analyse du REX insuffisantes ou incomplètes, des accidents ou risques non pris en compte ou négligés, la dissimulation de certains phénomènes ou événements ... [Dien *et al.*, 2006]) pour pouvoir le traiter dès son apparition.
- Concernant le capteur de détection d'oxygène, veiller à ce que les opérateurs en charge de l'action d'étalonnage aient les connaissances et compétences suffisantes pour réaliser cette action (former d'autres opérateurs de l'équipe de maintenance pour pouvoir conserver la connaissance et les compétences sur cette action).
- Concernant les erreurs de montage ou de remontage (initiateur), il est nécessaire de faire des investigations plus approfondies sur site pour pouvoir en identifier les causes.
- Concernant les points chauds sur les composants internes au silo (initiateur), vérifier avec l'industriel que ces composants respectent la nouvelle réglementation ATEX [Parlement européen et Conseil, 2000].

40. Gcdg : Gestion collective et dynamique de groupe
41. Fe : Facteurs d'environnement
42. Ai : Aides
43. REX : Difficulté à faire vivre un retour d'expérience
44. Ces solutions ont été proposées par le groupe d'experts en charge de l'analyse (experts techniques et organisationnels) à partir des résultats fournis par cette étude.

– Concernant les autres barrières (en particulier la surface soufflable), il est nécessaire de faire des investigations plus approfondies sur site pour pouvoir identifier les causes de son indisponibilité.

Les résultats de cette étude ont été présentés à l'industriel concerné pour qu'il puisse statuer sur les investissements à réaliser afin d'améliorer le niveau de sûreté des silos de stockage de produits fini.

Au niveau de l'utilisation du modèle, nous observons que :
– Plus les influences sont directes, plus les impacts sont importants (le nombre des variables a pour effet de filtrer les impacts).
– Plus les variables sont connectées dans le modèle (nombre de liens, notamment pour les items), plus elles sont sensibles aux variations des données du modèle (distributions initiales, échelle d'élicitation d'avis d'experts).
– Les valeurs quantifiées de l'échelle d'élicitation d'avis d'experts conditionnent fortement les niveaux d'indisponibilité, d'inefficacité, de présence des variables du modèle (plus cette échelle est discriminante plus les probabilités observées sur ces modalités sont fortes ; et en fonction de ces valeurs, certaines classifications diffèrent).
– Les distributions initiales conditionnent également ces niveaux (plus ces distributions sont initialement dégradées, plus les probabilités observées sur ces modalités sont fortes).
– Les probabilités données par le modèle ne peuvent être utilisées qu'en relatif (pour classer les variables) du fait de l'utilisation de cette échelle semi-quantitative.

4.7 Conclusions

Ces mises en application permettent de démontrer la faisabilité de la démarche sur un cas industriel réel (donc particularisée par rapport à l'approche générique, [Léger *et al.*, 2009]). En effet, du fait des caractéristiques des réseaux bayésiens, le modèle proposé permet d'identifier l'ensemble des causes (ou parents) prépondérantes pour une situation donnée, de classer ces causes corrélées (niveau par niveau), et de visualiser les évolutions du système lorsque l'on dégrade graduellement la situation (facteurs organisationnels).

Ces mises en applications permettent de valider la méthode de quantification (principe de dégradation) et les modèles (barrières, configuration humaine et organisationnelle) associès à cette méthodologie. En effet, les résultats observés sont robustes (comportements récurrents pour les différents cas testés) et cohérents avec les observations obtenues sur site : prépondérance de certains facteurs organisationnels (PP, AR, et COS), importance de la phase de réalisation de l'action d'étalonnage du capteur de détection d'oxygène (dûe à la complexité de l'action), prépondérance de certains items (Gcdg, Fe et Ai).

En l'état actuel, la démarche de construction du modèle n'est pas automatisée. De ce fait, les étapes de construction qualitative (configuration humaine et organisationnelle) et quantitative (tables de probabilités conditionnelles, distributions initiales) se font manuellement. Des travaux complémentaires sont donc nécessaires pour simplifier et automatiser ces étapes, comme par exemple le développement : de méthodes permettant d'identifier plus rapidement la présence/absence de liens au niveau des aspects humains et organisationnels

(cf. annexe I), de méthodes permettant de construire des objets réutilisables pour certaines parties du modèle (les barrières ...), d'interfaces utilisateurs pour pouvoir renseigner le plus naturellement possible l'ensemble des tables de probabilités conditionnelles du modèle de risque (cf. annexe F).

Des travaux complémentaires sont également nécessaires pour :
- S'assurer de la robustesse de l'échelle d'élicitation d'avis d'experts (en terme de nombre de modalités et des valeurs quantifiées associées). En effet, les cas traités ont montré que certaines variables du modèle (celles fortement connectées) étaient sensibles à ces variations, et de ce fait aboutissaient à des classifications différentes.
- S'assurer de la robustesse de la configuration humaine et organisationnelle (variables caractéristiques et influences identifiées) simplifiée pour un cas particulier. En effet, l'absence/présence de liens erronés peut fortement influer les classifications proposées par le modèle. En d'autre termes, s'assurer avec les experts (du facteur humain et des analyses organisationnelles) que cette simplification fasse sens.
- Étudier la possibilité d'intégrer les aspects humains et organisationnels au niveau des initiateurs, à partir de ce qui a été développé pour les barrières.

Conclusions et perspectives

La contribution principale développée dans nos travaux de thèse consiste en une méthodologie d'analyse quantitative des risques incidentels/accidentels qui intègre les connaissances représentatives du comportement de chacun des acteurs d'un système industriel de production.

La nécessité, pour les industriels, de développer une telle approche trouve son origine dans l'occurrence d'événements critiques, pour lesquels l'identification des causes techniques ne suffit pas à expliquer leur apparition. En effet, une analyse détaillée de ces accidents révéle, le plus souvent, des causes sous-jacentes provenant des dimensions humaines et/ou organisationnelles des systèmes de production concernés.
Nous avons, par ailleurs, pu souligner dans ce mémoire que l'analyse de risques est une discipline dont les évolutions résultent du recul acquis sur les phénomènes accidentels. Il est donc normal que ces méthodes d'analyses aient été développées, dans un premier temps, de manière sectorielle (*i.e.* en se focalisant sur un des acteurs du système). Mais, il semble aujourd'hui nécessaire, du fait de la complexité grandissante des systèmes de production, de dépasser ce cloisonnement sectoriel pour proposer des démarches qui permettent d'identifier l'ensemble des causes ayant initiées (et/ou précipitées) l'occurrence de l'événement critique. La mise en œuvre de ces démarches globales permet de prioriser les actions à mener et les investissements à réaliser, qui peuvent alors être utilisées comme des outils d'aide à la décision.

Partant de ces constats, nous avons établi une synthèse des caractéristiques de chacune des disciplines sectorielles concernées (les analyses techniques, l'étude des facteurs humains et les approches organisationnelles), ainsi que leurs apports pour le développement de démarches intégrées. Dans un premier temps, nous avons classés les principales méthodes d'analyses sectorielles en fonction des hypothèses de travail sous-jacentes, et des modèles utilisés pour représenter et tracer les résultats obtenus. Puis, nous avons étudié les caractéristiques d'un ensemble de méthodologies proposant l'intégration de ces démarches sectorielles. De cette synthèse, nous avons pu souligner le besoin de dépasser les limites actuellement rencontrées dans le développement de ces démarches intégrées. Ce dépassement peut être facilité en proposant des méthodologies qui ne cherchent plus à responsabiliser un acteur particulier du système, mais qui proposent une mesure quantifiée des risques de ces systèmes complexes (pour aider à la prise de décision), et qui fournissent des méthodes, outils et modèles génériques [45].
À partir de ces observations, notre contribution a été de structurer les étapes de construction de notre démarche méthodologique au travers de cinq phases distinctes : la définition des limites du système, l'extraction des connaissances, l'unification de ces dernières, la

45. Cette généricité permet d'appliquer la démarche à des systèmes appartenant à différents domaines d'activités.

construction du modèle de risque et sa représentation.

Ainsi, dans la première partie de nos développements méthodologiques, nous nous sommes focalisés sur la définition des dimensions constitutives des systèmes considérés et sur les principes permettant leur intégration dans un modèle de risque global.
Les dimensions retenues concernent les trois principales ressources nécessaires à l'exploitation d'un système industriel : le système technique, l'opérateur humain et l'organisation. Nous avons alors abordé l'analyse et la représentation de chacune de ces dimensions de manière sectorielle et nous avons justifié le choix des différentes méthodes retenues par une étude de l'adéquation des spécificités de ces dernières aux objectifs de notre approche.
L'intégration de ces différentes dimensions se traduit par l'extraction et la structuration des connaissances associées à chacune des ressources représentées. Cette étape consiste à utiliser les connaissances disponibles pour, d'une part, définir les variables représentatives du système et, d'autre part, élaborer des méthodes permettant d'identifier et de construire les influences pouvant exister entre ces variables.
De plus, en soulignant certaines spécificités des systèmes considérés, nous avons pu identifier les éléments pivots [46] de cette intégration, *i.e.* la disponibilité des barrières de défense, et nous avons pu également définir le principe théorique permettant cette intégration. Nous avons traduit ce principe, qui suppose que l'organisation impacte indirectement le système technique par le biais des comportements humains, en proposant des méthodes qui permettent d'analyser les élements suivants : comment l'efficacité des actions humaines (de maintenance et de conduite) est dégradée par la présence de facteurs organisationnels pathogènes, comment cette efficacité influence la disponibilité des barrières de défense, et comment cette disponibilité peut prévenir ou précipiter l'occurrence d'un événement du scénario accidentel étudié.
Nous avons également précisé que notre démarche vise l'identification des différentes faiblesses d'un système industriel pouvant mener à l'occurrence d'un événement redouté. Le traitement de ces faiblesses nécessite des analyses sectorielles spécifiques, et en ce sens notre approche ne cherche pas à se substituer à ces méthodes.
Une des contributions fortes de cette partie a été de réunir des experts de différentes disciplines autour d'une problématique commune, afin de pouvoir proposer une approche à la fois structurée, générique et applicable en milieu industriel.

Dans la deuxième partie de nos développements, nous avons abordé les points relatifs à la construction et à la représentation du modèle de risque.
Nous avons tout d'abord souligné la nécessité d'utiliser un outil de modélisation spécifique qui permette de représenter les particularités des systèmes étudiés, et de répondre aux objectifs de la problématique associée. En ce sens, nous avons analysé la compatibilité des caractéristiques de différents outils [47] avec les besoins liés à notre problématique [48], et nous avons pu, sur cette base, justifier le choix des réseaux bayésiens comme outil support aux modèles que nous proposons.
Nous avons ensuite défini les deux étapes nécessaires à la construction d'un modèle de risque : sa structuration et sa quantification.

46. Le terme « pivot » définit l'élément à l'interface des différentes dimensions du système.
47. Ces outils sont couramment utilisés pour des problématiques d'analyses de risques.
48. Ces besoins portent principalement sur la modélisation de systèmes complexes et l'estimation quantifiée des risques.

La structuration du modèle permet, d'une part, d'identifier et de modéliser les influences existantes entre les variables du modèle et, d'autre part, de définir les états que peuvent prendre ces variables. La phase de quantification porte sur le développement de méthodes qui permettent de renseigner les tables de probabilités présentes dans le modèle.
Nous avons alors souligné le fait qu'au sein des systèmes considérés, il existe des comportements locaux similaires qui permettent de scinder (et donc de simplifier) la construction du modèle de risque. Cette construction est alors réalisée au travers de trois phases distinctes : la modélisation du scénario technique, puis celle des éléments pivots de l'intégration (les barrières de défense) et, enfin, celle liée aux aspects humains et organisationnels.
Nous avons alors développé, pour chacune des parties étudiées du système, des méthodes et modèles à caractère générique, *i.e.* dont l'objectif est de pouvoir être particularisés ou instanciés aux cas spécifiques analysés.
La particularisation [49] est rendue possible par l'existence de modèles de références (pour l'élaboration de la configuration humaine et organisationnelle de la situation analysée).
L'instantiation [50] est rendue possible par l'existence de primitives réutilisables (concernant la modélisation de la disponibilité des barrières de défenses, des caractéristiques des actions humaines et de celles liées à l'organisation).
Nous avons notamment utilisé : des concepts permettant de traduire les arbres de défaillances en réseaux bayésiens, une formalisation orientée objet pour alléger la structure du modèle global et des fonctions spécifiques [51] qui permettent de particulariser chacune des influences présentes dans le modèle tout en limitant le nombre de paramètres à spécifier.
La mise en œuvre de notre démarche de modélisation aboutit à un modèle de risque global qui peut servir à la compréhension d'une situation particulière (par une analyse de la structure du modèle) et/ou à l'estimation des risques associés à cette situation (par inférences à partir des tables de probabilités). Ce modèle de risque peut ensuite être utilisé pour analyser, par simulation ou diagnostic, des situations pré-événementielles [52].
Notons que différentes déclinaisons opérationnelles de notre démarche ont été développées, par EDF et INERIS, afin de couvrir les particularités des systèmes analysés. Ces adaptations portent principalement sur la réduction du nombre de variables à considérer dans la modélisation et sur le choix des facteurs multiplicatifs de l'échelle d'élicitation d'avis d'experts.
Ainsi, dans cette partie, notre principale contribution a été de proposer un modèle de risque global, basé sur un formalisme unique (les réseaux bayésiens), qui permet de probabiliser les risques étudiés afin d'aider à la prise de décision.

Pour étudier la faisabilité de notre démarche méthodologique et valider les concepts, méthodes et modèles associés, nous avons particularisé nos développements à un cas industriel réel représentant un scénario d'explosion dans un silo de stockage de produit fini d'une installation classée. Par cette application, nous avons pu constater que le modèle global proposé permet d'identifier l'ensemble des causes prépondérantes pour une situation

49. La particularisation d'une approche générique consiste en une adaptation (pour le cas spécifique analysé) d'un modèle de référence.
50. L'instantiation consiste à dupliquer une primitive (définie de manière générique) afin de modéliser les caractéristiques (composants, influences ...) du cas spécifique étudié.
51. Ces fonctions sont les portes de type « noisy-OR (ou AND) ».
52. L'analyse d'une situation pré-événementielle se situe en amont de l'occurrence de l'événement redouté, à la différence de l'analyse d'un cas avéré qui se place en aval de cet événement.

donnée, de classer ces causes (niveau par niveau) et de visualiser les évolutions du système lorsque l'on dégrade graduellement la situation. Nous avons également pu souligner que les résultats obtenus sont robustes (au sens où l'on a pu observer des comportements récurrents pour les différents cas testés) et cohérents avec les observations obtenues sur site. Cette particularisation permet donc de valider une première applicabilité de nos travaux de thèse à des scénarios industriels critiques.
Mais ce cas d'application a également mis en lumière les manques et limites actuels de notre méthodologie. Ces points pourront être étudiés dans des travaux futurs afin d'étendre les possibilités d'analyses offertes par l'approche proposée.

En ce sens, nous présentons plusieurs axes de recherche visant à compléter et affiner les principes développés dans notre démarche méthodologique.
Ces différents axes de recherche portent sur :
– un renforcement du pouvoir descriptif du modèle (cf. points 1 à 3 dans la liste suivante),
– des aménagements d'exploitation de la méthodologie (cf. points 4 à 6),
– des extensions plus conséquentes (cf. points 7 à 9).

1. Dans notre approche, nous avons focalisé l'intégration au niveau des barrières de défense. Un apport serait de pouvoir également intégrer l'influence des aspects humains et organisationnels du système au niveau des initiateurs et/ou des événements des scénarios accidentels analysés. Cette perspective requiert de s'intéresser notamment aux travaux existants dans le domaine des études probabilistes de sûreté appliquées aux centrales nucléaires [Magne et Vasseur, 2006].

2. La quantification de certaines variables du modèle nécessite d'avoir recours à des jugements d'experts [53]. Cette caractéristique implique l'utilisation de tables de correspondances semi-quantitatives permettant d'éliciter ces avis d'experts [Lannoy et Procaccia, 2001].
Des travaux sont nécessaires pour s'assurer de la robustesse de ce type d'échelles, et plus particulièrement du nombre de modalités et des valeurs quantifiées associées ([Roberts, 1994], [Voisin, 1999], [Léger, 2005]). En effet, les cas traités dans l'application ont montré que certaines variables du modèle, celles fortement connectées, étaient sensibles à ces variations, et de ce fait aboutissaient à des classifications différentes.

3. La complexité des systèmes considérés et donc des modèles associés (nombre de variables, structures d'influences ...), et la nature des connaissances nécessaires à la quantification de ces modèles (comportements humains, décisions organisationnelles ...), induisent des incertitudes dont la mesure est importante pour qualifier la confiance que l'utilisateur peut avoir dans les résultats observés, et donc pour aider à la prise de décisions. Un apport serait de développer des méthodes permettant la mesure et la modélisation de ces différents types d'incertitudes [54]. Ces méthodes pourraient se baser sur des approches existantes (comme IDAFH, [Weber *et al.*, 2005]), ou sur les fonctions de croyances (telles qu'elles sont présentées dans [Simon *et al.*, 2008]).

53. Le jugement d'expert est utilisé pour quantifier des situations lorsqu'il y a peu, ou pas, de retour d'expérience.

54. Les incertitudes rencontrées peuvent être des incertitudes de modélisation, ou des incertitudes de quantification (stochastiques ou épistémologiques).

