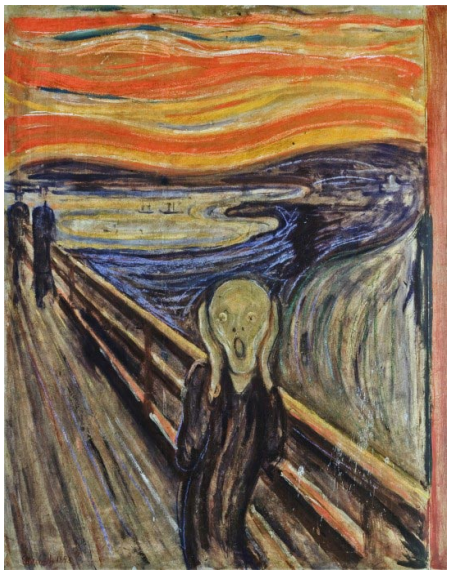
L'Ecosystème décisionnel du manager : une contribution au défi d'anticipation de la crise

Guillaume Delatour

Thèse
de doctorat
de l'UTT

Guillaume DELATOUR

L'écosystème décisionnel du manager : une contribution au défi d'anticipation de la crise



Edvard Munch, *Le cri* ©

Spécialité :
Développement Durable

2015TROY0017

Année 2015

utt
université de technologie
Troyes

THESE

pour l'obtention du grade de

DOCTEUR de l'UNIVERSITE DE TECHNOLOGIE DE TROYES

Spécialité : DEVELOPPEMENT DURABLE

présentée et soutenue par

Guillaume DELATOUR

le 30 juin 2015

L'Ecosystème décisionnel du manager : une contribution au défi d'anticipation de la crise

JURY

M. F. ROUSSEAUX	PROFESSEUR DES UNIVERSITES	Président
M. J.-F. BRILHAC	PROFESSEUR DES UNIVERSITES	Rapporteur
M. D. CALCEI	PROFESSEUR ASSOCIE ESC TROYES	Directeur de thèse
M. P. LACLÉMENCE	PROFESSEUR UTT	Directeur de thèse
M. C. MAZRI	DOCTEUR INGENIEUR D'ETUDE INERIS	Examinateur
M. A. TSOUKIÀS	DIRECTEUR DE RECHERCHE CNRS	Rapporteur
M. J.-L. WYBO	MAITRE DE RECHERCHE MINES PARISTECH - HDR	Examinateur

Remerciements

Ces remerciements représentent les derniers instants de rédaction de cette thèse. Je découvre alors la valeur des soutiens que j'ai reçu toute au long de ces cinq années. C'est donc avec beaucoup de plaisir et d'émotion que je m'applique à écrire ces quelques lignes.

Cette thèse a été menée au sein de l'Université de Technologie de Troyes, à l'Ecole Supérieure de Commerce de Troyes, et en partenariat avec l'Institut National de l'Environnement Industriel et des Risques. Elle est donc le fruit d'une collaboration dont je tiens à remercier les principaux piliers.

Ma profonde gratitude va en premier lieu à mes Directeurs de thèse Patrick Laclémence et Didier Calcei, ainsi qu'à Chabane Mazri. Ils ont fait preuve de grandes qualités humaines et professionnelles. J'ai toujours pu compter sur leur disponibilité et leurs conseils.

Je remercie également les membres du jury, Jean-François Brilhac, Alexis Tsoukiàs, Francis Rousseaux, et Jean-Luc Wybo. Je sais par avance que leurs commentaires et remarques seront profitables et constructifs.

Mes remerciements vont aussi aux membres de l'équipe du CREIDD, pour tous les moments quotidiens passés ensemble. Je vous adresse mes sincères amitiés.

Enfin, je tiens plus particulièrement à exprimer toute ma reconnaissance à ma famille, ainsi qu'à ma chère compagne. Merci pour le soutien inconditionnel que vous m'exprimez à chaque instant. Merci pour les encouragements que vous avez su me prodiguer dans les moments difficiles.

Table des matières

INTRODUCTION GENERALE

1. Introduction au contexte de la recherche. 11
2. Introduction à la question de recherche 14
3. Organisation du document 18

PREMIERE PARTIE : LES DEFIS DU MANAGER OPERATIONNEL

Sous-table des matières #1 23
Introduction de la Première Partie 25
I – De quelle sécurité parle-t-on ? 27
I.1 Essai de définition 27
I.2 La sécurité comme paradoxe 31
II – Retour sur 300 ans d'accidents industriels majeurs 34
II.1 Intuition et objectifs de l'étude 34
II.2 Démarche méthodologique adoptée 36
II.3 Analyse de 10 accidents industriels majeurs passés 53
III – L'évolution de l'environnement décisionnel du manager opérationnel 66
III.1 Le défi de la complexité 67
III.2 Le défi de l'érosion du temps 74
III.3 Le défi de la décision 76
Conclusion de la Première Partie 83
Résumé de la Première Partie 85