4. L'identification, pour une situation particulière, des influences existantes entre les variables représentatives des dimensions humaine et organisationnelle du système se fait par adaptation de la configuration générique proposée dans la partie 2.3.3.2. Cette adaptation se traduit généralement par une simplification de cette configuration générique. Or, nous avons montré, au travers du cas d'application, que l'absence/présence de liens erronés peut fortement influer les classifications proposées par le modèle.
   Il est par conséquent nécessaire de s'assurer (avec les experts des disciplines concernées) que cette simplification ait un sens, en développant une méthode qui facilite l'identification et la qualification de ces influences. Cette méthode peut, par exemple, prendre la forme d'organigrammes, comme celui décrit dans l'annexe I.

5. Du fait des particularités de certaines structures organisationnelles, actions humaines (de maintenance ou de conduite), et/ou composants techniques, un apport serait de définir des configurations types qui proposeraient, de manière pré-déterminée, des structures d'influences et une quantification associée. Ces configurations types permettraient de simplifier et d'automatiser la démarche de construction de modèles de risques particuliers, et de faciliter ainsi le transfert de la méthodologie dans le milieu industriel.
   Ces configurations pourraient, par exemple, prendre la forme : d'objets réutilisables modélisant certaines structures des systèmes considérés (comme par exemple pour des organisations de petites tailles, pour des actions humaines spécifiques ...) ou certains de leurs composants (comme par exemple pour les barrières de défense), d'interfaces utilisateurs permettant de renseigner de manière intuitive l'ensemble des tables de probabilités conditionnelles du modèle de risque.
   Ces points sont actuellement à l'étude dans le projet ANR - SKOOB [55] (projet 07 TLOG 021).

6. D'autres développements sont nécessaires pour pouvoir transférer la méthodologie proposée vers les instances opérationnelles des sites de production. Ces développement portent, par exemple, sur la proposition de protocoles d'enquêtes permettant de guider le recueil des informations lors des entretiens, sur l'élaboration d'un environnement logiciel dédié permettant d'automatiser la construction et la quantification des modèles, sur la création d'un outil permettant aux industriels de compléter et partager le retour d'expérience issu de l'application de notre méthodologie.

7. Afin d'éprouver la méthodologie développée dans ces travaux de thèse, il est nécessaire d'étendre le champ d'application initial (process chimique) à d'autres secteurs d'activités (centrale nucléaire, barrage hydraulique, automobile ...). Ces différentes mises en application permettraient d'étudier la robustesse des principes développés dans notre approche, de construire un retour d'expérience dédié à cette démarche d'analyse et de proposer (à terme) des configurations types en fonction du domaine d'activités et du process concernés.

8. Notre méthodologie propose une vision statique du système. Un apport serait d'intégrer la dimension temporelle dans les scénarios de risques analysés ([Weber *et al.*, 2004], [Weber et Jouffe, 2006]). En effet, l'introduction de la variable temps permettrait, par exemple, d'observer les réactions et reconfigurations du système technique (occurrence

55. SKOOB : Structuring Knowledge with Object Oriented Bayesian nets

ou non d'un événement redouté) face à un contexte organisationnel et humain changeant durant la fenêtre temporelle considérée.

9. Notre approche se base sur un ensemble de modèles et, comme tout modèle, elle offre une vision partielle de la réalité au sens où certains aspects sont représentés de manière simplifiés ou ne sont pas représentés. En l'état, les représentations utilisées dans notre démarche sont considérées comme étant exhaustives et partagées dans chacune des disciplines concernées. Ces représentations pourront évoluer et être complétées par de futurs travaux (réalisés par les experts de la discipline concernée) permettant, par exemple, de prendre en compte les aspects résilients[56] des opérateurs humains et des organisations ([Hollnagel *et al.*, 2006], [Seville *et al.*, 2006]). Les résultats de ces travaux pourront alors enrichir notre démarche méthodologique en permettant la représentation de nouveaux pans de la réalité.

56. En effet, la résilience est un concept récent dont les caractéristiques sont actuellement en cours de spécification.

Annexes

A : Typologie des actions de maintenance

La typologie des actions de maintenance, proposée par A. Despujols dans [Magne et Vasseur, 2006], est la suivante :

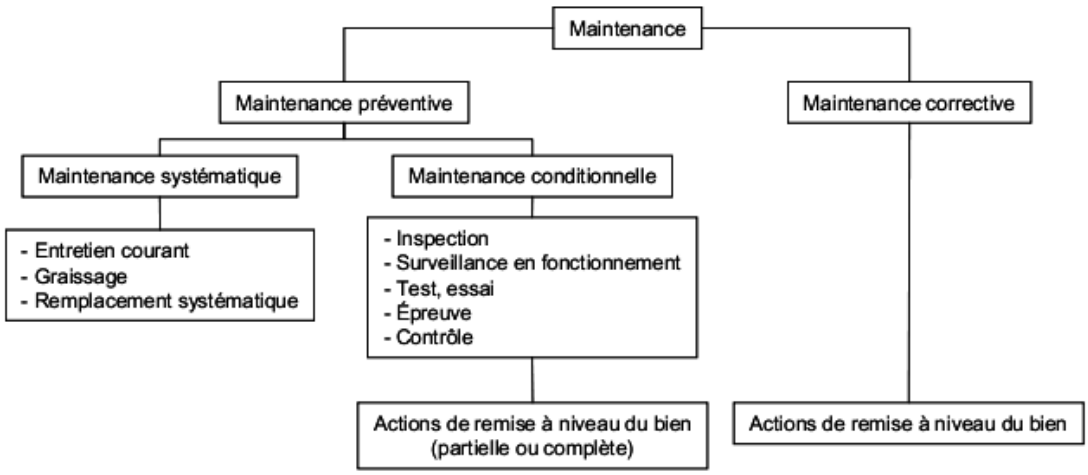

FIG. 11 – Typologie des actions de maintenance

La maintenance corrective consiste à intervenir afin de réparer un équipement une fois que celui-ci est défaillant.

La maintenance préventive consiste à intervenir sur un équipement avant que celui-ci ne soit défaillant, afin d'éviter la panne. On distingue :
- La maintenance préventive systématique (ou périodique/programmée), qui est effectuée systématiquement, soit selon un échéancier calendaire (à périodicité temporelle fixe), soit selon une périodicité d'usage (heure de fonctionnement, nombre d'unités produites, nombre de mouvements effectués ...).
- La maintenance préventive conditionnelle, qui est réalisée à la suite de relevés, de mesures, de contrôles révélateurs de l'état de dégradation de l'équipement.

Les tâches préventives sont ensuite classées et leurs effets sur la fiabilité des matériels (et donc sur les risques) sont analysés :
- Les remplacements systématiques de composants ont pour but de diminuer le taux de défaillance du matériel, et en quelque sorte, de le rajeunir. Ils nécessitent généralement son arrêt et son démontage et créent donc de l'indisponibilité et peuvent s'avérer coûteux. Ces tâches sont d'autant plus efficaces que la durée de vie des composants ou des matériels

remplacés est bien connue. On évite ainsi d'observer inutilement l'évolution des dégradations et on intervient au bon moment. Si en revanche cette durée de vie est fluctuante ou mal connue, on risque, de tomber malgré tout en panne si la période de remplacement systématique est trop grande, ou à l'inverse, de mettre au rebut des matériels en bon état si la période est trop courte.

- Le graissage est presque toujours une opération systématique qui consiste à faire des appoints de graisse ou d'huile. Il ne s'agit pas à proprement parlé de remplacement. Le graissage n'a pas pour effet de rajeunir le matériel, en revanche, il le préserve contre une dégradation trop rapide. On peut donc dire qu'il sert à maîtriser l'évolution du taux de défaillance.
- L'entretien courant (dépoussiérage, resserrage de connexions, purges ...) partage ce même objectif, c'est pourquoi, il sera classé dans de mêmes types de tâches, généralement simples et peu coûteuses.
- L'inspection externe consiste à examiner un matériel sans le démonter et sans outillage particulier. Ce type d'intervention ne crée généralement pas d'indisponibilité du matériel. Les rondes réalisées par les équipes de conduite en font notamment partie.
- La surveillance en fonctionnement, comme par exemple l'analyse vibratoire ou la thermographie, nécessite des moyens de mesure et d'analyse plus ou moins complexes et n'induit pas d'indisponibilité. Elles sont réalisées en fonctionnement ou à l'occasion d'essais.
- Les contrôles, comme par exemple l'examen visuel de composants internes, les contrôles par courant de Foucault, le ressuage ..., nécessitent généralement que le matériel soit hors service pour pouvoir effectuer des démontages. Leur objectif est également la découverte de dégradations annonciatrices de défaillances. Ce sont souvent des tâches relativement coûteuses qui créent de l'indisponibilité et qui donnent lieu à des remplacements de pièces notamment du fait des démontages. Les contrôles, comme la surveillance en fonctionnement, peuvent permettre de déterminer les lois d'évolution des dégradations observées.
- Les tests et les essais forment une catégorie à part parmi les tâches de maintenance préventive. En effet, ils s'appliquent à des matériels dont les fonctions sont en attente (en particulier les appareils de protection et les matériels de redondance passive) et permettent de s'assurer de leur capacité à remplir leur fonction lorsqu'elles sont requises. Ces tâches servent à détecter des pannes cachées et à remettre en état les matériels si nécessaire. On améliore ainsi leur disponibilité et on diminue le risque de pannes concomitantes. Enfin, on classera également dans cette catégorie de tâches les épreuves qui permettent de constater que l'on dispose de marges au-delà du régime de fonctionnement nominal.

B : Analyse du facteur humain - Exemples de pratiques (EDF et INERIS)

Exemple 1 - Installations hydrauliques - Questions utilisées par les experts d'EDF lors d'analyses d'activités

Ressources mobilisées
1. Quelles sont les personnes mobilisées pour cette intervention ? A quelles entités appartiennent-elles ? Est-ce suffisant ?
2. Quelle est la durée de l'intervention (en moyenne, la dernière) ? Est-ce suffisant ?
3. Combien de personnes sont impliquées ? Est-ce suffisant ?
4. Quel est votre rôle dans cette intervention ?

Préparation de l'intervention
5. L'action considérée est-elle référencée dans une procédure/formation/habilitation ? Si oui, préciser les caractéristiques de cette procédure/formation/habilitation. Si non, comment est-elle formalisée (documents, référence dans une formation) ? Quelle que soit la réponse, est-elle suivie/contrôlée par votre hiérarchie ?
6. A quelles difficultés êtes-vous confrontés lors de l'utilisation de ces documents ?
7. A quels autres documents vous référencez-vous pour préparer cette intervention ?
8. La réalisation de l'intervention est-elle une action planifiée/programmée à l'avance ?
9. Selon vous, quelles seraient les améliorations à prévoir concernant cette préparation ?

Réalisation de l'intervention
10. A quelles difficultés êtes-vous confrontés lors de la réalisation de l'intervention (utilisation des procédures/documents existants) ?
11. Quels autres documents utilisez-vous pour réaliser cette intervention ?
12. Quelles seraient selon vous, les évolutions à prévoir concernant cette intervention ?
13. Y a t il des contrôles en fin de chantier (validation de l'intervention) ?

Contrôle et retour d'expérience de l'intervention
14. Y a t il des contrôles avant/pendant/après l'intervention ?
15. Est-ce que l'intervention est régulièrement tracée ? (formulaire papier standardisé, autres supports, seuls quelques éléments ont été tracés dans des documents non spécifiques, analyse orale/non tracée ...)
16. Faites-vous un suivi des difficultés rencontrées durant la réalisation de l'intervention ?
17. Pendant l'intervention, avez-vous déjà été confrontés à des situations à risques non identifiées ? Si oui, préciser la situation et son traitement (temporaire, définitif ...).

18. Comment ces informations sont-elles remontées (mémos, rapports, réunions ...) ?

Plusieurs interrogations du questionnaire établi pour l'hydraulique sont en lien avec le niveau organisationnel (questions destinées aux autorités de contrôle) :
19. Selon-vous, dans l'organisation actuelle, qu'est-ce qui favorise cette attitude interrogative ?
20. Selon vous, que faudrait-il améliorer pour favoriser cette attitude interrogative ?

Exemple 2 - MIRIAM/ATHOS - Synoptique de la démarche développée par l'INERIS

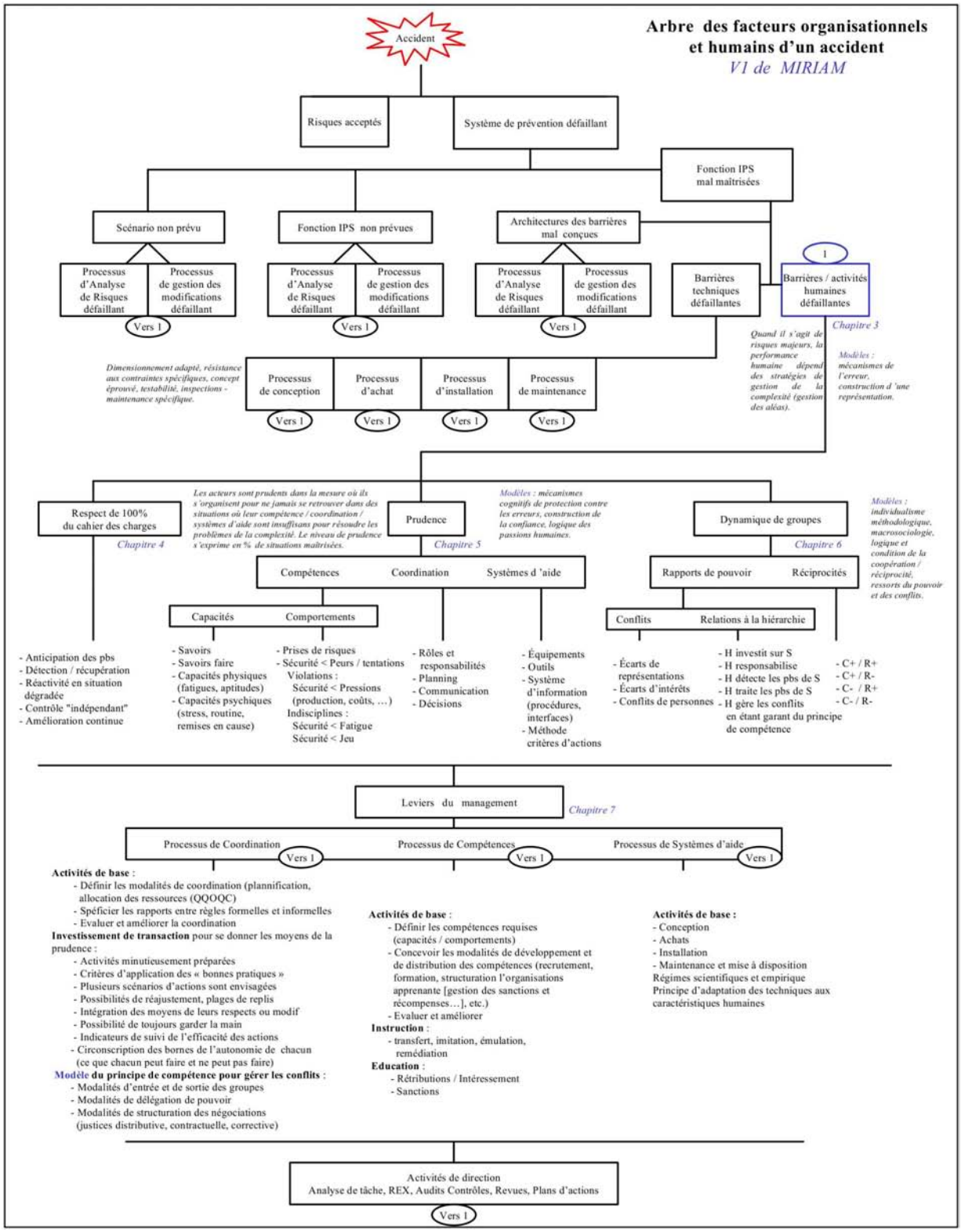

FIG. 12 – Arbre des facteurs organisationnels et humains d'un accident, [Plot, 2004]

C : Exemples de marqueurs, signes et symptômes associés aux FOP

Nous illustrons chacun des facteurs organisationnels pathogènes, définis dans [Dien *et al.*, 2006], par quelques-uns de leurs marqueurs, signes et symptômes. La description complète de ces marqueurs, signes, et symptômes est précisée dans la méthode DIONISOS[57] (méthode utilisée par EDF).