DEUXIEME PARTIE : DE L'ACCIDENT INDUSTRIEL A LA RUPTURE MANAGERIALE

Sous-table des matières #2 89

Introduction de la Deuxième Partie 91

I – Principales contributions à l'explication de la dynamique accidentelle 93

I.1 La construction de la sécurité industrielle au XX^{ème} siècle..... 93

I.2 Positionnement scientifique des principaux courants théoriques..... 108

II – Analyse des principaux modèles de production de sécurité 113

II.1 Présentation des principaux modèles théoriques existants..... 113

II.2 Analyse des modèles théoriques retenus..... 170

III – Nécessité d'un nouveau regard sur l'accident industriel 190

Conclusion de la Deuxième Partie 197

Résumé de la Deuxième Partie 199

TROISIEME PARTIE : CONFIGURER L'ECOSYSTEME DECISIONNEL POUR FACILITER LA DECISION MANAGERIALE

Sous-table des matières #3 203

Introduction de la Troisième Partie 205

I. De l'aide à la décision à l'aide à la gestion 207

I.1 La rupture managériale..... 207

I.2 Les limites de l'aide à la décision..... 210

I.3 Le recours à l'outil de Gestion..... 217

II. Développer l'écosystème décisionnel du manager 238

II.1 Le concept d'écosystème..... 238

II.2 Le manager opérationnel au cœur d'un écosystème décisionne..... 243

II.3 Dé complexifier la prise de décision..... 251

Conclusion de la Troisième Partie 261

Résumé de la Troisième Partie 263

CONCLUSION

Conclusion générale.....265

Références.....273

Liste des Figures.....291

Liste des Tableaux.....295

Annexes.....299

Introduction générale

1. Introduction au contexte de la recherche.

Quels sont les défis pour le manager du XXIème siècle ?

Le développement d'une civilisation de l'instant et du mouvement depuis la fin du XXème siècle soumet nos sociétés modernes à de nouveaux modes de fonctionnement plus rapides et déstabilisants. S'il est aujourd'hui possible de traverser la planète en quelques heures, que nos échanges et nos économies se développent dans un unique marché global, ce n'est possible que sous la protection de modèles complexes d'assistance et de surveillance. En quelques années, sous le triple effet de la globalisation, de la mondialisation, et des progrès des sciences et technologies, les rapports avec l'espace, le temps, et la matière, se sont considérablement modifiés (Laclémence, 2013). Tout d'abord, et insufflés par l'espace Schengen, la globalisation des espaces économiques, et l'effacement des frontières permettent la circulation à l'échelle mondiale des marchandises, des biens, et des individus. Ils conduisent à l'émergence d'entreprises internationales, et de productions délocalisées. Egalement, la mondialisation des réseaux, et l'affirmation des télécommunications à grande échelle, a conduit à une internationalisation des flux financiers, et une interdépendance des marchés et des biens à l'échelle mondiale. Enfin, les progrès des sciences et technologies placent l'individu aux limites de la matière. Biotechnologies et nanotechnologies seront les vecteurs de développement du XXIème siècle. Pourtant, les risques associés sont inconnus, et appellent encore au principe de précaution.

Dans ce monde en constante mutation, les systèmes sont de plus en plus complexes. Le comportement de chaque composant isolé, souvent connu, est difficile à prévoir une fois intégré. Les systèmes de protection et de sécurité subissent de profonds changements : privatisation de certaines activités ; importance croissante des relations internationales ; bouleversement de l'organisation et de la coordination des forces militaires et civiles ; impact des nouvelles technologies sur le rapport social ; décèlement des menaces et anticipation du risque. La sécurisation des activités est alors soumise à une multiplicité des acteurs, étatiques et non étatiques, spécialisés et localisés, qui au final, contribuent à la sécurité collective.

En conséquence, le risque associé à tout système est appelé à évoluer, soit du fait de la modification du risque existant, ou en raison de l'apparition de nouveaux. Le développement des biogaz par des opérateurs ne disposant pas a priori des capacités

techniques, organisationnelles, et culturelles adaptées à la gestion des risques majeurs ; l'élargissement de l'usage des antibiotiques au niveau mondial et ses conséquences sur le développement de germes résistants ; ou encore le développement de petits réacteurs nucléaires modulaires susceptibles d'être déployés à grande échelle sont des exemples de modifications de risques existants, ou de l'apparition de nouveaux (Mazri et al, 2014).

En outre, les approches de sécurisation se sont construites sur les fondations de thématiques : sécurité au travail, sécurité industrielle, sécurité informatique, sureté de fonctionnement, sureté nucléaire, sureté des espaces... Avec en mémoire cette étagère du risque, chacun utilise ses outils, et analyse son pré-carré.

Pourtant, la rupture survient encore. L'interdépendance des systèmes et le couplage des réseaux conduit à considérer de multiples origines potentielles, et la possibilité de scénarios non-imaginés par les spécialistes. L'accident de demain sera, et remettra profondément en cause la manière dont nous le comprenons. Il arrivera alors que tous les systèmes fonctionneront normalement, sans qu'aucune défaillance technique ou erreur ne soit constaté, et rendra inefficace les barrières de sécurité existantes (Amalberti, 2013).

Qui de l'ingénieur, du gestionnaire, ou du sociologue, détient la bonne explication des évènements ?

Face à l'approfondissement des spécialisations et des expertises, la sécurité globale apparait comme une voie prometteuse pour un Etat qui cherche des stratégies conciliant périmètre d'action et équilibre économique. Elle vise à « la capacité d'assurer à une collectivité donnée et à ses membres, un niveau suffisant de prévention et de protection contre les risques et les menaces de toutes natures et de tous impacts, d'où qu'ils viennent, dans des conditions qui favorisent le développement sans rupture de la vie et de ses activités collectives et individuelles[1] ». La stratégie en sécurité ne peut alors être que transversale et interdisciplinaire. La réponse globale doit être recherchée en croisant les regards entre professionnels et scientifiques.

Dans ce contexte d'instabilité, les modèles d'analyse de plus en plus poussée doivent s'accompagner d'espaces critiques, et de prise en compte des signaux faibles. Trois défis sont à relever pour le manager de risques, chargé du bon déroulement des opérations :

- *La complexité :* c'est le défi de la compréhension des systèmes, de leurs fonctionnements, et de leurs évolutions. Dans un monde de connexion globale,

[1] Définition proposée par l'Institut National des Hautes Etudes de Sécurité et de Justice INHESJ.

identifier la criticité des activités, connaitre les interdépendances, et préserver les points de rupture constituent les nouveaux piliers de la maitrise des risques.