– Défaillance dans la gestion quotidienne de la sûreté (GQS)

Marqueur : Signes et symptômes associés
Modifications organisationnelles non suivies de mesures correctives : - Charge de travail élevée menant à une organisation du travail hasardeuse - Rotations excessives à des postes-clés
Non-prise en compte de messages d'alerte du personnel : - Lanceurs d'alertes non écoutés et/ou sanctionnés - Lettres d'avertissement de cadres non-prises en compte (lettres mortes)
Anomalies de sûreté répétées et non corrigées : - Dysfonctionnements techniques répétitifs non remontés vers les centres décisionnels - Dispositifs ergonomiques d'assistance inadaptés

TAB. 34 – Exemple de marqueurs, signes et symptômes pour le facteur GQS

57. DIONISOS : Méthode pratique d'analyse et de diagnostic organisationnel de la sûreté

– Faiblesse des organismes de contrôle (OC)

Marqueur : Signes et symptômes associés
Absence ou insuffisance de contrôles internes : - Manque de compétence, de crédibilité des contrôles internes - Contrôles internes trop formels, schématiques et/ou instrumentalisés
Réglementation inexistantes, caduques, inadaptées : - Méthodes de certification insuffisantes ou inexistantes - Réglementations contre certains risques (incendies ...) insuffisantes
Dérives vis-à-vis de la sûreté non détectées par les autorités de sûreté : - Dérives dans les pratiques de sûreté et de formation, dans les ressources attribuées à la sûreté - Echec ou insuffisance des contrôles de sûreté

Tab. 35 – Exemple de marqueurs, signes et symptômes pour le facteur OC

– Mauvais traitement de la complexité organisationnelle (MT)

Marqueur : Signes et symptômes associés
Découpage important des fonctions et missions : - Division excessive des tâches et des missions - Difficultés pour reconstituer le réseau organisationnel concerné
Mauvaise représentation de chaque instance et de leurs missions : - Difficultés à établir qui fait quoi - Manque de coordination globale entre instances
Communication interne insuffisante ou biaisée : - Circuits de remontées d'informations bloqués, diminués - Affaiblissement progressif des informations remontant du terrain

Tab. 36 – Exemple de marqueurs, signes et symptômes pour le facteur MT

– Difficulté à faire vivre un retour d'expérience (REX)

Marqueur : Signes et symptômes associés
Système formel de REX absent ou insuffisant : - Système de REX lacunaire, insuffisamment détaillé, trop rigide, trop instrumentalisé - Choix des événements trop restreint
Processus concret de REX absent ou insuffisant : - Personnel réalisant les investigations insuffisamment qualifié ou formé - Recommandations peu claires, trop restreintes, trop ciblées
Processus de mise en œuvre des résultats du REX inadaptés ou lacunaires : - Absence de responsabilités claires pour l'exécution des recommandations - Absence de bilan suite à la mise en œuvre et à l'application

Tab. 37 – Exemple de marqueurs, signes et symptômes pour le facteur REX

– Pressions de production (PP)

Marqueur : Signes et symptômes associés
Effectifs insuffisants et/ou en réduction : - « Downsizing » généralisé - Diminution des effectifs chargés de la sûreté
Ressources financières insuffisantes et/ou en réduction : - Accent placé excessivement sur contraintes financières et sur les économies - Economies faites sur les études de risques (ou de danger)
Délais trop limités affectant la sûreté : - Raccourcissement des délais de fourniture, des études, des contrôles et audits (sûreté) - Augmentation de la charge de travail avec maintien des délais et moyens initiaux

TAB. 38 – Exemple de marqueurs, signes et symptômes pour le facteur PP

– Absence de réexamen des hypothèses de conception (AR)

Marqueur : Signes et symptômes associés
Non traitement des défauts identifiés et analysés : - Ressources absentes ou inexistantes pour le traitement des défauts - Mise en œuvre effectuée mais insuffisante, inadaptée, non suivie, non évaluée
Non identification de vulnérabilité (défauts latents graves) : - Défauts apparus en cours d'exploitation mal identifiés - Insuffisances dans les essais de certification servant à éviter d'éventuels « black-spots »
Absence ou insuffisance d'analyse des défauts : - Défauts reconnus mais déclassés en terme de risques, normalisés - Modifications d'exploitation non analysées en termes de risques et de tenue

TAB. 39 – Exemple de marqueurs, signes et symptômes pour le facteur AR

D : Justification des influences génériques FOP-items/phases d'une action

Cette annexe présente les justifications génériques proposées pour la présence ou l'absence d'influence entre les variables caractéristiques de l'action humaine (items et phases) et les facteurs organisationnels pathogènes.

Rappel des sigles utilisés pour les différents facteurs organisationnels pathogènes (FOP) : **COS** (faiblesse de la culture organisationnelle de sûreté), **GQS** (défaillance dans la gestion quotidienne de la sûreté), **OC** (faiblesse des organismes de contrôle), **MT** (mauvais traitement de la complexité organisationnelle), **REX** (difficulté à faire vivre un retour d'expérience), **PP** (pressions de production), **AR** (absence de réexamen des hypothèses de conception).

Nous abordons tout d'abord les justifications associées à chacun des items, puis celles associées à chacune des phases.

ITEMS

Délégation (De)

La justification de la présence des influences est la suivante :
- **MT** - Si la configuration organisationnelle ne permet pas d'identifier les personnes compétentes, dans chacun des domaines, alors la délégation d'une tâche à une personne non compétente peut être facilitée.
- **PP** - Le temps, les budgets, les moyens et les ressources sont revus à la baisse mais les objectifs restent constants, ce qui peut favoriser des décisions contraintes, et donc une mauvaise délégation.

La justification de l'absence des influences est la suivante :
- **COS** - La définition de l'item se positionne au niveau des capacités des personnes qui vont réaliser les actions (acteurs à qui l'on a délégué la tâche) et non au niveau de la personne qui a fait le choix de déléguer sa tâche. Celle du facteur organisationnel est axée sur le niveau donné à la culture de sûreté au sein de l'entreprise, et donc plus sur la validité des choix du décideur.
  Si la définition de l'item avait été axée sur la personne qui délègue alors ce lien serait présent (le décideur n'est pas suffisamment sensibilisé à certaines notions de sûreté et peut donc mal déléguer sa tâche).
- **GQS** - La définition de l'item se positionne au niveau des capacités des personnes qui vont réa-

liser les actions (acteurs à qui l'on a délégué la tâche) et non au niveau de la personne qui a fait le choix de déléguer sa tâche. Celle du facteur organisationnel est axée, entre autre, sur l'adéquation des tâches à accomplir et des compétences des personnels (résultats de décisions prises par l'encadrement).
Si la définition de l'item avait été axée sur la personne qui délègue alors ce lien serait présent (le décideur ne prend pas en compte cette adéquation tâche/compétences pour effectuer sa délégation).
- **OC** - La définition de l'item se positionne au niveau des capacités des personnes qui vont réaliser les actions (acteurs à qui l'on a délégué la tâche). La définition du facteur organisationnel, ainsi que ses marqueurs, sont axés sur le fonctionnement et l'influence des organismes de contrôle au sein (ou à l'extérieur) de l'entreprise. Ces définitions ne permettent pas de faire un lien direct entre ce facteur organisationnel et cet item.
- **REX** - La définition de l'item se positionne au niveau des capacités des personnes qui vont réaliser les actions (acteurs à qui l'on a délégué la tâche). La définition du facteur organisationnel est axée sur la pérennité du processus de retour d'expérience au sein de l'entreprise. Ces définitions ne permettent pas de faire un lien direct entre ce facteur organisationnel et cet item.
Si la définition de l'item avait été axée sur la personne qui délègue alors ce lien serait présent (le décideur n'a pas toutes les informations lui permettant de déléguer la tâche à la bonne personne). Si on crée un lien à ce niveau on se positionne au niveau du retour d'expérience interne à un opérateur (son expérience propre).
- **AR** - La définition de l'item précise uniquement qu'il y aura une personne (ou plusieurs) pour réaliser l'action et que ces personnes peuvent être plus ou moins aptes à le faire. Les hypothèses de conception n'ont pas de liens directs avec la notion de délégation car elles permettent de définir le dimensionnement technique et social nécessaire au bon fonctionnement du système et non la manière dont ce dimensionnement peut être remanié pour répondre à ces hypothèses.

Aides (Ai)

La justification de la présence des influences est la suivante :
- **COS** - Si les risques sont mal identifiés alors la définition des plans d'actions peut être inadaptée aux risques réellement présents dans l'installation.
- **OC** - L'absence de contrôle sur les procédures, et les dérives potentielles (banalisation des déviances) qui peuvent survenir par rapport à ces dernières, ont un impact sur la qualité des aides. On considérera à minima les organismes de contrôle interne.
- **REX** - Si des problèmes au niveau des aides (outils, documents, procédures ...) ont été identifiés durant une action et qu'ils ne sont pas résolus au moment de refaire cette action, alors les problèmes risquent d'apparaître à nouveau du fait du non-traitement de ce dysfonctionnement.
- **PP** - Le temps, les budgets, les moyens et les ressources sont revus à la baisse mais les objectifs restent constants, ce qui peut avoir pour effet une mauvaise adéquation des outils et de la tâche à réaliser.
- **AR** - Si la définition des plans d'actions n'évolue pas au même rythme que les modifications du système alors les documents utilisés pour préparer l'action risquent de devenir caduques.

La justification de l'absence des influences est la suivante :
- **GQS** - Les aides définissent les documents et outils permettant aux collectifs de réaliser convenablement leurs activités. La définition du facteur organisationnel est axée sur les notions de formation, parcours professionnel, veille, tenue des habilitations ... Ces définitions ne permettent pas de faire un lien direct entre ce facteur organisationnel et cet item.
- **MT** - Si des problèmes apparaissent au niveau des aides cela provient d'autres facteurs (difficultés à faire vivre un retour d'expérience, pressions de production). Absence de connaissance suffisante

pour permettre une justification de la présence du lien.

Formation (Fo)

La justification de la présence des influences est la suivante :
- **GQS** - Si les plans de formation ne sont pas réactualisés (en fonction des évolutions du système socio-technique) alors la formation du personnel d'intervention risque de devenir insuffisante (partielle, absente ...).
- **OC** - La fonction de validation des programmes de formations n'est pas réalisée (ou que partiellement) par les organismes de contrôles concernés, pouvant ainsi aboutir à des formations inadaptées et/ou incomplètes.
- **MT** - Si la communication et la coordination sont défaillantes alors : certaines informations risquent d'être bloquées et non présentées dans les sessions de formations, et/ou la planification des sessions de formations et la participation des opérateurs à ces sessions peuvent être rendues difficiles.
- **REX** - La difficulté à faire vivre le retour d'expérience peut avoir pour conséquence une identification de certaines situations à risques biaisée (partielle ou absente), et donc une sensibilisation (partielle ou absente) du personnel d'intervention en ce qui concerne ces situations.
- **PP** - Le temps, les budgets, les moyens et les ressources sont revus à la baisse mais les objectifs restent constants, ce qui peut avoir pour effet de limiter le nombre, la durée des formations (car jugées non utile, à court terme, par rapport à l'aspect production).

La justification de l'absence des influences est la suivante :
- **COS** - La définition du facteur organisationnel, ainsi que ses marqueurs, sont axés sur le niveau de la culture de sûreté présent au sein de l'entreprise et non sur les moyens mis en œuvre pour aboutir à ce niveau de sûreté. L'item considéré est un des moyens permettant d'atteindre ce niveau de sûreté. D'où l'absence de lien entre ce facteur organisationnel et cet item.
- **AR** - La définition de l'item est axée sur l'aptitude du personnel d'intervention à réaliser certaines actions compte-tenu des formations qui lui sont proposées (organisées et suivies par le personnel d'encadrement). La définition du facteur organisationnel est axée sur la non réactualisation des hypothèses de dimensionnement technique et social compte-tenu du fonctionnement réel du système. De plus, l'absence de réexamen des hypothèses de conception est plutôt une activité à la charge des concepteurs. Ces définitions ne permettent pas de faire un lien direct entre ce facteur organisationnel et cet item.
  Si la définition de l'item était axée sur la construction de ces modules de formation (par l'encadrement) alors il y aurait un lien entre cet item et le facteur.

Expérience (Ex)

La justification de la présence des influences est la suivante :
- **GQS** - Si la gestion quotidienne de la sûreté est insuffisante ou déficiente, alors le risque de perte du savoir-faire (objectif du faire-faire, sous-traitance ...) est accru, et donc le niveau d'expérience peut être diminué.
- **PP** - Le manque de temps ne permet pas d'acquérir une expérience convenable. Les pressions de production ont eu une influence sur les actions passées, donc l'expérience acquise à ce sujet est biaisée (ou peut être une mauvaise expérience, habitudes de travail).

La justification de l'absence des influences est la suivante :
- **COS** - La définition du facteur organisationnel, ainsi que ses marqueurs, sont axés sur le niveau de la culture de sûreté présent au sein de l'entreprise et non sur les moyens mis en œuvre pour aboutir à ce niveau de sûreté. L'item considéré est un des moyens permettant d'atteindre ce niveau de sûreté (connaissances acquises par le collectif pour assurer, entre autre, cette sûreté). D'où l'absence de lien entre ce facteur organisationnel et cet item.
- **OC** - La définition de l'item est axée sur les connaissances acquises par les acteurs du collectif de travail dans l'exercice de leurs activités professionnelles. La définition du facteur organisationnel est axée sur le fonctionnement et l'influence des organismes de contrôles au sein (à l'extérieur) de l'entreprise. Ces définitions ne permettent pas de faire un lien direct entre ce facteur organisationnel et cet item.
- **MT** - Comme l'expérience a été définie au niveau de l'opérateur (lui permettant de tirer des conclusions sur les situations vécues), les notions de communication organisationnelle et de coordination n'ont pas de lien direct avec cet item.
- **REX** - On parle du processus au niveau du facteur organisationnel et du résultat au niveau de l'item (expérience du collectif de travail, c'est plus quelque chose de personnel/local qu'organisationnel). D'où l'absence de lien entre ce facteur organisationnel et cet item.
- **AR** - L'expérience s'acquiert en observant le fonctionnement réel de l'installation, les hypothèses de conception n'entrent pas en considération dans ce processus.

(possibilité de) Respect du cahier des charges (Rcc)

La justification de la présence des influences est la suivante :
- **COS** - Si les risques ont été mal identifiés (dans les analyses prévisionnelles) alors le personnel d'intervention ne pourra respecter que les recommandations et prescriptions décrites dans le cahier des charges (partielles par rapport aux situations rencontrées).
- **GQS** - La perte de savoir-faire et de compétences peut engendrer des déviances par rapport au contenu du cahier des charges (et donc aboutir au non-respect de ce dernier).
- **OC** - Les cahiers des charges des procédures accidentelles utilisées en centrales nucléaires sont contrôlées par le service sûreté de la centrale concernée. Si ce contrôle est partiel ou défaillant, le respect de ces procédures ne peut plus être prouvé.
- **MT** - La définition de l'item se focalise sur la communication/coordination (coopération, collaboration) présente dans le collectif de travail pour atteindre les objectifs fixés par le cahier des charges. S'il y a des problèmes de communication et de coordination généralisés au sein de l'entreprise, cela peut avoir une influence sur le respect de ce cahier des charges.
- **PP** - Le temps, les budgets, les moyens et les ressources sont revus à la baisse mais les objectifs restent constants, ce qui peut avoir pour conséquence de limiter les actions du personnel d'intervention (entraînant un non-respect de certains points du cahier des charges, favorisant les courts-circuits).

La justification de l'absence des influences est la suivante :
- **REX** - Le processus de retour d'expérience peut avoir une influence sur le collectif de travail mais pas sur le respect du cahier des charges.
- **AR** - Le facteur organisationnel traite des modifications dans le système qui ne sont pas mises à jour dans les documents, alors que l'on suppose que le cahier des charges est correct (au niveau de l'item). Si l'on crée un lien entre ce facteur organisationnel et cet item, on va à l'inverse des définitions proposées. D'où l'absence de lien entre ce facteur organisationnel et cet item.

Facteurs contextuels (Fe)

La justification de la présence des influences est la suivante :
- **MT** - La définition du facteur organisationnel est axée sur les notions de communication et de coordination, si des problèmes apparaissent à ce niveau, ceci peut avoir une influence négative sur l'action (exemple : le fait de transporter une pièce d'un local à un autre nécessite de coordonner différents services, de mettre à disposition le local et l'outillage ...).
- **REX** - Si les informations relatives aux incidents, presque-accidents et accidents dus à des événements contextuels, ne sont pas (ou que partiellement) recensées pour des actions similaires, alors le personnel d'intervention ne pourra être sensibilisé à ces notions.
- **PP** - Si le manque de temps, de budgets, de moyens et de ressources est étendu au système (ou localisé dans certains services), ceci engendre une effervescence, externe à l'action considérée, pouvant nuire à sa réalisation.
- **AR** - Si les informations concernant le système (techniques, humaines et organisationnelles) ne sont pas actualisées quand les conditions d'exploitation sont modifiées, alors le personnel d'intervention évolue dans ce système avec une vision caduque de ce dernier pouvant nuire à la réalisation de l'action. Par exemple, on supprime un éclairage dans un local sans l'indiquer dans les procédures.

La justification de l'absence des influences est la suivante :
- **COS** - On peut définir cet item comme étant le bruit englobant une action. On se focalise donc au niveau des mouvements (autres actions, déplacement géographiques de personnes/de pièces) pouvant avoir une influence sur l'action qui est en cours de réalisation. Cette vision amène au fait que le facteur organisationnel, permettant d'apprécier le niveau de la culture de sûreté présent au sein de l'entreprise, est trop globalisant pour avoir une influence directe sur cet item.
- **GQS** - Le facteur organisationnel est axé sur le personnel et son évolution, cette définition amène au fait que ce facteur aura une influence sur le collectif en charge de l'action. Or ce collectif ne fait pas partie des facteurs d'environnement mais est une composante principale de l'action considérée, un lien direct entre ce facteur organisationnel et cet item ne peut donc être défini.
- **OC** - La définition de l'item est axée sur les événements externes à l'action mais pouvant la conditionner. La définition du facteur organisationnel se focalise sur le fonctionnement et l'influence des organismes de contrôles au sein de l'entreprise. Ces définitions ne permettent pas de faire un lien direct entre ce facteur organisationnel et cet item.

Gestion collective et dynamique de groupe (Gcdg)

La justification de la présence des influences est la suivante :
- **COS** - Si la sûreté n'a pas sa place dans l'organisation alors le collectif de travail peut avoir un comportement visant à faire taire cette notion de sûreté (culture du blâme ...) et à travailler dans des conditions dangereuses sans le savoir.
- **GQS** - La définition du facteur et certains de ses marqueurs mentionnent la notion de transmission des savoir-faire, ce que l'on retrouve dans la composante métier de l'item.
- **MT** - Si le climat du site (luttes entre services, relations d'influence entre responsables ...) est négatif et/ou le mode d'organisation est inadapté au site, alors les informations peuvent mal circuler et entraîner une faible réactivité du collectif de travail.
- **REX** - L'item se positionne au niveau du métier (retour d'expérience du groupe) alors que le facteur organisationnel est vu comme un processus global à l'entreprise. De manière générale : comme on s'appuie sur les opérateurs (qui se font leur propre retour d'expérience), l'état du processus de retour d'expérience ne devrait pas influencer cet item. Mais si le processus de retour

d'expérience (global au site) est bien fait cela peut faciliter la gestion collective (du fait du climat dans lequel évoluent les opérateurs). C'est pourquoi un lien d'influence a été identifié entre ce facteur organisationnel et cet item.
- **PP** - Le temps, les budgets, les moyens et les ressources étant revus à la baisse avec des objectifs constants, un climat de stress peut apparaître et nuire à la bonne réalisation de l'intervention.