- *La décision :* c'est le défi des flux grandissants et ininterrompus de signaux et d'informations, couplé à une responsabilité politique et médiatique systématiquement revendiquée, qui efface la décision devant l'attente des conditions de légitimation explicites. Les questionnements relatifs au rassemblement des conditions d'émergence de la phase de décision, de son déclenchement, et de son évaluation, constituent alors les nouveaux leviers d'anticipation de la rupture.
- *Le défi du temps :* c'est le défi posé par l'instantanéité du monde actuel : instantanéité économique avec les intérêts à court terme, instantanéité de la communication avec les réseaux sociaux, instantanéité médiatique avec les informations en continu, et enfin instantanéité professionnelle, avec les missions à court terme, et la recherche de manager toujours plus rapidement opérationnels et redéployables. Il s'agit alors de trouver les nouvelles combinaisons entre le temps présent et l'inscription sans rupture subie dans le long terme (Rosa, 2013).

2. Introduction à la question de recherche

Depuis une cinquantaine d'années, la maitrise des risques repose sur différentes méthodologies (sureté de fonctionnement, modèles intégrant les facteurs humains et organisationnels...). Celles-ci ont pour finalité de réduire les probabilités de l'accident industriel. A ces approches se greffent de multiples considérations nouvelles, sous la forme de responsabilités et de retours d'expérience. La société assurantielle s'est développée au même rythme, prévoyant un accompagnement de la rupture et une forme de continuité d'avant à après par le passage à la responsabilité. Ainsi, la volonté est forte de restreindre l'incertitude et au fil des évènements, on constate que la maîtrise des risques se normalise sous la forme réglementaire, pendant que la gestion des crises s'organise. A travers des directives comme Seveso I, II, et III, par la mise en place de structures de débat participatif, avec le plan de maitrise des risques technologiques, par la mise en œuvre de politiques publiques de plan l'urbanisation, par la démarche de responsabilisation sociale des entreprises, ou encore par l'émergence de considérations éthiques, les autorités en charge améliorent encore la gestion des sites industriels à risques. Néanmoins, face à ce défi, nous espérons réduire l'incertitude et modéliser un environnement sociotechnique nous protégeant de toute surprise. Si la gestion des risques est en évolution constante, pour reprendre une formule très populaire, l'objectif du risque zéro est louable, mais il est peu réaliste, allant même jusqu'à la prise en compte des catastrophes naturelles. Sans remettre en cause les avancées absolument certaines en la matière, il reste certainement quelques doutes sur l'érosion usuelle et temporelle de la gestion des incertitudes par les systèmes sociotechniques mis en place. La remise en cause est permanente et les écosystèmes qui accompagnent le décideur évoluent au même rythme que la société. Des évènements récents, comme le naufrage de la plateforme pétrolière Deepwater Horizon (Deepwater Horizon Study Group, 2011), l'accident de la centrale de Fukushima (Office for Nuclear Regulation, 2011), ou encore l'explosion du Lac Mégantic (Transportation safety Board of Canada, 2014), nous démontrent les limites de la sécurité de ces systèmes. A l'instar du fleuve qui coule, le temps s'écoule et les évolutions sont emprunts d'expériences douloureuses. Chaque accident industriel majeur remet en cause la planification et nous rappelle notre soumission au doute de l'existant. Si aujourd'hui ces « big-ones » (Dechy et al., 2008) sont plus rares, que l'accident industriel aux conséquences extrêmes reste exceptionnel, les conséquences sont souvent beaucoup plus importantes, car soumis à un environnement interconnecté et beaucoup plus complexe. La rupture est alors brutale et

impacte profondément les mémoires. Il n'y a qu'à prononcer des noms et les angoisses rejaillissent du plus profond. Qui n'a jamais entendu parler de Bhopal, ou encore de Tchernobyl ?

Alors, que devons-nous faire ? Sommes-nous soumis à nos peurs ? Doit-on reprendre la totalité des réflexions, actions et réponses ?

Construites au rythme d'expériences douloureuses, les améliorations en matière de gestion des risques sont indéniables. Les processus de sécurité sont de mieux en mieux adaptés et donc acceptés de tous comme des évolutions positives et compréhensibles. Or, si la planification, la normalisation, la gestion, la prévention, la sûreté de fonctionnement, les plans de continuités etc… rendent « vivable » un écosystème industriel complexe, il est aussi primordial de mesurer l'exact défi que nous devons relever pour éviter la surprise et la fracture.

Si les médias évoquent chaque catastrophe au prisme de la surprise, de l'incompréhension et de la peur, une légère prise de recul suffit à nous montrer que cette problématique n'est pas nouvelle. A chaque nouvel accident, la société redécouvre avec douleur les risques associés à la mise en œuvre de technologies. A titre d'exemple, nos règlementations contemporaines sur le risque industriel prennent racine au XVIIIème siècle. Le 31 août 1794, à 7h15 du matin, plusieurs dizaines de tonnes de poudre explosent dans le magasin de poudre du Château de Grenelle situé près de l'Ecole militaire, en zone urbaine (Barpi, 2006). Plus de mille victimes sont à déplorer parmi les employés et la population riveraine. Les bâtiments, maisons et arbres voisins sont détruits. La prise de conscience des risques technologiques entraînée par cette catastrophe passe pour être à l'origine de la réglementation française à partir du décret impérial de 1810 sur les établissements dangereux, insalubres et incommodes. Après la fatalité de l'évènement, et l'exclusion de l'acte malveillant, l'Etat reconnait sa responsabilité. Les activités industrielles dangereuses doivent être encadrées, et maitrisées.