La justification de l'absence des influences est la suivante :
- **OC** - L'item se focalise sur la cohésion du collectif de travail durant la réalisation de l'action. La définition du facteur organisationnel est axée sur l'influence des organismes de contrôle au sein de l'entreprise. Ces définitions ne permettent pas de faire un lien direct entre ce facteur organisationnel et cet item.
- **AR** - Les hypothèses de conception doivent être étudiées avant la réalisation d'une action, alors que l'item se positionne dans le fonctionnement réel du système. Ce facteur organisationnel n'a donc pas de lien direct avec cet item. Ce sont deux niveaux de réflexion différents.

Contrôle et atteinte des objectifs (Cao)

La justification de la présence des influences est la suivante :
- **OC** - L'amélioration continue (qui inclut la notion de contrôle en temps-réel) se définit en partie par la notion de contrôle. Il y a donc un lien avec les organismes de contrôle. De plus le point-clé du processus de qualité est de participer à l'amélioration continue. Aujourd'hui, en interne, les organismes de contrôles sont submergés (plus au niveau des pressions de production). On peut également ajouter les problèmes de collusion entre les services qui peuvent influencer le déroulement des contrôles.
- **REX** - Le travail effectué durant le processus du retour d'expérience permet d'identifier les problèmes et de proposer des solutions pour les pallier (donc de participer à l'amélioration du fonctionnement du système). Si le retour d'expérience est défaillant alors les solutions proposées peuvent être partielles (ou dans le pire des cas absentes ou dangereuses).
- **PP** - Si le temps, les budgets, les moyens et les ressources sont revus à la baisse mais que les objectifs restent constants, alors certaines actions deviennent connexes aux actions de production et donc non prioritaires (car non productrices de valeurs à court-terme).
- **AR** - Si l'historique du système (contenant les étapes de conception et les hypothèses émises au départ) n'est pas connu, il ne peut y avoir d'amélioration continue.

La justification de l'absence des influences est la suivante :
- **COS** - La définition du facteur organisationnel est axée sur le niveau de la culture de sûreté présent au sein de l'entreprise. L'item se définit au travers des notions de contrôles et d'atteinte des objectifs. Ces définitions ne permettent pas de faire un lien entre ce facteur organisationnel et cet item.
- **GQS** - L'item vise à une amélioration des performances du système (technique, humaine et organisationnelle) via des contrôles et la vérification de l'atteinte des objectifs pour chaque action réalisée. Alors que le facteur organisationnel se focalise sur l'évolution du personnel (formation, tenue des habilitations ...) et sur la connaissance présente dans le système (sous-traitance). Ce facteur organisationnel n'a donc pas de lien direct avec cet item.
- **MT** - L'amélioration continue ne traite pas des notions de communication/coordination, aucun lien n'a donc pu être identifié entre ce facteur organisationnel et cet item.

Retour d'expérience (Rex)

La justification de la présence des influences est la suivante :
- **COS** - Certains marqueurs abordent des notions qui peuvent aller à l'encontre du retour d'expérience (blâme, dilution des activités de sûreté, non prise en compte des alertes). En particulier pour la culture du blâme : les gens auront beaucoup de mal à faire état de leurs difficultés.
- **GQS** - Le retour d'expérience se focalise sur l'analyse d'événements liés au fonctionnement du système, et le facteur organisationnel sur l'évolution du personnel et des connaissances qu'il a du système. Un lien existe donc entre ces notions (car sans connaissances sur le système, l'analyse d'événements risque de ne pas être exhaustive).
- **MT** - Le retour d'expérience est une démarche qui nécessite un ensemble de ressources humaines. Si des problèmes de communication et de coordination apparaissent au sein de l'entreprise, cela peut avoir une influence négative sur la constitution de ce retour d'expérience.
- **REX** - La pérennité du retour d'expérience lié à une action est conditionnée par l'évolution globale du système de collecte du retour d'expérience présent dans l'entreprise.
- **PP** - Si le temps, les budgets, les moyens et les ressources sont revus à la baisse mais que les objectifs restent constants, alors certaines actions deviennent connexes aux actions de production et donc non prioritaires (car non productrices de valeurs à court-terme).

La justification de l'absence des influences est la suivante :
- **OC** - La mise en place du retour d'expérience, sa collecte et son suivi dépendent plus de la culture de l'entreprise que des organismes de contrôles. Aucun lien n'a donc été identifié entre ce facteur organisationnel et cet item. Par contre, si la mise en place du retour d'expérience, spécifique à l'action étudiée, résulte d'une injonction des organismes de contrôles alors ce lien apparaît.
- **AR** - Comme le retour d'expérience est une analyse d'événements avérés, donc issus du fonctionnement réel, à partir desquels sont proposées des solutions, la référence aux hypothèses de conception n'est pas indispensable (car déjà prises en compte lors de la mise en place du système de retour d'expérience).

PHASES

Préparation (P)

La justification de la présence des influences est la suivante :
- **COS** - L'étape de préparation est l'étape dans laquelle les différents objectifs (sûreté, disponibilité, durabilité) sont étudiés et pour lesquels les objectifs à atteindre sont définis. Si la culture de sûreté n'est pas développée au sein de l'entreprise, le risque est de privilégier par exemple les aspects disponibilité et durabilité (en lien direct avec l'aspect production) au dépend de l'aspect sûreté.
- **GQS** - Si les personnes en charge de l'action n'ont pas les compétences requises alors la préparation de cette action risque d'être incomplète voire erronée (oubli de matériel, procédure à suivre non connue ...).
- **OC** - Les organismes de contrôle interviennent, dans l'étape de préparation, au niveau des procédures, aides et formations.
- **MT** - Si pour une action il est nécessaire de solliciter plusieurs acteurs/collectifs (appartenant à des unités différentes), il apparaît qu'une mauvaise communication et/ou coordination dans l'étape de préparation peut détériorer/ralentir cette étape.
- **REX** - En phase de préparation, il est nécessaire de prendre connaissance des derniers éléments du retour d'expérience concernant l'action afin d'éviter de reproduire les mêmes erreurs.

- **PP** - Si le temps, les budgets, les moyens et les ressources sont revus à la baisse avec des objectifs constants, alors l'étape de préparation risque d'être réalisée partiellement (voire non réalisée).
- **AR** - En phase de préparation, il est nécessaire de réfléchir à l'adaptation des principes de conception à la réalité du moment. On se base à la fois sur les documents prescriptifs, sur les documents opératoires issus du fonctionnement réel du système et sur le retour d'expérience disponible. Une réflexion sur les aides, qui sont un reflet de la vision du fonctionnement du système, permet de les adapter à l'action (formalisation de la modification) qui va être réalisée (par rapport à ce qui était fait avant).

Réalisation (R)

La justification de la présence des influences est la suivante :
- **COS** - Ce facteur permet d'apprécier le niveau de la culture de sûreté présent au sein de l'entreprise. Si ce niveau n'est pas assez important alors le collectif peut évoluer dans des situations à risques qu'il n'aura pas su identifier.
- **GQS** - Si les personnes en charge de l'action n'ont pas les compétences requises alors la réalisation de cette action risque d'être inefficace (*i.e.* ne répondant pas aux finalités pour lesquelles elle a été mise en place) et aboutir à des situations à risques.
- **MT** - Si pour une action il est nécessaire de solliciter plusieurs acteurs/collectifs (appartenant à des unités différentes), il apparaît qu'une mauvaise communication et/ou coordination peut détériorer/ralentir l'étape de réalisation de l'action.
- **REX** - C'est un facteur organisationnel qui intervient principalement en amont et à la suite de la réalisation de l'action. En effet, en phase de préparation, il est utile pour avoir un historique des événements concernant cette action et, en phase de clôture, il permet d'actualiser les connaissances liées à cette action. Mais il est nécessaire de le considérer en phase de réalisation car un mauvais retour d'expérience engendre une connaissance imparfaite des situations à risques (qui peuvent apparaître durant la réalisation de l'action).
- **PP** - Si le temps, les budgets, les moyens et les ressources sont revus à la baisse avec des objectifs constants, alors l'étape de réalisation risque d'être effectuée hâtivement (en ignorant certaines phases critiques ...) et aboutir à des situations à risques.

La justification de l'absence des influences est la suivante :
- **OC** - Ce facteur organisationnel intervient principalement en amont et en aval de la réalisation de l'action, dans les processus de contrôles.
- **AR** - Ce facteur organisationnel n'est pas envisageable dans l'étape de réalisation car le réexamen des hypothèses de conception ne peut être envisagé que dans une phase stable du système. Or l'étape de réalisation est celle qui va conditionner le plus fortement le processus de changement (c'est la phase la moins stable de l'action et donc la plus sujette à risques).

Clôture (C)

La justification de la présence des influences est la suivante :
- **GQS** - Le facteur organisationnel est focalisé sur l'adéquation tâche/compétences (via les formations, la transmission des savoir-faire ...). L'étape de clôture permet d'actualiser la connaissance que l'on a sur une partie du système. Cette connaissance peut se transmettre via les formations, le retour d'expérience, le compagnonnage ... De ce fait la défaillance dans la gestion quotidienne de la sûreté peut engendrer des difficultés pour la phase de clôture (informations recueillies incomplètes ...).
- **OC** - L'étape de clôture englobe la notion de contrôles (permettant de veiller au bon déroulement

d'une action). Si les organismes de contrôles sont peu présents ou que leur influence est faible, il pourra être plus facile de contourner leurs recommandations et injonctions.
- **MT** - Cette étape de clôture vise à assurer la continuité de l'action dans le système. Il est donc nécessaire que les informations concernant cette action circule correctement (si la communication est défaillante alors la pérennité de l'action risque d'être malmenée).
- **REX** - Une fois que l'action a été réalisée, le retour d'expérience permet de capitaliser et d'analyser les dysfonctionnements qui ont pu survenir afin qu'ils ne réapparaissent pas lors de la prochaine itération de l'action. Si le fonctionnement du retour d'expérience est défaillant alors certains dysfonctionnements peuvent réapparaître d'une itération de l'action à une autre.
- **PP** - Si le temps, les budgets, les moyens et les ressources sont revus à la baisse avec des objectifs constants, alors cette étape de l'action peut être ignorée (car non productrice de valeurs à court-terme, par rapport à la production).
- **AR** - L'étape de clôture permet d'identifier les manques relatifs à l'action qui vient d'être réalisée pour proposer des améliorations permettant de combler ces manques. Ceci sera d'autant plus efficace si les hypothèses de conception sont accessibles, mises à jours ...

La justification de l'absence des influences est la suivante :
- **COS** - La définition de cette étape est axée sur les moyens permettant d'assurer la pérennité de l'action dans le système. Le facteur organisationnel est axé sur le niveau de la culture de sûreté présent au sein de l'entreprise. Ces définitions ne permettent pas de faire un lien entre ce facteur organisationnel et cette étape de l'action.

E : Justification des influences FOP-items pour le cas d'application

Dans cette annexe, nous développons la justification des simplifications apportées aux configurations humaines et organisationnelles des actions d'étalonnage du capteur, et de surveillance des tresses.
Rappelons que ces simplifications ne sont valables que dans le cadre d'un contexte organisationnel donné. En d'autres termes, si ce contexte venait à être modifié, alors ces simplifications (et les justifications associées) devraient être reconsidérées.

Justification des simplifications pour l'action d'étalonnage du capteur

Cette configuration particulière se justifie de la manière suivante :

Items	FOP	Justification de l'absence de l'influence
De	PP, MT	Cette action est toujours réalisée par un binôme du service maintenance (dont au moins un des opérateurs fait partie du binôme dédié spécifiquement à cette action, et est en charge des tâches les plus complexes). Si les opérateurs de ce binôme spécifique sont absents alors l'action n'est pas réalisée. La délégation est ici bien organisée et les personnes compétentes clairement identifiées.
Fo	OC	Il n'y a pas de formation particulière nécessaire à la réalisation de cette action (hormis l'habilitation électrique que possède le binôme spécifique), c'est plus du compagnonage qui est utilisé ici. Les organismes de contrôles n'interviennent donc pas dans ce processus.
Fo	MT	La structure organisationnelle du site X est relativement simple (peu de personnel et peu de niveaux hiérarchiques), l'action est toujours coordonnée par un personne experte de cette dernière, et il n'y a pas de formation spécifique pour cette action. La complexité organisationnelle n'influence donc pas cet item.
Ex	GQS	Comme cette action est toujours réalisée en présence d'un des opérateurs dédié à cette action, le risque de perte de savoir-faire est considéré (au moment de l'analyse) comme étant absent. De plus cette action est réalisée sur un élément EIPS, et la politique de maintenance du site X n'autorise pas de sous-traitance pour ce type de matériel.
Ex	PP	Les pressions de production ont peu d'influence sur le personnel du service maintenance, et cette action se fait toujours en présence d'une personne experte (qui connaît bien le comportement du sous-système considéré). De ce fait, l'influence n'a pas été identifiée pour cette configuration.
Rcc	GQS	Comme le risque de perte de savoir-faire est absent (cf. absence de lien entre Ex et GQS), le risque de déviation par rapport au cahier des charges peut être également considéré comme absent.

Rcc	OC	Il n'y a pas d'organisme de contrôles (interne ou externe) dédié à la validation de ce cahier des charges (rappel : peu de modes opératoires de maintenance sont formalisés pour cette installation).
Rcc	MT	La complexité organisationnelle n'influence pas cet item car la communication et la coordination de cette action sont assurées par la présence d'un opérateur expert de cette dernière.
Fe	MT	La réalisation de cette action ne sollicite que le service maintenance et est effectuée lors des arrêts programmés. L'apparition de problèmes de communication/coordination est minimisée par les réunions hebdomadaires entre les équipes de production et le service maintenance.
Fe	PP	De part la localisation du matériel (au niveau du toit du silo), le service concerné (la maintenance) et la planification de la réalisation de cette action (lors des arrêts programmés), l'influence des pressions de production sur les facteurs d'environnement de cette action est considéré comme absente.
Gcdg	MT	Le collectif de travail étant réduit (deux personnes), bien organisé (présence d'un opérateur expert lors de la réalisation de l'action), et non concerné par les récentes restructurations (qui touchent plus l'encadrement), le risque de mauvaise circulation des informations est considéré comme absent (du fait également de la simplicité de la structure organisationnelle).
Cao	OC	Il n'y a pas d'organisme (interne ou externe) dédié aux contrôles de cette action. Aucune influence ne peut donc être identifiée.
Cao	AR	Comme cette action est toujours réalisée en présence d'un opérateur expert de ce sous-système (et interne à l'entreprise), qui possède l'historique du sous-système concerné, l'amélioration continue se fait naturellement.
Rex	MT	Le retour d'expérience est collecté (dans une base de données dédiée) par les opérateurs en charge de l'action. Le risque de problèmes de coordination/communication est alors considéré comme absent.

TAB. E.1 - Justification de la simplification de la configuration humaine et organisationnelle pour l'action d'étalonnage du capteur de détection d'oxygène

Justification des simplifications pour l'action de surveillance des tresses

Cette configuration particulière se justifie de la manière suivante :

Items	FOP	Justification de l'absence de l'influence
De	PP, MT	Cette action fait partie des tâches habituelles des équipes de production (maintenance de premier niveau). Elle est donc incluse dans l'évaluation de la charge de travail et peut-être réalisée par n'importe quel opérateur de production. Les influences des pressions de production et de la complexité organisationnelle n'ont donc pas été identifiées.
Ai	COS, PP, OC, REX, AR	Cette surveillance étant simple et réalisée de manière visuelle lors de rondes, l'opérateur n'a pas besoin de mode opératoire précis ni d'outils spécifiques. Si une aide est toutefois nécessaire, il est d'usage d'utiliser le compagnonage. Aucune influence des facteurs organisationnels n'a été identifiée.
Fo	OC	Il n'y a pas de formation particulière nécessaire à la réalisation de cette action du fait de la simplicité de la tâche. Il est d'usage, comme précédemment, d'utiliser le compagnonage pour guider le nouvel opérateur. Les organismes de contrôles n'interviennent donc pas dans ce processus.
Fo	MT	La structure organisationnelle du site X est relativement simple (peu de personnel et peu de niveaux hiérarchiques), l'action est integrée dans les activités des équipes de production (définie lors de l'affectation des rondes), et il n'y a pas de formation spécifique pour cette action. La complexité organisationnelle n'influence donc pas cet item.
Ex	GQS	Comme cette action est toujours réalisée par une personne de l'équipe production (en effet ces éléments étant EIPS, la maintenance n'est pas sous-traitée), le risque de perte de savoir-faire est considéré (au moment de l'analyse) comme étant absent.
Rcc	COS	Les éléments considérés étant EIPS, les risques ont été précisément identifiés (et remis à jour lors de la nouvelle étude réalisée pour la nouvelle directive ATEX, [Parlement européen et Conseil, 2000]) et de plus, l'action est réalisée par du personnel interne au site X (qui a une bonne connaissance du système considéré). Ces différents éléments permettent, pour cette action, de retirer cette influence.
Rcc	OC	Il n'y a pas d'organisme de contrôles (interne ou externe) pour vérifier le contenu du cahier des charges. Aucun lien d'influence n'a donc pu être identifié.
Rcc	MT	L'action est réalisée par un seul opérateur, et est commune à tous les opérateurs de production. Le risque de problème de communication et de coordination (pouvant géner l'atteinte des objectifs fixés par le cahier des charges) est ici considéré comme absent.
Fe	MT	L'action est réalisée par un seul opérateur, ne nécessite aucun mouvement de matériel (donc pas de coordination avec d'autres services) et est réalisable par l'ensemble des opérateurs de production. Le risque de problème de communication et de coordination (pouvant géner la réalisation de cette action) est ici considéré comme absent.
Gcdg	COS, PP, GQS, OC, MT, REX, AR	L'action est réalisée par un seul opérateur et est planifiée lors de l'affectation des rondes en réunion hebdomadaire. L'existance d'un collectif de travail, pour la réalisation de cette action, n'a donc pas été identifiée. De ce fait, aucune influence des facteurs organisationnels n'a pu être définie.
Cao	OC	Du fait de la simplicité de l'action, l'organisation en place n'a pas jugée nécessaire d'y adjoindre un contrôle dédié. Aucune influence ne peut donc être identifiée.