Dans notre monde globalisé et mondialisé, cette problématique émerge à nouveau. Les systèmes industriels font l'objet de nouvelles vulnérabilités jusque-là non définies. Les facteurs de déstabilisation sont nombreux. Citons les leviers exogènes : ruptures technologiques, globalisation des échanges, mondialisation de la compétitivité, fortes contraintes normatives, nouveaux traitements médiatiques, superposition de systèmes : énergie, télécom.... et les leviers endogènes : pression budgétaire, nouvelles méthodes de management, érosion des équipements et infrastructures, intensification des couplages

internes, augmentation des tolérances, recherche de productivité... L'accélération du rythme de production des entreprises, accompagné du rallongement de la durée de vie des systèmes technologiques à risques, et combiné à une augmentation et une densification de la population exposée, modifie durablement le champ de risque généré par les systèmes industriels. Celui-ci n'est plus défini et localisé, mais erratique et diffus. Il n'est plus constant, mais croissant, évolutif et dynamique.

Les outils de gestion classiques (analyse des risques, sureté de fonctionnement, barrières techniques et organisationnelles…) atteignent leurs limites. Celles-ci prennent plusieurs formes. Tout d'abord, une longue période sans accident majeur peut générer une dégradation progressive des moyens de prévention. Et cette érosion du temps construit chez le manager une représentation du système où aucune défaillance majeure ne peut être gérée. De plus, l'accident industriel revêt aujourd'hui un caractère dynamique et systémique. Les origines de l'accident sont parfois très éloignées des évènements composant la séquence accidentelle. Ces contributions sont généralement diffuses, dans la gestion du système et de son environnement. Enfin, la multiplicité des scénarios possibles engage le concepteur à faire des choix, et créant ainsi des points de faiblesses. Exceptionnel et peu probable, l'accident est d'autant plus surprenant et étonnant. Le déroulement est inattendu. Le lien entre la cause et les effets est masqué, voire inexistant. Les conséquences dues à l'interdépendance du système industriel à son environnement sont globales et majeures. Ces difficultés à décrire et expliquer l'occurrence du phénomène accidentel ont été mis en avant lors d'accident technologiques récents, tels que la perte de la navette Columbia (NASA, 2003) l'explosion de la raffinerie de Texas City (Mogford, 2005), et l'accident nucléaire de Fukushima (Office for Nuclear Regulation, 2011).

En conséquence, l'enjeu sécuritaire est le maintien d'une vigilance constante et sa permanence à long terme au sein des systèmes industriels à hauts-risques. Une revue des principales théories relatives à la production de sécurité industrielle nous montre les limites des connaissances actuelles. Celles-ci sont globalement disciplinaires, et majoritairement descriptives. Elles règlent bien la prévention, quelque fois l'action, souvent la réaction, mais rarement se pose la question en terme d'anticipation. Ainsi, la problématique posée est alors celle de l'anticipation lors des accidents majeurs.

Une analyse contextuelle permet d'identifier deux hypothèses structurantes de ce travail. La première porte sur l'accident industriel. Celui-ci est un construit dynamique qui peut être évité. Dans ce cadre, l'orientation porte sur l'anticipation de l'accident.

La seconde hypothèse se focalise sur la question de l'anticipation des accidents industriels sur les modes de gestion de l'entreprise. Dans ce cadre, nous faisons l'hypothèse que le manager opérationnel doit jouer un rôle déterminant dans l'anticipation des accidents.

Pour répondre à cette problématique, une méthodologie spécifique a été choisie. Elle prend le pari de lier passé et futur, à travers le retour d'expérience, et le management opérationnel. C'est par l'étude historique des accidents industriels qu'ont été élaborées les nouvelles voies de maitrise des risques industriels.

3. Organisation du document

La problématique posée est celle de la décision d'anticipation. Quelle aide apporter au manager, pour améliorer sa capacité à anticiper les dynamiques accidentelles, au sein de systèmes sociotechniques complexes ?

Pour répondre à cette question, nous proposons de structurer la démarche de la manière suivante (Figure 1).

Tout d'abord, une première partie porte sur le contexte décisionnel rencontré par le manager opérationnel. L'objectif de cette première phase est d'une part la compréhension de la dynamique accidentelle, et d'autre part l'analyse est d'identifier les contraintes qui s'imposent au manager, dans sa phase de prise de décision. La méthodologie adoptée est celle de l'analyse de cas. Afin de mettre en perspective les faiblesses d'une évolution continue de la production de sécurité, la voie choisie est celle de l'analyse historique des principales catastrophes industrielles, sur la période des 300 dernières années. Par l'étude des marqueurs communs à chacun des évènements, le but est d'identifier les défis auxquels fait face le manager opérationnel.

Sur la base des résultats de cette première analyse, une deuxième partie porte sur les principaux modèles de production de sécurité. L'objectif est de se questionner sur la capacité de ces modèles à prendre en charge les défis qui s'imposent au manager, et déterminé dans la première partie. La méthodologie adoptée est une analyse bibliographique. Plusieurs modèles, parmi les grandes contributions scientifiques, sont sélectionnés et décrits. Chaque modèle théorique est ensuite mis en perspectives avec les défis du manager identifiés dans la première partie.