Rex	COS	Les éléments considérés étant EIPS, il existe une base de données qui est renseignée par l'opérateur en fin d'action (volonté du site d'intégrer la sécurité à tous les niveaux). Aucun lien d'influence n'a donc pu être identifié lors de l'analyse.
Rex	MT	L'opérateur en charge de l'action renseigne dans une base de données dédiée, les problèmes identifiés lors de la réalisation de cette action (cette étape confirme la finalisation de l'action). Aucun problème de communication/coordination n'a été identifié à ce niveau.

TAB. E.2 - Justification de la simplification de la configuration humaine et organisationnelle pour l'action de surveillance des tresses de continuité électrique

F : Classeur Excel pour la construction des tables de probabilités

Cette annexe permet de décrire la manière dont les tables de probabilités conditionnelles du cas d'application ont été construites.

Le classeur utilisé est organisé de la manière suivante :

N° feuille	Intitulé feuille	Contenu de la feuille
Feuille 0	Modèle	Cette feuille décrit le modèle graphique utilisé et associe les différentes feuilles du classeur aux variables de ce modèle.
Feuille 1	Utilisation du classeur	Cette feuille donne des précisions quant à l'utilisation de ce document.
Feuille 2	Abréviations	Cette feuille décrit les variables utilisées dans le modèle et définit les abréviations utilisées dans la suite du document.
Feuille 3	Table facteurs (alphas)	Cette feuille permet de renseigner les valeurs des alphas qui seront utilisés pour la quantification des influences.
Feuille 4	Distributions initiales	Cette feuille permet de renseigner les distributions initiales (i.e. dans un contexte complètement favorable) des variables utilisées dans le modèle.
Feuille 5	Alpha-Fo-Items	Cette feuille permet de quantifier les facteurs d'aggravation existant entre les facteurs organisationnels et les items.
Feuille 6	Alpha-Fo-PRC	Cette feuille permet de quantifier les facteurs d'aggravation existant entre les facteurs organisationnels et les phases de l'action.
Feuille 7	Alpha-Items-PRC	Cette feuille permet de quantifier les facteurs d'aggravation existant entre les items et les phases de l'action.
Feuille 8	Alpha-PRC-Efficacité	Cette feuille permet de quantifier les facteurs d'aggravation existant entre les phases de l'action et l'efficacité de cette dernière.
Feuille 9	Alpha-Efficacité-Disponibilité	Cette feuille permet de quantifier les facteurs d'aggravation existant entre l'efficacité de l'action et le disponibilité du composant technique de la barrière.
Feuilles 10 à 18	TPC-Items	Ces feuilles contiennent les tables de probabilités conditionnelles relatives aux items d'une action.
Feuilles 19 à 21	TPC-Phases	Ces feuilles contiennent les tables de probabilités conditionnelles relatives aux phases de l'action.
Feuille 22	TPC-Efficacité	Cette feuille contient la table de probabilités conditionnelles relative à l'efficacité de l'action.
Feuille 23	TPC-Disponibilité-Intrinsèque	Cette feuille contient la table de probabilités conditionnelles relative à la disponibilité intrinsèque du composant technique de la barrière.
Feuille 24	TPC-Disponibilité-Op-Cpt	Cette feuille contient la table de probabilités conditionnelles relative à la disponibilité initiale/opérationnelle du composant technique de la barrière.
Feuille 25	TPC-Disponibilité-Op-Bar	Cette feuille contient la table de probabilités conditionnelles relative à la disponibilité opérationnelle de la barrière.

Légende	
	Feuilles de description, d'explicitation des caractéristiques du classeur et du modèle.
	Feuilles à renseigner avec le groupe de travail.
	Feuilles dont le contenu devra être copié dans le modèle sous BayesiaLab.

FIG. F.1 - Organisation du classeur Excel utilisé pour le cas d'application

Étape 1 : Définir les valeurs quantifiées de l'échelle d'élicitation d'avis d'experts (cf. figure F.2 et annexe G de ce mémoire).

Table facteurs (alphas)

Paramètres	Alphas
Pas d'impact	1
Peu d'impact	0,95
Impact	0,75
Impact important	0,5
Impact total	0,01

Retour sommaire
Retour Modèle
Retour 'Utilisation du classeur'

FIG. F.2 - Feuille du classeur dédiée à la définition des valeurs de l'échelle

Étape 2 : Renseigner les valeurs des distributions initiales pour les facteurs organisationnels

pathogènes, les items, les phases, l'efficacité de l'action considérée, ainsi que les disponibilités (intrinsèque et opérationnelle) du composant considéré (cf. figure F.3).

Distributions initiales

Facteurs organisationnels	Non pathogène	Pathogène
COS	99	1
GQS	99	1
OC	99	1
MT	99	1
REX	99	1
PP	99	1
AR	99	1

Items	Présent	Dégradé
De	99	1
Ai	99	1
Fo	99	1
Ex	99	1
Rcc	99	1
Fe	99	1
Gcdg	99	1
Ac	99	1
Rex	99	1

Phases de l'action	Efficace	inefficace
P	99	1
R	99	1
C	99	1

Efficacité de l'action	Efficace	Inefficace
Action	99	1

Disponibilité intrinsèque	Disponible	Indisponible	Absent
Di0	98	2	0

Disponibilité opérationnelle	Disponible	Indisponible	Absent
Do	100	0	0

Retour sommaire
Retour modèle
Retour 'Utilisation du classeur'

FIG. F.3 - Feuille du classeur dédiée à la définition des distributions initiales

Étape 3 : Renseigner pour chaque lien identifié (facteurs organisationnels-items, items-phases de l'action, phases de l'action-efficacité, efficacité de l'action-disponibilité du composant) l'importance de l'impact.
Un exemple est donné au travers de la figure F.4 pour les liens identifiés entre les facteurs organisationnels et les items Délégation (De), Aides (Ai) et Formation (Fo).

Facteurs d'aggravation
Facteurs organisationnels-Items

Facteurs	Item	Alpha
COS	De	1
GQS	De	1
OC	De	1
MT	De	1
REX	De	1
PP	De	1
AR	De	1
COS	Ai	0,95
GQS	Ai	1
OC	Ai	0,75
MT	Ai	1
REX	Ai	0,95
PP	Ai	0,95
AR	Ai	0,75
COS	Fo	1
GQS	Fo	0,95
OC	Fo	1
MT	Fo	1
REX	Fo	0,95
PP	Fo	0,95
AR	Fo	1

FIG. F.4 - Quantification des liens entre les FOP et les items De, Ai et Fo

Les valeurs définies dans les étapes 1 à 3 sont valables pour l'ensemble du classeur (utilisation d'étiquettes sous Excel).

Étape 4 : Copier le contenu de chacune des tables calculées (automatiquement) sous Excel vers la table de probabilités conditionnelles de la variable concernée du modèle sous BayesiaLab.
Un exemple est donné au travers de la figure F.5 pour la table de probabilités conditionnelles associée à la variable Formation.

			Item	Formation
GQS	REX	PP	Présent	Dégradé
Absent	Absent	Absent	99	1
Absent	Absent	Présent	94,05	5,95
Absent	Présent	Absent	94,05	5,95
Absent	Présent	Présent	89,3475	10,6525
Présent	Absent	Absent	94,05	5,95
Présent	Absent	Présent	89,3475	10,6525
Présent	Présent	Absent	89,3475	10,6525
Présent	Présent	Présent	84,880125	15,119875

Retour sommaire
Retour modèle
Retour 'Utilisation du classeur'

FIG. F.5 - Table de probabilités conditionnelles pour la variable Formation

G : Élaboration de l'échelle d'élicitation d'avis d'experts

L'échelle semi-quantitative utilisée pour le cas d'application traité (dans le chapitre 4 de ce mémoire) a été construite en suivant les règles décrite dans cette annexe.

Règle A : Définir un nombre de modalités sur l'échelle qui reste dans les limites du discernement humain (pas plus de 7 modalités, [Roberts, 1994], [Léger, 2005], [Voisin *et al.*, 2005]) et qui soit adapté aux besoins de l'étude.
Dans notre cas, nous avons choisi une échelle à cinq niveaux afin de pouvoir représenter une graduation plus fine (Impact Faible, Impact Important) entre un impact moyen (Impact) et les modalités aux limites de l'échelle (Pas/Peu d'Impact, Impact Total).

Règle B : Les valeurs quantifiées associées à chacun des paramètres doivent être : différentes pour chaque modalité, croissantes (de Pas/Peu d'Impact à Impact Total) et comprises dans l'intervalle [0, 1] (pour avoir une valeur de probabilité qui ne dépasse pas 1). Dans notre cas, cela se traduit par la règle suivante :
$1 \geq$ valeur(Pas/Peu d'Impact) $>$ valeur(Impact Faible) $>$ valeur(Impact) $>$ valeur(Impact Important) $>$ valeur(Impact Total) ≥ 0.

Règle C : Sur cette échelle à cinq niveaux, la modalité Impact constitue la modalité centrale. Cela signifie que cette modalité peut prendre toutes les valeurs dans l'intervalle]0,1[(mais elle se trouve généralement autour de la valeur 0.5).

Règle D : La logique de dégradation (cf. partie 3.3) implique, du fait de l'opérateur utilisé, qu'un impact faible ne peut dégrader fortement la distribution concernée (et inversement, un impact fort ne peut dégrader faiblement la distribution concernée).
Cela signifie que certaines valeurs ne sont pas utilisables pour certaines modalités. En effet, les modalités les plus impactantes ne peuvent prendre que des valeurs comprises dans l'intervalle [0, 0.5] alors que les modalités les moins impactantes se situent dans l'intervalle [0.5, 1].

Nous proposons les intervalles suivants pour les différentes modalités de l'échelle :

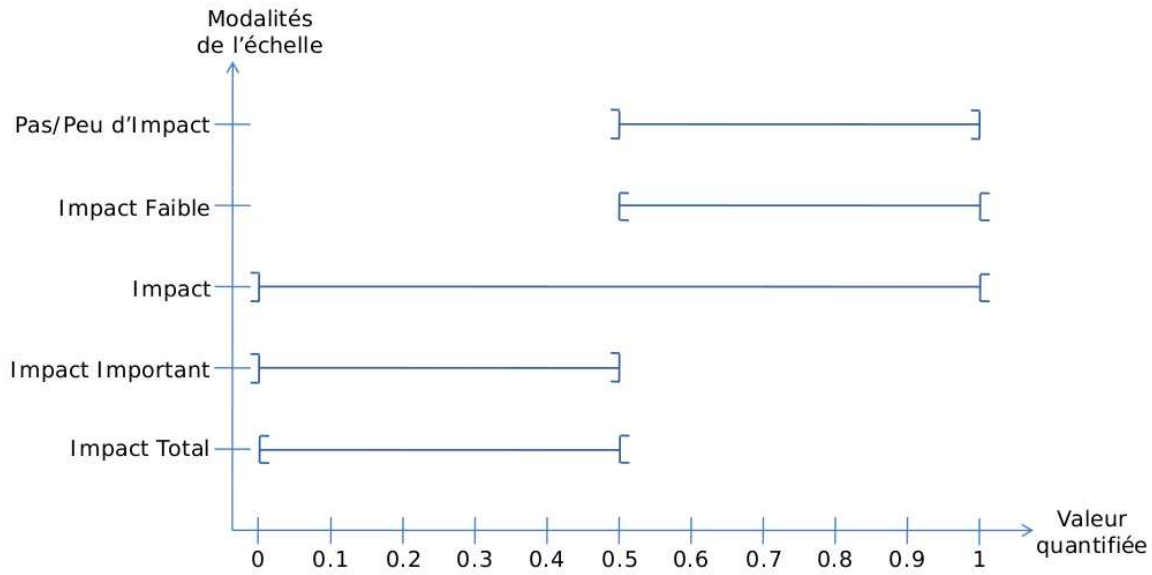

FIG. G.1 - Intervalles de valeurs possibles pour les modalités de l'échelle

Un exemple d'élaboration des valeurs quantifiées des modalités de l'échelle semi-quantitative est proposé dans la suite de cette annexe :

Étape 1 : On fixe la modalité centrale (Impact). Dans notre cas, Valeur(Impact) = 0.75 (cf. figure G.2). Les modalités restantes doivent donc être différentes de 0.75.

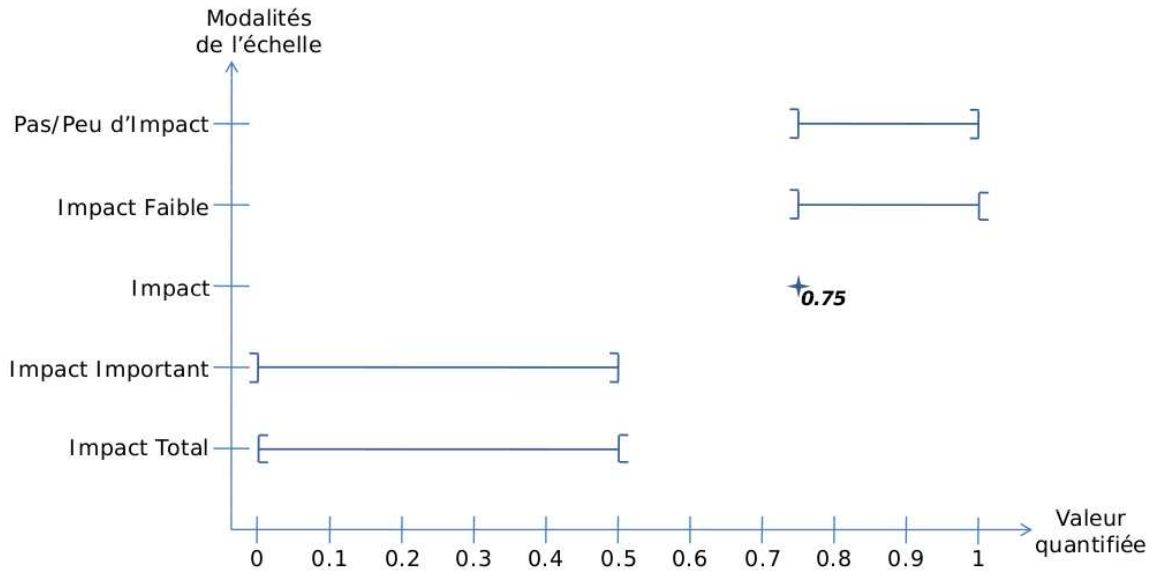

FIG. G.2 - Intervalles de valeurs libres après choix d'une valeur pour la modalité Impact

Étape 2 : On fixe ensuite les modalités adjacentes à la modalité centrale (valeur(Impact Faible) = 0.95 et valeur(Impact Important) = 0.5, cf. figure G.3). On raisonne ainsi de proche en proche pour fixer l'ensemble des modalités de l'échelle.

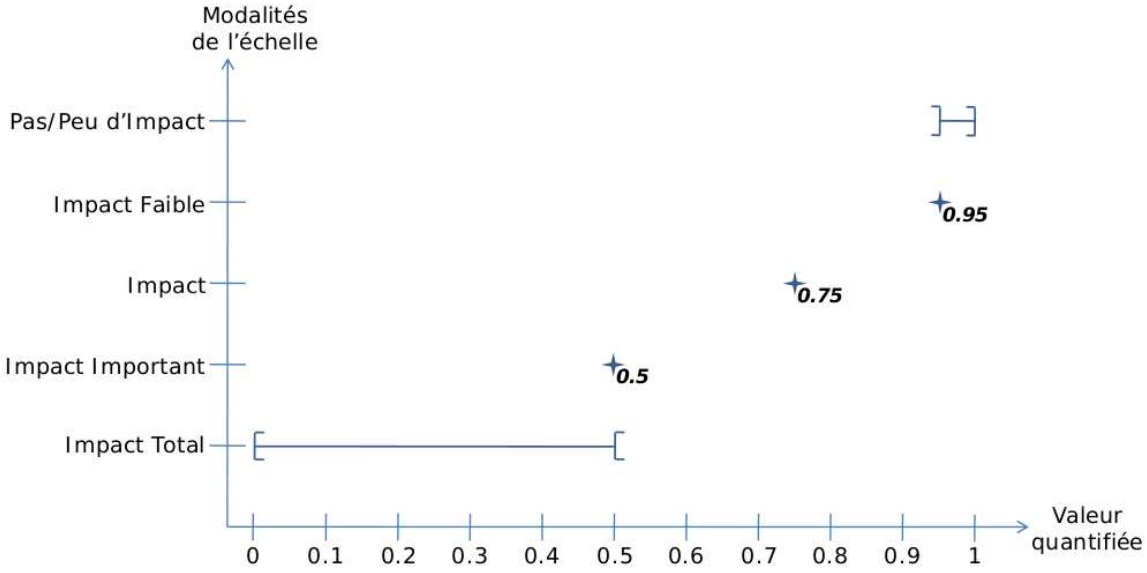

FIG. G.3 - Intervalles de valeurs libres après choix de valeurs pour les modalités Impact Faible et Impact Important

Dans cet exemple on sait à présent que valeur (Pas/Peu d'Impact) > 0.95, et que valeur(Impact Total) < 0.5 (cf. figure G.4).