Enfin, après avoir identifié les intérêts et limites de la littérature existante, une troisième apporte une réponse à la problématique posée. Il s'agit de contribuer à l'aide à la décision pour l'anticipation des accidents industriels majeurs, au sein de systèmes sociotechniques complexes. Pour cela, la méthodologie proposée est la suivante. Tout d'abord, l'efficacité des principaux outils existants est analysée, au regard des résultats des deux premières parties. Enfin, une réponse à la problématique sera proposée. Dans ce nouveau schéma, le management opérationnel est un levier d'anticipation incontournable. Est alors proposé une nouvelle voie d'anticipation, à travers le développement de l'écosystème décisionnel du manager opérationnel.

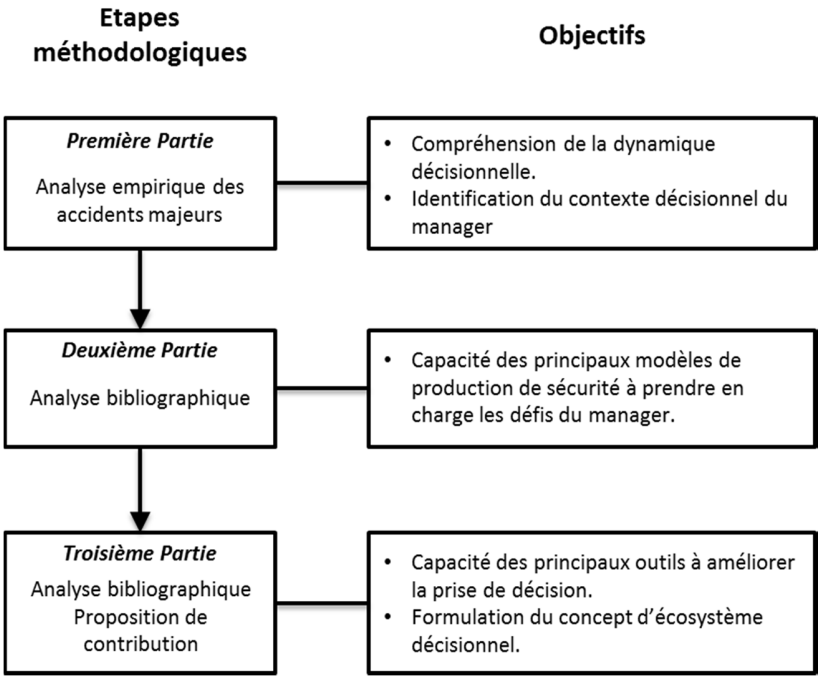


Figure 1 : Structure méthodologique du mémoire

Première Partie

Les défis du manager opérationnel

Sous-table des matières #1

Sous-table des matières #1 23
Introduction de la Première Partie 25
I – De quelle sécurité parle-t-on ? 27
I.1 Essai de définition 27
I.2 La sécurité comme paradoxe 31
II – Retour sur 300 ans d'accidents industriels majeurs 34
II.1 Intuition et objectifs de l'étude 34
II.2 Démarche méthodologique adoptée 36
II.3 Analyse de 10 accidents industriels majeurs passés 53
III – L'évolution de l'environnement décisionnel du manager opérationnel 66
III.1 Le défi de la complexité 67
III.2 Le défi de l'érosion du temps 74
III.3 Le défi de la décision 76
Conclusion de la Première Partie 83
Résumé de la Première Partie 85

Introduction de la Première Partie

Comment relever les défis du manager opérationnel ?

Les changements sociétaux de ces vingt dernières années imposent aux entreprises industrielles d'intégrer les évolutions face aux risques et à modifier leur fonctionnement. Intégrant un cadre normatif de plus en plus contraignant, la société est de plus en plus sensible aux risques, d'autant que la captation médiatique de l'instant impose la gestion des émotions.

Au cœur du système, la tension entre action et réaction se focalise sur le manager opérationnel, chargé du bon déroulement des opérations de production. La maitrise des processus à risques est alors plus que jamais un enjeu majeur. Pourtant, arrive-t-on à un palier ? Chaque nouvel accident challenge les progrès réalisés, et les efforts consentis à maintenir un haut niveau de sécurité.

Dans l'hyper sécurisation des processus techniques, la décision d'arrêter le système est lourde de conséquences. Pourquoi, malgré des signaux identifiés de plus en plus finement après chaque accident, l'arrêt du système n'a-t-il pas été choisi à la continuité d'activité ? Est-ce une trop extrême prudence ? Le dilemme de la décision est-il un conflit insoluble ?

Notre objectif est de mettre en perspective les faiblesses de l'évolution continue de la production de sécurité. La voie choisie est celle de l'analyse historique des principales catastrophes industrielles, sur la période des 300 dernières années. Par l'étude des marqueurs communs à chacun des évènements, le but est d'identifier les défis auxquels fait face le manager opérationnel. Pour cela, dans une première sous-partie nous aborderons le concept de sécurité industrielle tout d'abord, et également les manières dont il se décline et s'applique en France. La deuxième sous-partie est allouée à l'analyse historique des accidents. Après avoir explicité de manière précise la démarche méthodologique adoptée, les marqueurs communs, résultats de l'étude, sont décrits. Enfin, une troisième sous-partie propose une analyse de l'environnement décisionnel du manager opérationnel, et des défis qui lui sont imposés.

I – De quelle sécurité parle-t-on ?

Dans tous les mondes, la sécurité est une pierre angulaire des systèmes urbains, industriels... Elle est également une réalité omniprésente de l'industrie. Transport, aviation, énergie, télécommunication... La sécurité est permanente dans les organisations, et il en est difficile d'identifier son périmètre. Sans aborder un questionnement philosophique majeur sur la notion, par ailleurs qualifiée de concept fondamentalement contradictoire (Hansson, 2012), un essai de définition est développé ici.