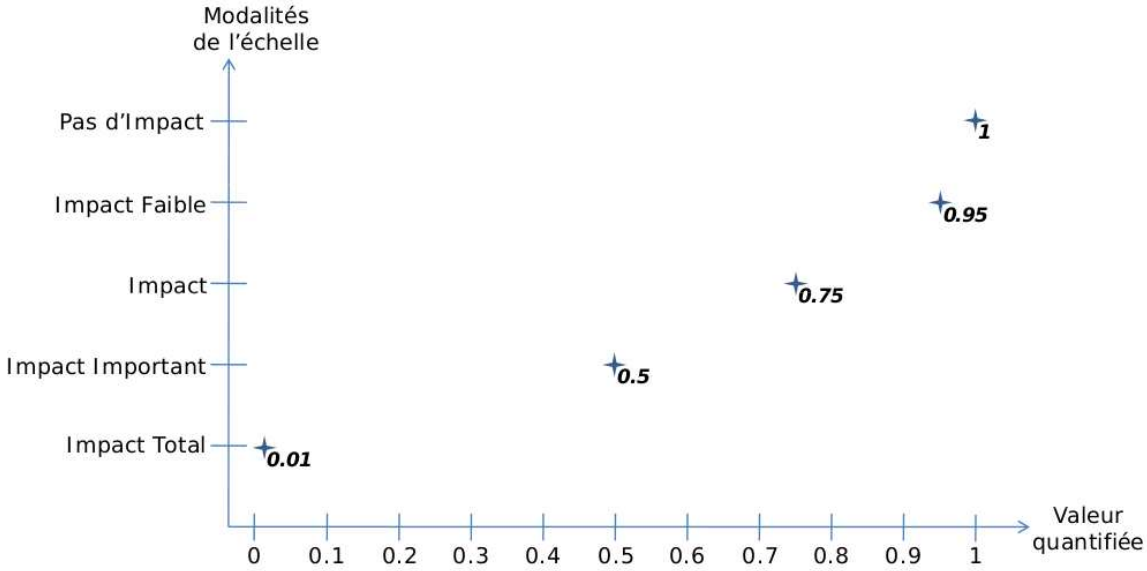

FIG. G.4 - Proposition de valeurs quantifiées pour l'échelle d'élicitation d'avis d'experts

Étape 3 : L'échelle semi-quantitative ainsi obtenue doit ensuite faire l'objet d'études de sensibilités (via le modèle de risques, mais aussi par le biais d'études statistiques).
Dans le cadre du cas d'application développé dans le chapitre 4 de ce mémoire, nous proposons de faire une première étude de sensibilité avec les échelles définies dans la figure G.5.

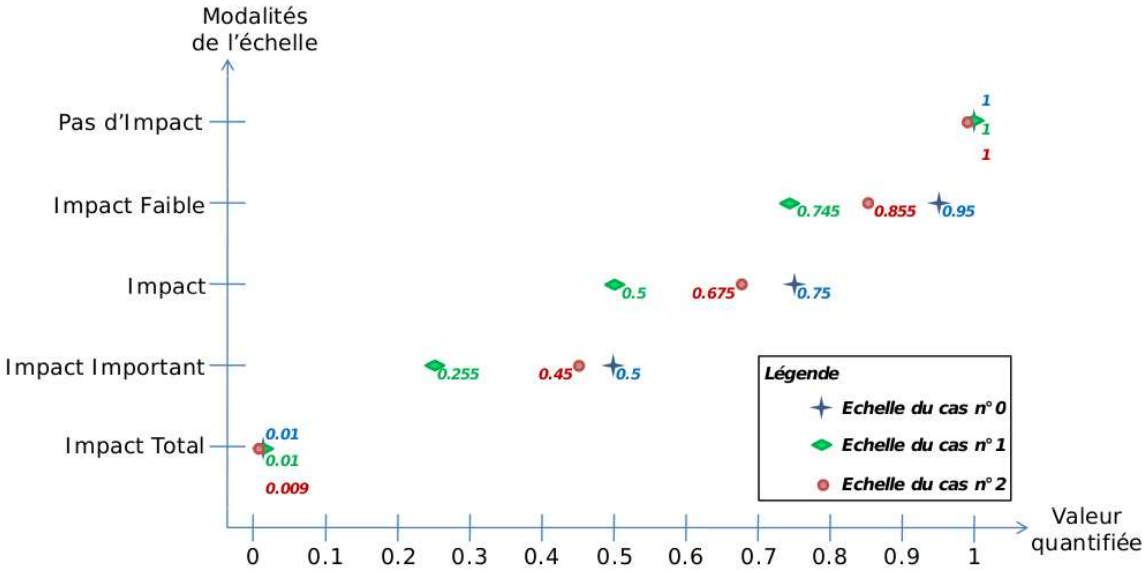

FIG. G.5 - Différentes valeurs quantifiées pour l'échelle d'élicitation d'avis d'experts (études de sensibilité)

H : Valeurs quantifiées du cas d'application

Cette annexe permet de donner les valeurs des probabilités associées aux variables du modèle pour les différents cas traités dans le chapitre applicatif de ce mémoire de thèse.

1. Cas de simulation : Présence du caractère pathogène des facteurs organisationnels AR, PP et COS

1.1. Modification des valeurs quantifiées de l'échelle de dégradation

1.1.1. Cas n°1

Variable du modèle	Modalité	AR, PP et COS présents
Étalonnage du capteur	Inefficace	93.75
Disponibilité opérationnelle de la détection d'oxygène à 5%	Indisponible	70.71
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	70.98
Surveillance des tresses	Inefficace	74.36
Disponibilité opérationnelle des tresses	Indisponible	19.02
Impact sûreté	Présent	1.07

Tab. H.1 - État de certaines variables du système (en %) en présence des trois FOP

Variable du modèle	Modalité	AR présent	PP présent	COS présent
Étalonnage du capteur	Inefficace	70.49	65.84	63.10
Disponibilité opérationnelle de la détection d'oxygène à 5%	Indisponible	53.68	50.28	48.28
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	54.10	50.73	48.74
Surveillance des tresses	Inefficace	34.05	70.80	6.54
Disponibilité opérationnelle des tresses	Indisponible	8.72	18.11	1.70
Impact sûreté	Présent	0.47	0.73	0.22

TAB. H.2 - État de certaines variables du système (en %) en présence d'un des FOP

1.1.2. Cas n°2

Variable du modèle	Modalité	AR, PP et COS présents
Étalonnage du capteur	Inefficace	69.33
Disponibilité opérationnelle de la détection d'oxygène à 5%	Indisponible	39.84
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	40.38
Surveillance des tresses	Inefficace	37.91
Disponibilité opérationnelle des tresses	Indisponible	5.56
Impact sûreté	Présent	0.27

TAB. H.3 - État de certaines variables du système (en %) en présence des trois FOP

Variable du modèle	Modalité	AR présent	PP présent	COS présent
Étalonnage du capteur	Inefficace	41.16	36.04	34.38
Disponibilité opérationnelle de la détection d'oxygène à 5%	Indisponible	24.64	21.88	20.98
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	25.32	22.58	21.69
Surveillance des tresses	Inefficace	13.09	34.34	3.83
Disponibilité opérationnelle des tresses	Indisponible	1.95	5.04	0.60
Impact sûreté	Présent	0.11	0.14	0.08

TAB. H.4 - État de certaines variables du système (en %) en présence d'un des FOP

1.2. Modification des distributions initiales - aspects humains et organisationnels

1.2.1. Cas n°3

Variable du modèle	Modalité	AR, PP et COS présents
Étalonnage du capteur	Inefficace	46.14
Disponibilité opérationnelle de la détection d'oxygène à 5%	Indisponible	25.17
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	25.84
Surveillance des tresses	Inefficace	24.14
Disponibilité opérationnelle des tresses	Indisponible	1.27
Impact sûreté	Présent	0.10

TAB. H.5 - État de certaines variables du système (en %) en présence des trois FOP

Variable du modèle	Modalité	AR présent	PP présent	COS présent
Étalonnage du capteur	Inefficace	29.49	17.31	13.10
Disponibilité opérationnelle de la détection d'oxygène à 5%	Indisponible	17.02	9.10	9.00
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	17.77	9.92	9.82
Surveillance des tresses	Inefficace	4.36	21.93	0.03
Disponibilité opérationnelle des tresses	Indisponible	0.27	1.16	0.05
Impact sûreté	Présent	0.06	0.04	0.03

TAB. H.6 - État de certaines variables du système (en %) en présence d'un des FOP

1.2.2. Cas n°4

Variable du modèle	Modalité	AR, PP et COS présents
Étalonnage du capteur	Inefficace	46.40
Disponibilité opérationnelle de la détection d'oxygène à 5%	Indisponible	25.30
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	25.97
Surveillance des tresses	Inefficace	24.28
Disponibilité opérationnelle des tresses	Indisponible	1.28
Impact sûreté	Présent	0.10

TAB. H.7 - État de certaines variables du système (en %) en présence des FOP

Variable du modèle	Modalité	AR présent	PP présent	COS présent
Étalonnage du capteur	Inefficace	29.87	13.80	17.58
Disponibilité opérationnelle de la détection d'oxygène à 5%	Indisponible	17.21	9.34	9.23
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	17.95	10.15	10.05
Surveillance des tresses	Inefficace	4.61	22.09	0.30
Disponibilité opérationnelle des tresses	Indisponible	0.28	1.16	0.07
Impact sûreté	Présent	0.06	0.04	0.03

TAB. H.8 - État de certaines variables du système (en %) en présence d'un des FOP

1.2.3. Cas n°5

Variable du modèle	Modalité	AR, PP et COS présents
Étalonnage du capteur	Inefficace	54.16
Disponibilité opérationnelle de la détection d'oxygène à 5%	Indisponible	29.10
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	29.74
Surveillance des tresses	Inefficace	28.95
Disponibilité opérationnelle des tresses	Indisponible	1.51
Impact sûreté	Présent	0.12

TAB. H.9 - État de certaines variables du système (en %) en présence des trois FOP

Variable du modèle	Modalité	AR présent	PP présent	COS présent
Étalonnage du capteur	Inefficace	40.96	28.15	27.81
Disponibilité opérationnelle de la détection d'oxygène à 5%	Indisponible	22.63	16.36	16.20
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	23.33	17.12	16.95
Surveillance des tresses	Inefficace	12.18	27.08	8.60
Disponibilité opérationnelle des tresses	Indisponible	0.66	1.42	0.48
Impact sûreté	Présent	0.08	0.07	0.06

TAB. H.10 - État de certaines variables du système (en %) en présence d'un des FOP

1.2.4. Cas n°6

Variable du modèle	Modalité	AR, PP et COS présents
Étalonnage du capteur	Inefficace	70.39
Disponibilité opérationnelle de la détection d'oxygène à 5%	Indisponible	37.04
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	37.61
Surveillance des tresses	Inefficace	40.30
Disponibilité opérationnelle des tresses	Indisponible	2.08
Impact sûreté	Présent	0.17

Tab. H.11 - État de certaines variables du système (en %) en présence des trois FOP

Variable du modèle	Modalité	AR présent	PP présent	COS présent
Étalonnage du capteur	Inefficace	63.34	56.59	56.18
Disponibilité opérationnelle de la détection d'oxygène à 5%	Indisponible	33.59	30.29	30.08
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	34.19	30.91	30.71
Surveillance des tresses	Inefficace	29.61	39.11	27.48
Disponibilité opérationnelle des tresses	Indisponible	1.54	2.02	1.44
Impact sûreté	Présent	0.14	0.14	0.13

Tab. H.12 - État de certaines variables du système (en %) en présence d'un des FOP

1.2.5. Cas n°7

Variable du modèle	Modalité	AR, PP et COS présents
Étalonnage du capteur	Inefficace	97.62
Disponibilité opérationnelle de la détection d'oxygène à 5%	Indisponible	50.37
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	50.82
Surveillance des tresses	Inefficace	76.51
Disponibilité opérationnelle des tresses	Indisponible	3.91
Impact sûreté	Présent	0.29

Tab. H.13 - État de certaines variables du système (en %) en présence des trois FOP

Variable du modèle	Modalité	AR présent	PP présent	COS présent
Étalonnage du capteur	Inefficace	97.44	97.31	97.28
Disponibilité opérationnelle de la détection d'oxygène à 5%	Indisponible	50.29	50.22	50.21
Disponibilité opérationnelle de la détection d'oxygène à 7%	Indisponible	50.73	50.67	50.66
Surveillance des tresses	Inefficace	75.86	76.43	75.76
Disponibilité opérationnelle des tresses	Indisponible	3.88	3.91	3.87
Impact sûreté	Présent	0.29	0.29	0.29

TAB. H.14 - État de certaines variables du système (en %) en présence d'un des FOP

2. Cas de diagnostic : Inefficacité de l'action d'étalonnage du capteur de détection d'oxygène

2.1. Modification des valeurs quantifiées de l'échelle de dégradation

Item	Cas n°1	Cas n°2
Gcdg	18.32	20.50
Fe	14.83	13.39
Ai	17.66	11.43
Ex	7.08	7.64
Rex	18.15	11.57
Rcc	10.42	8.10
Fo	9.16	5.65
Cao	8.06	4.88
De	4.04	3.15

TAB. H.15 - État (dégradé) des items de l'action d'étalonnage du capteur en présence d'une inefficacité de l'action pour les cas 1 et 2 (en %)

FOP	Cas n°1	Cas n°2
AR	6.53	5.45
REX	6.59	5.26
PP	6.10	4.77
COS	5.85	4.55
GQS	4.65	3.57
OC	3.25	2.17
MT	1	1

TAB. H.16 - État (pathogène) des FOP en présence d'une inefficacité de l'action pour les cas 1 et 2 (en %)

2.2. Modification des distributions initiales des aspects humains et organisationnels

Item	Cas n°3	Cas n°4	Cas n°5	Cas n°6	Cas n°7
Gcdg	18.08	12.13	19.78	24.71	56.22
Fe	12.10	12.19	15.11	23.29	63.89
Ai	7.29	7.40	10.98	20.76	64.63
Ex	7.61	7.68	9.75	15.71	57.54
Rex	5.85	6.02	11.47	25.57	76.06
Rcc	5.24	5.34	8.41	16.83	50.44
Fo	2.46	2.55	5.50	13.62	53.70
Cao	1.84	1.95	5.38	14.68	57.37
De	1.93	2.01	4.63	11.93	50.04

TAB. H.17 - État (dégradé) des items de l'action d'étalonnage du capteur en présence d'une inefficacité de l'action pour les cas 3 à 7 (en %)

FOP	Cas n°3	Cas n°4	Cas n°5	Cas n°6	Cas n°7
AR	4.53	4.60	6.91	13.47	50.13
REX	2.43	2.50	5.04	12.17	50.06
PP	2.05	2.13	4.75	12.04	50.05
COS	2.01	2.09	4.69	11.95	50.05
GQS	1.31	1.39	4.10	11.60	50.04
OC	0.97	1.05	3.80	11.37	50.01
MT	0.01	0.10	3	10.90	50

TAB. H.18 - État (pathogène) des FOP en présence d'une inefficacité de l'action pour les cas 3 à 7(en %)

I : Organigramme pour la qualification des influences FOP-items

La démarche proposée consiste, à partir des influences identifiées dans la configuration générique (cf. chapitre 2 de ce mémoire), à construire (avec les experts organisationnels) des logigrammes permettant de qualifier de manière générique l'importance de ces influences. Un premier travail a été réalisé pour l'item Délégation (cf. figure I.1), et doit être finalisé et étendu à l'ensemble des items.

Rappel
Facteurs organisationnels ayant, de manière générique, un impact sur l'item Délégation :
*- Pressions de Production (**PP**)*
*- Mauvais Traitement de la complexité organisationnelle (**MT**)*

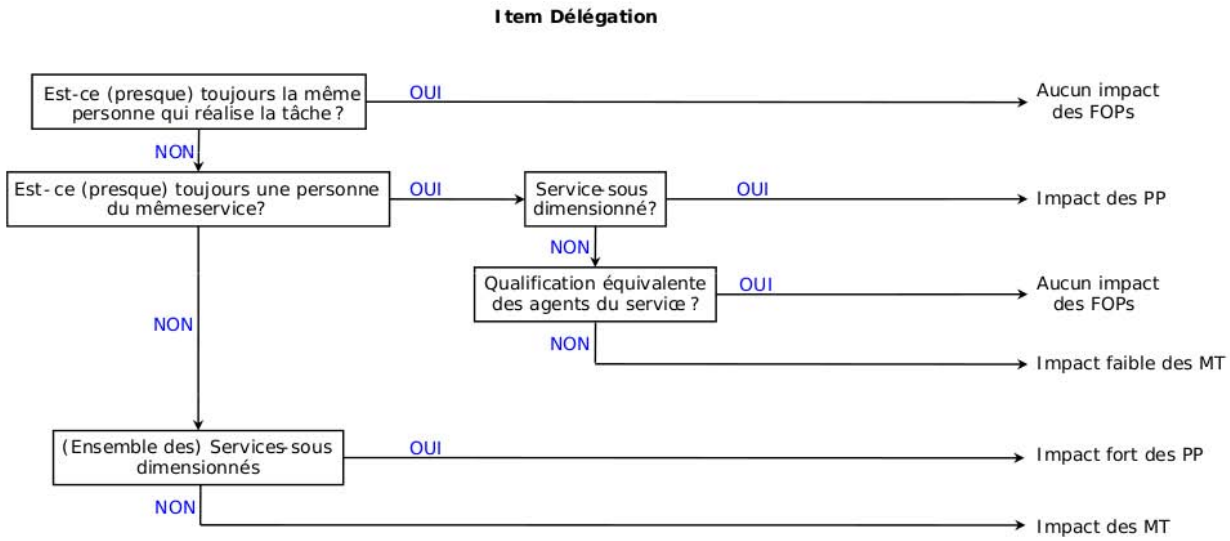

Fig. I.1 - Organigramme pour la quantification des influences entre l'item Délégation et les FOP

Bibliographie

[AFNOR, 1997] AFNOR (1997). *NF EN 1127-1. Atmosphères explosives. Prévention de l'explosion et protection contre l'explosion. Partie 1. Notions fondamentales et méthodologie.* Première édition.

[AFNOR, 2001] AFNOR (2001). *NF EN 13306. Terminologie de la maintenance.*

[AFNOR, 2002] AFNOR (2002). *FD X 60-000. Maintenance industrielle. Fonction maintenance.*

[Amalberti, 1998] Amalberti, R. (1998). Les facteurs humains à l'aube de l'an 2000. *Phoebus*, pages 5–12.

[Andersen *et al.*, 2004] Andersen, H., Casal, J., Dandrieux, A., Debray, B., Dianous, V. D., Duijm, N. J., Delvosalle, C., Fievez, C., Goossens, L., Gowland, R. T., Hale, A. J., Hourtolou, D., Mazzarotta, B., Pipart, A., Planas, E., Prats, F., Salvi, O. et Tixier, J. (2004). Aramis user guide. http ://aramis.jrc.it.

[Auger, 1992] Auger, P. (1992). *Hiérarchie et niveaux de complexité. Systémique - Théorie et Applications.* Editions Lavoisier.

[Ayrault et Bouchet, 2005] Ayrault, N. et Bouchet, S. (2005). Evaluation des dispositifs de prévention et de protection utilisés pour réduire les risques d'accidents majeurs. (DRA - 039). Oméga 10. Evaluation des barrières techniques de sécurité. INERIS.

[Barriere *et al.*, 2000] Barriere, M., Bley, D., Cooper, S., Forester, J., Kolaczkowski, A., Luckas, W., Parry, G., Ramey-Smith, A., Thompson, C., Whitehead, D. et Wreathall, J. (2000). Technical basis and implementation guideline for a technique for human event analysis. ATHEANA. NUREG-1624. Rev.1. US Nuclear Regulatory Commission.

[Barthelemy *et al.*, 2001] Barthelemy, F., Hornus, H., Roussot, J., Hufschmitt, J. P. et Raffoux, J. F. (2001). Rapport de l'inspection générale de l'environnement. Affaire IGE/01/034. Usine de la société Grande Paroisse à Toulouse : Accident du 21 septembre 2001.

[Barthélemy, 2000] Barthélemy, B. (2000). *Gestion des risques - Méthode d'optimisation globale.* Editions d'Organisation.

[Bieder *et al.*, 1998] Bieder, C., Le Bot, P., Desmares, E., Bonnet, J. L. et Cara, F. (1998). MERMOS : EDF's new advanced HRA method. *Proceedings of Fourth Probabilistic Safety Assessment and Management (PSAM4).*

[Bobbio *et al.*, 2001] Bobbio, A., Portinale, L., Minichino, M. et Ciancamerla, E. (2001). Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliability Engineering and System Safety*, 71:249–260.

[Boudali et Dugan, 2005] Boudali, H. et Dugan, J. B. (2005). A discrete-time bayesian network reliability modeling and analysis framework. *Reliability Engineering and System Safety*, 87:337–349.

[CAIB, 2003] CAIB (2003). Columbia Accident Investigation Board. Volume 1.

[Calvez, 1990] Calvez, J. P. (1990). *Spécification et conception des systèmes. Une méthodologie MCSE.* Editions Masson.

[Chevreau *et al.*, 2006] Chevreau, F. R., Wybo, J. L. et Cauchois, D. (2006). Organizing learning processes on risks by using the bow-tie representation. *Journal of Hazardous Materials*, 130:276–283.

[Clegg *et al.*, 1996] Clegg, S., Hardy, C. et Nord, W. (1996). *Handbook of Organization Studies.* Sage Publications.

[Cooper *et al.*, 1996] Cooper, S. E., Ramey-Smith, A., Wreathall, J., Parry, G. W., Bley, D. C., Taylor, J. H. et Luckas, W. J. (1996). A technique for Human Error Analysis. ATHEANA. Technical basis and methodology description. NUREG/CR-6350. US Nuclear Regulatory Commission.

[Courtot, 2002] Courtot, H. (2002). *La gestion des risques dans les projets. Dans E. Niel, E. Craye. Maîtrise des risques et sûreté de fonctionnement des systèmes de production.* Collection IC2 : Informatique - Commande - Communication. Editions Hermès Science.

[De Souza et Ochoa, 1992] De Souza, E. et Ochoa, P. M. (1992). State space exploration in Markov models. *Proceedings of the 1992 ACM SIGMETRICS Joint International Conference on Measurement and Modeling of Computer Systems*, pages 152–166.

[De Terssac et Dubois, 1992] De Terssac, G. et Dubois, P. (1992). *Les nouvelles rationalisations de la production.* Editions Cépadues.

[Dejours, 1995] Dejours, C. (1995). *Le facteur humain. Que sais-je ?* Presses Universitaires de France.

[Deleuze, 2002] Deleuze, G. (2002). Grille d'analyse des risques GLORIA. Note interne. EDF.

[Delmotte, 2003] Delmotte, F. (2003). A socio-technical framework for the integration of human and organizational factors in project management and risk analysis. Mémoire de D.E.A., Faculté de Virginie, Etats-Unis.

[Department of Energy, 1987] Department of Energy (1987). Health and Environmental Consequences of the Chernobyl Nuclear Power Plant Accident. US Department of Energy.

[Department of Transport, 1975] Department of Transport (1975). Health and Safety Executives. The Flixborough Disaster. The court of enquiry.

[Despujols, 2004a] Despujols, A. (2004a). *Approche fonctionnelle de la maintenance. MT 9 020.* Techniques de l'ingénieur.

[Despujols, 2004b] Despujols, A. (2004b). *Optimisation de la maintenance par la fiabilité (OMF). MT 9 310.* Techniques de l'ingénieur.

[Desroches *et al.*, 2006] Desroches, A., Leroy, A., Quaranta, J. F. et Vallée, F. (2006). *Dictionnaire d'analyse et de gestion des risques.* Editions Hermès-Lavoisier.

[Desroches *et al.*, 2007] Desroches, A., Leroy, A. et Vallée, F. (2007). *La gestion des risques. Principes et pratiques. Deuxième édition.* Editions Hermès-Lavoisier.

[Diebolt, 1998] Diebolt, S. (1998). Le petit lexique de la complexité. www.mcxapc.org.

[Dien *et al.*, 2006] Dien, Y., Bourrier, M. et Pierlot, S. (2006). Définition des facteurs organisationnels pathogènes de la sécurité. Note interne. EDF.

[Dien et Llory, 2008] Dien, Y. et Llory, M. (2008). Modèles d'accidents et modèles d'organisations dysfonctionnelles ou pathologiques : caractéristiques et limites de ces modèles. Note interne. EDF.

[Donnadieu *et al.*, 2003] Donnadieu, G., Durand, D., Neel, D., Nunez, E. et Saint Paul, L. (2003). L'approche systémique : De quoi s'agit-il ? Synthèse des travaux du groupe AFSCET. Diffusion de la pensée systémique.

[Dufour, 2008] Dufour, L. (2008). *Le risque dans sa diversité. Une approche pluridisciplinaire.* Editions Hermès-Lavoisier.

[Durand, 1994] Durand, D. (1994). *La systémique. Que-sais-je ?* Sixième édition. Presses Universitaires de France.

[Dutuit *et al.*, 1997] Dutuit, Y., Chatelet, E., Signoret, J. P. et Thomas, P. (1997). Dependability modelling and evaluation by using stochastic Petri Nets : application to two test cases. *Reliability Engineering and System Safety*, 55:117–124.

[Duval *et al.*, 2005a] Duval, C., Bailleul-Bertin, H., Merad, M., Le Coze, J. C. et Farret, R. (2005a). Utilisation des diagrammes d'influence (réseaux bayésiens) dans la méthodologie d'analyse de risques. Opération A1. BCRD. MEDD.

[Duval *et al.*, 2006] Duval, C., Bailleul-Bertin, H., Merad, M., Le Coze, J. C. et Farret, R. (2006). Utilisation des diagrammes d'influences (réseaux bayésiens) dans la méthodologie d'analyse de risques. Opération A2. BCRD. MEDD.

[Duval *et al.*, 2005b] Duval, C., Bertin, H., Léger, A. et Farret, R. (2005b). Choix d'une méthode d'analyse de risques d'un système socio-technique complexe. *Lambda-Mu 15. Lille, France.*

[Duval *et al.*, 2008] Duval, C., Léger, A., Farret, R. et Weber, P. (2008). Méthodologie d'analyse de risques pour les systèmes socio-techniques complexes et application à un cas industriel. *Lambda-mu 16. Avignon, France.*

[Duval *et al.*, 2007] Duval, C., Léger, A., Weber, P., Levrat, E., Iung, B. et Farret, R. (2007). Choice of a risk analysis method for complex socio-technical systems. *European Safety and Reliability conference. Stavanger, Norvège.*

[Embrey, 2002] Embrey, D. (2002). Using influence diagrams to analyse and predict failures in safety critical systems. *Twenty-third ESReDA Seminar. Decision Analysis : Methodology and Applications for Safety of Transportation and Process Industries. Delft, Pays-Bas.*

[Embrey *et al.*, 1984] Embrey, D. E., Humphreys, P., Rosa, E. A., Kirwan, B. et Rea, K. (1984). SLIM-MAUD : an approach to assessing human error probabilities using structured expert judgment. NUREG/CR-3518. US Nuclear Regulatory Commission.

[European Council, 1997] European Council (1997). Council directive 96/82/EC on the major accident hazards of certain industrial activities. SEVESO II. Official Journal of the European Communities. Luxembourg.

[Farret *et al.*, 2007] Farret, R., Duval, C. et Léger, A. (2007). Protocole d'analyse des risques techniques, humains et organisationnels adapté au projet DIRIS et à son schéma conceptuel. INERIS.

[Fayol, 1999] Fayol, H. (1999). *Administration industrielle et générale.* Deuxième édition. Collection Stratégie et Management. Editions Dunod.

[Forest *et al.*, 2007] Forest, C., Miché, E., De Dianous, V. et Chaumette, C. (2007). Probabilistic assessment of potential major accidents : Estimating reliability of safety barriers. *European Safety and Reliability conference. Stavanger, Norvège.*

[Galàn *et al.*, 2007] Galàn, S. F., Mosleh, A. et Izquierdo, J. M. (2007). Incorporating organizational factors into probabilistic safety assessment of nuclear power plants through canonical probabilistic models. *Reliability Engineering and System Safety*, 92:1131–1138.

[Gouriveau, 2003] Gouriveau, R. (2003). *Analyse des risques. Formalisation des connaissances et structuration des données pour l'intégration des outils d'étude et de décision.* Thèse de doctorat, Institut National Polytechnique de Toulouse.

[Gregoriades et Sutcliffe, 2008] Gregoriades, A. et Sutcliffe, A. (2008). Workload prediction for improved design and reliability of complex systems. *Reliability Engineering and System Safety*, 93:530–549.

[Hall *et al.*, 1982] Hall, R. E., Fragola, J. R. et Wreathall, J. W. (1982). Post event human decision errors : operator action tree/time reliability correlation. NUREG/CR-3010. US Nuclear Regulatory Commission.

[Hannaman et Spurgin, 1984] Hannaman, G. W. et Spurgin, A. J. (1984). Systematic Human Action Reliability Procedure (SHARP). NUS Corporation. EPRI NP 3583.

[Hannaman *et al.*, 1984] Hannaman, G. W., Spurgin, A. J. et Lukic, Y. D. (1984). Human cognitive reliability model for PRA analysis. EPRI Project RP-2170-3.

[Hollnagel, 1993] Hollnagel, E. (1993). *Human Reliability Analysis : Context and Control.* Academic Press.

[Hollnagel, 1998] Hollnagel, E. (1998). *Cognitive Reliability and Error Analysis Method (CREAM).* Elsevier Editions.

[Hollnagel, 2004] Hollnagel, E. (2004). *Barriers and accident prevention.* Ashgate Editions, Aldershot (UK).

[Hollnagel *et al.*, 2006] Hollnagel, E., Woods, D. D. et Leveson, N. (2006). *Resilience Engineering : Concepts and Precepts.* Ashgate Editions, Aldershot (UK).

[IEC, 2004] IEC (2004). *Functional Safety. Safety instrumented systems for the process industry sector. All parts.* International Electrotechnical Commission.

[INERIS-MEDD, 2008] INERIS-MEDD (2008). Guide de l'état de l'art sur les silos pour l'application de l'arrêté ministériel relatif aux risques présentés par les silos et les installations de stockage de céréales, de grains, de produits alimentaires ou de tout autre produit organique dégageant des poussières inflammables. Version 3.

[ISO, 1999] ISO (1999). *ISO 14121. Sécurité des machines. Appréciation du risque.* Première édition. Organisation Internationale de Normalisation.

[ISO, 2000] ISO (2000). *ISO 9001. Systèmes de management de la qualité. Exigences.* Première édition. Organisation Internationale de Normalisation.

[ISO, 2003] ISO (2003). *ISO 12100-1. Sécurité des machines. Notions fondamentales, principes généraux de conception. Partie 1 : Terminologie de base, méthodologie.* Organisation Internationale de Normalisation.

[ISO, 2004] ISO (2004). *ISO 14001. Systèmes de management environnemental. Exigences et lignes directrices pour son utilisation.* Première édition. Organisation Internationale de Normalisation.

[ISO, 2007] ISO (2007). *ISO 14121-1. Sécurité des machines. Appréciation du risque. Partie 1 : Principes.* Organisation Internationale de Normalisation.

[ISO-CEI, 2002] ISO-CEI (2002). *ISO/CEI Guide 73. Management du risque. Vocabulaire. Principes directeurs pour l'utilisation dans les normes.* Première édition. ISO-CEI.

[Iung, 1992] Iung, B. (1992). *Contribution à une intelligence distribuée dans les équipements de niveau zéro des processus industriels complexes.* Thèse de doctorat, Université Henri Poincaré, Nancy, France.

[Jensen, 2001] Jensen, J. C. (2001). *Bayesian Networks and Decision Graphs.* Springer Editions.

[Karim, 2008] Karim, R. (2008). *A service-Oriented Approach to e-Maintenance of Complex technical industrial systems.* Thèse de doctorat, Université Technologique de Lulea, Suède.

[Kemeny, 1979] Kemeny, J. G. (1979). Report of the President's Commission on The Accident at Three Mile Island.

[Kervern et Rubise, 1991] Kervern, G. Y. et Rubise, P. (1991). *L'archipel du danger : Introduction aux cindyniques.* Editions Economica.

[Kim et Seong, 2006] Kim, M. C. et Seong, P. H. (2006). A computational method for probabilistic safety assessment of I and C systems and human operators in nuclear power plants. *Reliability Engineering and System Safety*, 91:580–593.

[Langseth et Portinale, 2007] Langseth, H. et Portinale, L. (2007). Bayesian networks in reliability. *Reliability Engineering and System Safety*, 92:92–108.

[Lannoy, 2008] Lannoy, A. (2008). *Maîtrise des risques et sûreté de fonctionnement.* Volume 1. Editions Tec et Doc, Lavoisier.

[Lannoy et Procaccia, 2001] Lannoy, A. et Procaccia, P. (2001). *L'utilisation du jugement d'expert en sûreté de fonctionnement.* Editions Tec et Doc, Lavoisier.

[Le Gallou, 1993] Le Gallou, F. (1993). *Représentation graphique et modélisation globale.* Actes du deuxième Congrès Européen de Systémique.

[Le Moigne, 1990] Le Moigne, J. L. (1990). *La modélisation des systèmes complexes.* Afcet Systèmes, Editions DUNOD.

[Lee *et al.*, 2008] Lee, S. I., Kim, M. C. et Seong, P. H. (2008). An analytical approach to quantitative effect estimation of operation advisory system based on human cognitive process using the bayesian belief network. *Reliability Engineering and System Safety*, 93:567–577.

[Leroy et Signoret, 1992] Leroy, A. et Signoret, J. P. (1992). *Le risque technologique. Que sais-je ?* Presses Universitaires de France.

[Lesbats *et al.*, 1997] Lesbats, M., Dos Santos, J., Perilhone, P. et MADS (1997). Présentation de la science du danger. Editions Elsevier.

[Lewin, 1951] Lewin, K. (1951). *Field theory in Social Science.* D. Cartwright, Harper and Row Editions.

[Léger, 2005] Léger, A. (2005). Estimation des risques associés à l'utilisation d'une machine industrielle : étude bibliographique et conditions d'utilisation des méthodes floues. Mémoire de D.E.A., Université Henri Poincaré, Nancy, France.