I.1 Essai de définition

A priori, ce que l'on vise en matière de sécurité industrielle, est une absence. Les organisations industrielles sont confrontées à de multiples dangers : phénomènes physicochimiques incontrôlés, énergie cinétique, haute tension électrique... Ces dangers entraînent des risques, c'est-à-dire la possibilité de dommages aux personnes, aux biens, et à l'environnement. C'est l'objet de la sécurité industrielle que de prévenir ces risques. Il s'agit d'éviter l'occurrence d'événements dont la gravité pourrait être élevée, même si leur probabilité a priori est faible. Et ainsi, éviter que se produisent des événements aux conséquences potentielles jugées inacceptables. La sécurité est donc « un non-événement dynamique » (Daniellou et al., 2010), dans le sens où elle correspond à une situation qui perdure dans le temps et pendant laquelle l'évènement redouté ne se produit pas.

Selon Nilsen et al. (2004), la sécurité industrielle est davantage qu'une notion passive, « ce qui ne blesse pas ». Gérer la sécurité est un acte proactif. Il s'agit de créer un environnement dans lequel les activités dangereuses prennent place avec succès, sans générer de dommages. La sécurité doit être gérée activement pour permettre le profit. C'est par exemple le cas pour l'aviation civile, ou encore les industries pétrolières, qui sont naturellement dangereuses, mais dont l'exploitation en sécurité permet de dégager une rente certaine. Dans les deux cas, le risque est au cœur de l'activité. Les organisations qui gèrent le mieux ce risque font le plus grand profit. Au contraire, les organisations plus laxistes sont plutôt perçues comme dangereuses, et sont généralement forcées à sécuriser leurs activités, sous peine de mettre en jeu leur pérennité. Un bon exemple est l'existence de

listes noires des compagnies aériennes ne satisfaisant pas les standards internationaux de sécurité aérienne.

Selon le *Center for Chemical Process Safety* (CCPS, 2010), la sécurité du process peut être définie comme un mélange de compétences d'ingénierie et de management portant sur la prévention des accidents catastrophiques, et notamment les explosions, les incendies, et les fuites toxiques associées à l'utilisation de produits chimiques dangereux. La sécurité peut être atteinte en éliminant les dangers, en prévenant les évènements initiateurs de chaines accidentelles, et en se protégeant des conséquences (Hollnagel, 2008).

Selon Hollnagel (Hollnagel, 2008), risque et sécurité sont liés conceptuellement et pragmatiquement. Le lien conceptuel peut être identifié à travers les définitions comparées des deux notions. Le risque, par exemple, est généralement défini comme la probabilité d'occurrence d'un évènement indésirable. De même, la sécurité est définie comme l'absence d'évènement non désirés, ce qui signifie essentiellement l'absence de risques. Le lien pragmatique montre cette réciprocité entre les concepts. Le niveau de sécurité est généralement mesuré par le nombre d'évènements non désirés qui ont eu lieu, comme les pannes, ou les accidents. Un haut niveau de sécurité est équivalent à un bas niveau d'occurrence, un bas niveau de risque. Selon ces définitions, pour s'assurer d'un haut niveau de sécurité, il est nécessaire de se prévenir de l'occurrence d'évènements non désirés (Figure 2). En pratique, cela est impossible. La mise en place de barrières de protection est donc importante pour se prémunir de conséquences catastrophiques. En d'autres termes, les barrières sont utilisées comme éléments réactifs, c'est-à-dire comme une réponse à l'évènement. Cependant, la sécurité ne peut être garantie seulement par une voie réactive. Il est également important de regarder vers le futur, identifier les nouveaux risques potentiels, et adapter les barrières de sécurité.

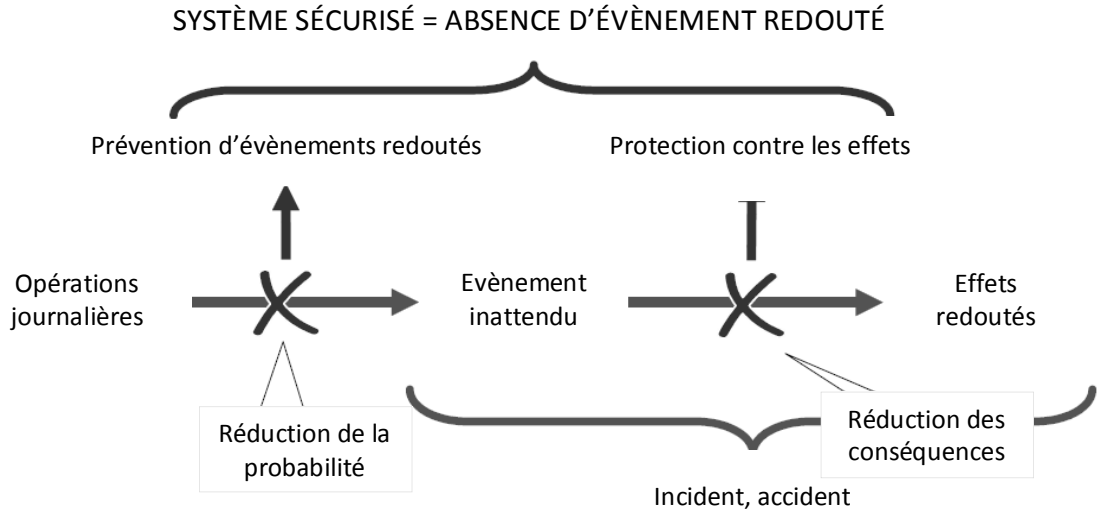


Figure 2 : La sécurité à travers à la prévention et la protection, adapté de Hollnagel (2008)

La sécurité peut être vue de deux manières : comme une finalité du système, ou comme une contrainte sur les conditions de réalisation de la mission. C'est par exemple le cas dans le domaine industriel, où les objectifs de production et de sécurité apparaissent au premier abord comme antagonistes (Leveson et al., 2009). Certaines organisations ont la nécessité, et la capacité de passer d'un système de référence à l'autre, en fonction de leur environnement. La sécurité, initialement prévue comme une finalité, devient une contrainte de fonctionnement parmi d'autres, à l'image du porte-avion. En temps de paix, la sécurité des pilotes est une finalité. En temps de guerre, elle devient une contrainte de réalisation de la mission.

Au prisme des organisations hautement fiables, la sécurité est une propriété équivalente à celle de fiabilité. La théorie décrit une culture de fiabilité, considérant ainsi l'absence de défaillance de l'Homme. La sécurité est alors définie comme l'absence de pertes inacceptables. Pour ce type d'organisation, la suite de la sécurité n'est pas seulement dans la prévention des défaillances isolées, humaines ou techniques. Elle est plutôt dans la construction d'un système aussi robuste que possible face aux dangers opérationnels. Une

organisation hautement fiable n'est pas dénuée d'évènements non-désirées, mais elle a appris à convertir ces revers occasionnels en capacité de résilience (Reason, 1997).

Ainsi, la définition de la sécurité industrielle est encore largement discutée dans la littérature (Aven, 2014). Hollnagel (2014) propose une synthèse des trois principales définitions du concept de sécurité : la sécurité comme épiphénomène, la sécurité comme non-évènement dynamique, et la sécurité comme construit social.

- **La sécurité comme épiphénomène :** La sécurité est définie comme l'absence d'évènements non désirables lors des opérations (panne, incident, accident). C'est une définition indirecte de la sécurité, et une définition de l'insécurité. Cette définition tend à focaliser l'attention sur les évènements indésirables, et les situations de perte de maitrise. En conséquence, la gestion de la sécurité se réfère à des mesures d'absence de sécurité (taux de panne, taux d'accident), plutôt qu'à des mesures de niveau de sécurité. Paradoxalement, la notion de sécurité est recherchée mais impossible à mesurer.

- **La sécurité comme un non-évènement dynamique :** définie initialement par Weick (2001), le « non-évènement » signifie que la sécurité est présente lorsqu'aucun évènement indésirable n'a eu lieu. Le terme « dynamique » signifie que l'état de sécurité ne peut être atteint que par des moyens passifs. La sécurité nécessite l'ajout de barrières de sécurité complémentaire, et une attention continue.

- **La sécurité comme une construction sociale :** Rochlin (1999) substitue la notion de *Safe operation* à celle de *safety*. C'est une action interactive, dynamique et communicative, au sein de systèmes sensibles aux perturbations, dont le but est de réduire le risque d'erreur. Il s'agit de détecter et d'anticiper les éventuelles difficultés qui vont se poser. En d'autres termes, il ne s'agit pas de comprendre les facteurs qui ont conduit à l'accident, mais plutôt les facteurs de succès, qui ont permis de l'éviter.

En outre, la définition aujourd'hui prépondérante de la sécurité est déclinée de celle de la résilience. C'est la capacité du système à anticiper la survenue d'évènements indésirables, à les gérer, les mitiger lors de leur survenue et à revenir à son état normal (Hollnagel et al., 2006). Cela nécessite de la part du système l'élaboration et la mise en œuvre de différents processus ou pratiques de management qui amélioreront sa résilience face aux dangers intrinsèques de son activité. Avec cette approche proactive, la

sécurité peut être comparée au système immunitaire qui, dans le domaine de la santé, protège le corps humain contre toute agression d'agents pathogènes. Pour évaluer la présence de sécurité, il faut donc s'intéresser à l'efficacité des différentes fonctions vitales du système organisationnel dédiées à développer sa résilience interne et à accroitre la sécurité en son sein. Plus ces fonctions vitales seront efficaces, plus les résultats indésirables (accidents, incidents, presque accidents, etc.) deviendront rares. La logique de l'approche proactive est donc d'accentuer ces fonctions vitales, d'amplifier la résistance interne du système pour faire disparaitre et éliminer les résultats indésirables ainsi que les échecs de la sécurité.

En synthèse, la sécurité telle qu'elle est pensée de nos jours est perçue comme une finalité, et également une propriété active du système. Elle est le résultat d'un processus de gestion dédié à la coordination des activités impliquées, de manière directe ou indirecte, dans la surveillance et le contrôle des opérations de production. Au pilotage de ce processus, le manager opérationnel joue donc un rôle critique dans la gestion des risques industriels.

I.2 La sécurité comme paradoxe

Dans son ouvrage « Piloter la sécurité », de 2013, Amalberti décrit un rapport plutôt paradoxal de la société face à ses exigences en matière de sécurité (Amalberti, 2013).

En effet, la société est confrontée à des accidents industriels majeurs (Texas City en 2005, Fukushima en 2011...), et à des crises atteignant les services publics (erreurs médicales par exemple). Plus encore que le nombre de morts, qui a plutôt tendance à diminuer en proportion, c'est la diversité des milieux concernés qui frappe l'imagination, et la gravité croissante des sinistres, avec leurs immenses répercussions économiques. L'auteur décrit le monde actuel comme des systèmes en équilibre précaire, dans lequel la tendance est à produire toujours plus, avec des outils plus complexes, dans des endroits plus difficiles, en générant forcément toujours plus de risques d'accompagnement. Les multiples fonctions d'échanges provoquent des tensions contradictoires entre accès à l'innovation et aux nouveaux risques, marchés concurrentiels, libre entreprise, limitation des contraintes légales, sécurité des biens et des personnes, sécurité à court terme et sécurité à long terme.