[Léger *et al.*, 2008a] Léger, A., Duval, C., Farret, R., Weber, P., Levrat, E. et Iung, B. (2008a). Modeling of human and organizational impacts for system risk analyses. *Ninth Probabilistic Safety Assessment and Management Conference. Hong Kong, Chine.*

[Léger *et al.*, 2006] Léger, A., Duval, C., Weber, P., Levrat, E. et Farret, R. (2006). Risk analysis of complex socio-technical systems by using Bayesian Network modelling. *Workshop on Advanced Control and Diagnosis. Nancy, France.*

[Léger *et al.*, 2008b] Léger, A., Farret, R., Duval, C., Levrat, E., Weber, P. et Iung, B. (2008b). A safety barriers-based approach for the risk analysis of socio-technical systems. *Seventeenth IFAC World Congress. Séoul, Corée du Sud.*

[Léger *et al.*, 2008c] Léger, A., Levrat, E., Weber, P., Iung, B., Duval, C. et Farret, R. (2008c). Methodology for a probabilistic risk analysis of socio-technical systems. *INSIGHT - INCOSE - The best of France - Forum académique et Robafis*, 11:25–26.

[Léger *et al.*, 2009] Léger, A., Levrat, E., Weber, P., Iung, B., Duval, C. et Farret, R. (2009). Methodological developments for probabilistic risk analyses of socio-technical systems. *Journal of Risk and Reliability.* Article à paraître.

[Lord Cullen, 1987] Lord Cullen (1987). The public Inquiry into the Piper Alpha Disaster.

[Lord Cullen, 2001] Lord Cullen (2001). The Ladbroke Grove Rail Inquiry, Part I and II reports. HSE Books.

[Lugan, 2006] Lugan, J. C. (2006). Lexique de systémique et de prospective. Conseil Economique et Social Midi-Pyrénées. Section Prospective.

[Magne et Vasseur, 2006] Magne, L. et Vasseur, D. (2006). *Risques industriels. Complexité, incertitude et décision : une approche interdisciplinaire.* Editions Lavoisier.

[Marais *et al.*, 2004] Marais, K., Dulac, N. et Leveson, N. (2004). Beyond normal accidents and high reliability organizations : the need for an alternative approach to safety in complex systems. *Massachusetts Institute of Technology.*

[Méchin, 2000] Méchin, B. (2000). *La préparation. Guide du responsable de maintenance.* Editions Weka.

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

[Medina Oliva *et al.*, 2009] Medina Oliva, G., Weber, P., Simon, C. et Iung, B. (2009). Bayesian networks Applications on Dependability, Risk Analysis and Maintenance. *Second IFAC Workshop on Dependable Control of Discrete System. Bari, Italie.*

[Miché *et al.*, 2006] Miché, E., Prats, F. et Chaumette, S. (2006). Formalisation du savoir et des outils dans le domaine des risques majeurs. (DRA - 035). Oméga 20. Démarche d'évaluation des barrières humaines de sécurité. INERIS.

[Millot, 1997] Millot, P. (1997). *La supervision et la coopération homme-machine dans les grands systèmes industriels ou de transport.* Sécurité et Cognition, J.P. Ganascia. Editions Hermès.

[Millot et Vanderhaegen, 2008] Millot, P. et Vanderhaegen, F. (2008). Toward Cooperative and Human Error-Tolerant Systems. *Seventeenth IFAC World Congress. Séoul, Corée du Sud.*

[Mintzberg, 1995] Mintzberg, H. (1995). *Structure et dynamique des organisations.* Les éditions d'organisation.

[Mohaghegh *et al.*, 2008] Mohaghegh, Z., Kazemi, R. et Mosleh, A. (2008). Incorporating Organizational Factors into Probabilistic Risk Assessment (PRA) of Complex Socio-technical Systems : A hybrid Technique Formalization. *Reliability Engineering and System Safety*, 94:1000–1018.

[Narbonne, 2005] Narbonne, Y. (2005). *Complexité et systémique.* Editions Hermès-Lavoisier.

[OCDE, 1999] OCDE (1999). Identification and assessment of organizational factors related to the safety of NPP's. State of the art report.

[OHSAS, 1999] OHSAS (1999). Ohsas 18001. Occupational health and safety management systems. Specifications. First edition.

[Onisko *et al.*, 2001] Onisko, A., Druzdzel, M. J. et Wasyluk, H. (2001). Learning bayesian network parameters for small data sets : application of Noisy-OR gates. *International Journal of Approximate Reasoning*, 27:165–182.

[Papazoglou *et al.*, 2003] Papazoglou, I. A., Bellamy, L. J., Hale, A. R., Aneziris, O. N., Ale, B. J. M., Post, J. G. et Oh, J. I. H. (2003). I-Risk : Development of an integrated technical and management risk methodology for chemical installations. *Journal of Loss Prevention in the Process Industries*, 16:575–591.

[Parlement européen et Conseil, 2000] Parlement européen et Conseil (2000). Directive 1999/92/CE du Parlement et du Conseil, du 16 décembre 1999, concernant les prescriptions minimales visant à améliorer la protection en matière de sécurité et de santé des travailleurs susceptibles d'être exposés au risque d'atmosphères explosives. *Journal Officiel*, L023:0057–0064.

[Paté-Cornell et Murphy, 1996] Paté-Cornell, M. E. et Murphy, D. M. (1996). Human and Management factors in probabilistic risk analysis : the SAM approach and observations from recent applications. *Reliability Engineering and System Safety*, 52:115–126.

[Perrow, 1990] Perrow, C. (1990). *Normal Accidents : Living with High-Risk Technologies.* Princeton University Press.

[Pidgeon et O'Leary, 2000] Pidgeon, N. et O'Leary, M. (2000). Man-made disasters : why technology and organizations (sometimes) fail. *Safety Science*, 34:15–30.

[Pierlot, 2007] Pierlot, S. (2007). Veille technologique et scientifique. Accidents, incidents et crises. Les enseignements des accidents. L'importance de l'étude des accidents. Note interne. EDF.

[Pierlot *et al.*, 2007] Pierlot, S., Dien, Y. et Llory, M. (2007). From organizational factors to an organizational diagnosis of the safety. *European Safety and Reliability conference.* Stavanger, Norvège.

[Plot, 2004] Plot, E. (2004). Guide de la prise en compte du facteur humain dans l'évaluation des systèmes de gestion des risques majeurs. Présentation du référentiel MIRIAM et des protocoles ATHOS. INERIS.

[Portinale et Bobbio, 1999] Portinale, L. et Bobbio, A. (1999). Bayesian networks for Dependability analysis : an application to digital control reliability. *Proceedings of the fifteenth conference on Uncertainty in Artificial Intelligence*. Stockholm, Suède.

[Pradier, 2004] Pradier, P. C. (2004). Histoire du risque. Santos del Cerro J., Garcia Secades M., éd.. Historia de la Probabilidad y la Estadistica. Madrid. Delta Publicaciones.

[Project Management Institute, 1992] Project Management Institute (1992). *Risk Management. A guide to managing Project Risks ans Opportunities*. R. Max Wideman.

[Project Management Institute, 1996] Project Management Institute (1996). *A guide to Project Management Body of Knowledge*. PMI standards Commitee.

[Rakoto, 2004] Rakoto, H. (2004). *Intégration du Retour d'Expérience dans les processus industriels. Application à Alstom Transport*. Thèse de doctorat, Institut National Polytechnique de Toulouse.

[Rasmussen, 1975] Rasmussen, N. C. (1975). Reactor safety study. An assessment of accident risks in US commercial nuclear power plants. Rapport WASH-1400. NUREG 74/014. US Nuclear Regulatory Commission.

[Reason, 1990] Reason, J. (1990). *Human Error*. Cambridge University Press.

[Reason, 1997] Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate Editions, Aldershot (UK).

[Reer *et al.*, 2004] Reer, B., Dang, V. N. et Hirschberg, S. (2004). The CESA method and its application in a plant-specific pilot study on errors of commission. *Reliability Engineering and System Safety*, 83:187–205.

[Research and Technology Organization, 2000] Research and Technology Organization (2000). The Human Factor in System Reliability. Is Human Performance Predictable ? *Human Factors and Medicine Panel Workshop*.

[Reynaud, 1997] Reynaud, J. D. (1997). *Les règles du jeu : l'action collective et la régulation sociale*. Editions Armand Colin.

[Robert, 2008] Robert, P. (2008). *Le Nouveau Petit Robert de la langue française*. Editions Le Robert.

[Roberts, 1994] Roberts, F. S. (1994). Limitations on conclusions using scales of measurement. *Handbooks in Operations Research and Management Science*, 6:621–671.

[Roberts, 1993] Roberts, K. (1993). *New Challenges to understanding organizations*. Mac Millan Publishing Company.

[Roberts, 1990] Roberts, K. H. (1990). Managing High Reliability Organizations. *California Management Review*, 32:101–114.

[Roger's Commission, 1986] Roger's Commission (1986). The Roger's Commision Report. Report of the Presidential Commission on the Space Shuttle Challenger Accident.

[Roger's Commission, 1987] Roger's Commission (1987). Report to the President. Implementation of the Recommandations of the Presidential Commission on the Space Shuttle Challenger Accident.

[Sagan, 1993] Sagan, S. D. (1993). *The Limits of Safety, Organizations, Accidents and Nuclear Weapons*. Princeton University Press.

[Salvi et Bernuchon, 2003] Salvi, O. et Bernuchon, E. (2003). Formalisation du savoir et des outils dans le domaine des risques majeurs (DRA - 035). Oméga 6. Eléments Importants Pour la Sécurité (EIPS). Première édition. INERIS.

[Schneider Electric, 2004] Schneider Electric (2004). Intersections. La sûreté de fonctionnement (SdF).

[Seveso, 1982] Seveso (1982). *Original Seveso directive 82/501/EEC (Seveso1).*

[Seville *et al.*, 2006] Seville, E., Brunsdon, D., Dantas, A., Le Masurier, J., Wilkinson, J. et Vargas, J. (2006). Building Organisational Resilience : A summary of key research findings. Research report. Resilient organizations programme.

[Siebenborn, 2005] Siebenborn, T. (2005). *Une approche de formalisation du processus de changement dans l'entreprise.* Thèse de doctorat, Université de Savoie, France.

[Simon *et al.*, 2008] Simon, C., Weber, P. et Evsukoff, A. (2008). Bayesian networks influence algorithm to implement Dempster-Shafer theory in reliability analysis. *Reliability Engineering and System Safety*, 93:950–963.

[Svedung et Rasmussen, 2002] Svedung, I. et Rasmussen, J. (2002). Graphic representation of accident scenario : mapping system structure and the causation of accidents. *Safety Science*, 40:397–417.

[Swain, 1987] Swain, A. D. (1987). Accident Sequence Evaluation Programme (ASEP). Human Reliability Analysis Procedure. NUREG/CR-4772.

[Swain et Guttman, 1983] Swain, A. D. et Guttman, H. E. (1983). Handbook of human reliability analysis with emphasis on nuclear power plant applications. NUREG/CR-1278. US Nuclear Regulatory Commission.

[Torres-Toledano et Sucar, 1998] Torres-Toledano, J. G. et Sucar, L. E. (1998). Bayesian networks for reliability analysis of complex systems. *IBERAMIA'98.* Lisbonne, Portugal.

[Trucco *et al.*, 2008] Trucco, P., Cagno, E., Ruggeri, F. et Grande, O. (2008). A bayesian belief network modelling of organisational factors in risk analysis : a case study in maritime transportation. *Reliability Engineering and System Safety*, 93:823–834.

[Turner et Pidgeon, 1997] Turner, B. A. et Pidgeon, N. F. (1997). *Man-made Disasters. Second edition.* Butterworth-Heinenmann Editions, Londres.

[Union Carbide Corporation, 1985] Union Carbide Corporation (1985). Bhopal Methyl Isocyanate Incident Investigation team report.

[Vaughan, 1996] Vaughan, D. (1996). *The Challenger Launch Decision. Risky technology, culture, and deviance at NASA.* The Chicago University Press.

[Villemeur, 1988] Villemeur, A. (1988). *Sûreté de fonctionnement des systèmes industriels. Fiabilité, Facteurs Humains, Informatisation.* Editions Eyrolles.

[Villemeur, 1992] Villemeur, A. (1992). *Reliability, Availability, Maintainability and Safety Assessment, Volume 1 : Methods and Techniques.* Wiley and Sons Editions.

[Vogel, 1988] Vogel, C. (1988). *Génie cognitif.* Sciences cognitives, Editions Masson.

[Voisin, 1999] Voisin, A. (1999). *Contribution à l'évaluation subjective et son automatisation : du concept à l'application.* Thèse de doctorat, Université Henri Poincaré, Nancy, France.

[Voisin *et al.*, 2005] Voisin, A., Léger, A., Levrat, E. et Lamy, P. (2005). Estimation des risques associés à l'utilisation d'une machine industrielle : Apport des méthodes floues et exemples d'application. *Lambda-Mu 15. Lille, France.*

[Von Bertalanffy, 1968] Von Bertalanffy, L. (1968). *General System Theory.* G. Braziller Editions.

[Weber, 2002] Weber, P. (2002). Dynamic Bayesian Networks model to estimate process availability. *Eight International conference on Quality, Reliability, Maintenance (CCF 2002).* Sinaïa, Roumanie.

[Weber *et al.*, 2005] Weber, P., Iung, B., Levrat, E. et Voisin, A. (2005). Projet IDAFH. Analyse d'une approche de modélisation par réseaux Bayésiens. Rapport de fin de contrat. EDF-UHP-UNI/2004/044.

[Weber et Jouffe, 2003] Weber, P. et Jouffe, L. (2003). Reliability modelling with dynamic bayesian network. *Fifth IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes.* Washington, D.C., USA.

[Weber et Jouffe, 2006] Weber, P. et Jouffe, L. (2006). Complex system reliability modelling with dynamic object oriented bayesian networks (DOOBN). *Reliability Engineering and System Safety*, 91:149–162.

[Weber *et al.*, 2004] Weber, P., Munteanu, P. et Jouffe, L. (2004). Dynamic bayesian networks modelling the dependability of systems with degradations and exogenous constraints. *Eleventh IFAC Symposium on Information Control Problems in Manufacturing.* Salvador-Bahia, Brésil.

[William, 1986] William, J. C. (1986). HEART. A proposed method for assessing and reducing human error. *Proceedings of the ninth Advances in Reliability Technology Symposium.* Université de Bradford, UK.

[Zaidat, 2005] Zaidat, A. (2005). *Spécification d'un cadre d'ingénierie pour les réseaux d'organisations.* Thèse de doctorat, Ecole des Mines de Saint-Etienne et Université Jean Monnet, France.

[Zio, 2009] Zio, E. (2009). Reliability engineering : Old problems and new challenges. *Reliability Engineering and System Safety*, 94:180–186.

Titre : *Contribution à la formalisation unifiée des connaissances fonctionnelles et organisationnelles d'un système industriel en vue d'une évaluation quantitative des risques et de l'impact des barrières envisagées*

Résumé : Depuis la révolution industrielle, l'Homme développe des systèmes industriels pour satisfaire ses exigences de production. Mais exploiter ces installations n'est pas sans risques pour les utilisateurs. De ce fait, l'analyse des risques s'est largement développée durant ces dernières décennies. En effet, si dans les années 70, les études se focalisaient sur les défaillances technologiques, des accidents ont souligné l'importance des facteurs humains et organisationnels dans leur occurrence. Si bien que dans les années 80, des méthodes consacrées à l'identification de ces facteurs ont émergées. Ces études, impliquant différentes disciplines, étaient jusqu'alors conçues et conduites séparément les unes des autres. Cet état de fait amène à une sectorisation des analyses et ne permet pas d'avoir une vision globale de la situation étudiée. Mais, depuis peu, des méthodologies proposent d'intégrer (partiellement) ces dimensions dans la démarche d'analyse. Le manque d'intégration constitue aujourd'hui une problématique, scientifique et industrielle, pour les exploitants de systèmes critiques. Ainsi, notre contribution porte sur le développement d'une méthodologie permettant l'analyse de risques de systèmes socio-techniques en exploitation. Ce type d'analyse vise à probabiliser le risque à des fins d'aide à la décision. En ce sens, nous proposons une démarche de formalisation, d'intégration, de représentation et de modélisation des différentes connaissances du système. Le modèle présenté permet d'identifier l'ensemble des causes menant à l'occurrence d'un événement critique, en considérant les données techniques du système et les données liées aux opérateurs et à l'organisation.

Mots-clés : risques industriels, statistique bayésienne, industrie-mesures de sécurité, systèmes socio-techniques, complexité

Title : *Contribution to the unified formalization of functional and organizational knowledge of an industrial system for a quantitative risks assessment and an estimation of barrier impacts*

Abstract : Since the industrial revolution, human being develops industrial systems to meet his production needs. But the operation of such facilities involves risks for the users. As a result the risk analysis has expanded during these last decades. Indeed, if in the Seventies, the studies were focused on the technological failures, several major accidents have underlined the importance of human and organisational factors in their occurrence, and have changed this initial way of thinking. So that in the Eighties, different methods allowing an identification of these factors have emerged. These studies, implying different fields of expertise, were so far independently built and applied. This fact leads to sector-based analyses and prevents from having an overall view of the studied situation. But, recently, some methodologies propose to (partially) integrate these different methods to study risks in a global approach. This lack of integration constitutes nowadays a scientific and industrial issue for the owners of critical systems. Thus, our contribution concerns the development of a methodology enabling the risk analyses of socio-technical systems in operation. This kind of analysis aims to probabilistically estimate risks for helping the decision-making. In that way, we propose an approach that enables to formalise, integrate, characterise and represent the different knowledge of the system. Our model allows an identification of the whole of the causes that lead to the occurrence of a critical event, by considering the technical data of the system and the data related to human operators and organisational features.

Keywords : industrial risks, bayesian statistics, industry-safety devices, socio-technical systems, complexity