Selon Amalberti, « l'accident de demain, rare mais probablement encore plus dramatique, sera un accident ou les règlements existaient pour éviter le problème, ou peut-être même

personne n'aura fait une erreur caractérisée, ou aucun système n'aura été vraiment en panne, mais ou l'érosion aura affaibli toutes les composantes, l'ampleur de variation des conditions de fonctionnement d'un jour aura suffi pour dépasser les seuils de couplage tolérables. Paradoxalement, la sécurité du système aura tout misé sur des procédures rassurantes, qui l'auront fait progresser, puis l'auront mis en confiance, puis se seront affaiblis au fil du temps à la fois par l'érosion des défenses, l'augmentation des tolérances, et par la perte d'expertise à gérer des situations difficiles » (Amalberti, 2013).

Dans ce contexte, qui devra prendre la décision de prudence et arrêter le système avant la catastrophe ? Contraint entre risques et éthique, le management du risque contribue de façon tangible à l'atteinte des objectifs et à l'amélioration des performances d'une organisation. Il répond à plusieurs enjeux de l'organisation, par exemple dans le domaine de la santé et de la sécurité des personnes et des biens, de la conformité aux exigences légales et réglementaires, de l'acceptation par le public, de la protection de l'environnement, de la qualité des produits, du management de projets, de l'efficacité opérationnelle et de la gouvernance de l'organisme, ainsi que de sa réputation (Gayon, 2001). Face à des perturbations de plus en plus importantes, la résistance de l'organisation nécessite un management des risques. Pour exemple, la norme ISO 31000 décrit un processus de management des risques d'une organisation, et affiche les objectifs suivants (ISO 31000 : 2009) :

- ✓ d'accroître la vraisemblance d'atteindre les objectifs,
- ✓ d'encourager un management proactif,
- ✓ de prendre conscience de la nécessité d'identifier et de traiter le risque à travers tout l'organisme,
- ✓ d'améliorer l'identification des opportunités et des menaces,
- ✓ de se conformer aux obligations légales et réglementaires ainsi qu'aux normes internationales,
- ✓ d'améliorer la rédaction des rapports obligatoires et volontaires,
- ✓ d'améliorer la gouvernance,
- ✓ d'accroître l'assurance et la confiance des parties prenantes,
- ✓ d'établir une base fiable pour la prise de décision et la planification,
- ✓ d'améliorer les moyens de maîtrise,
- ✓ d'allouer et d'utiliser efficacement les ressources pour le traitement du risque,
- ✓ d'améliorer l'efficacité et l'efficience opérationnelles,

- ✓ de renforcer les performances en matière de santé et de sécurité, ainsi que de protection environnementale,
- ✓ d'améliorer la prévention des pertes et le management des incidents,
- ✓ de minimiser les pertes,
- ✓ d'améliorer l'apprentissage organisationnel, et
- ✓ d'améliorer la résilience organisationnelle.

II – Retour sur 300 ans d'accidents industriels majeurs

Chaque nouvel accident industriel montre la faillite des processus de gestion de la sécurité. Erreur humaine ? Défaillance technique ? A travers le diagnostic d'accidents parmi les plus marquants, et issus de périodes et de domaines industriels différents, le but est de comprendre pourquoi, malgré d'importantes mesures de sécurité, le drame n'a pu être évité. Dans un deuxième temps, la mise en perspective des cas étudiés, nous permettra d'identifier les marqueurs communs à l'ensemble des évènements. Les tableaux d'analyses de chaque cas ont été placés en annexe (Annexe n°1).

II.1 Intuition et objectifs de l'étude

Les systèmes industriels actuels sont souvent considérés « ultra-sûrs » (Amalberti, 1996). Ainsi, les risques liés au transport aérien ont été divisés par dix depuis la seconde guerre mondiale, et atteint un niveau actuel d'environ un accident mortel par million d'heures de vol (Ministère de l'écologie, du Développement Durable, et de l'Energie, 2013). Pourtant, sans rentrer dans le débat des indicateurs utilisés, les données de « performances de sécurité » ont tendance à stagner. Du point de vue des résultats, les industries à risques dansent « le tango sur une asymptote » (Frantzen, 2004). Pour une année donnée, ceux-ci sont soit légèrement meilleurs, soit légèrement moins bons que ceux de l'année précédente. Une vue plus précise de ces indicateurs montre également la présence des « big-ones » tels que Tchernobyl[2], AZF[3], ou encore diverses catastrophes aériennes. Apparaissent également des répétitions de ces « big-ones », comme l'est la perte de la navette spatiale américaine Columbia[4] par rapport à Challenger[5]. Si aujourd'hui ces évènements sont rares au regard du

[2] L'accident nucléaire de la centrale du Tchernobyl, en Ukraine, eu lieu le 26 avril 1986. La perte de contrôle et la fusion du réacteur a libéré un nuage contenant des éléments radioactifs sur une grande partie de l'Europe. La gravité de l'évènement a conduit au classement de l'explosion de Fukushima au niveau le plus élevé (sept) sur l'échelle INES (Echelle Internationale des Evènements Nucléaires).

[3] L'usine AZF de Toulouse a été détruite le 21 septembre 2001 par l'explosion d'un stock de nitrate d'ammonium, causant 31 morts, plus de 2500 blessés, et d'importants dégâts matériels.

[4] L'accident de la navette spatiale Columbia se déroula le 1er février 2003. Lors de la phase de rentrée dans l'atmosphère de la mission STS-107, une défaillance du bouclier thermique causa la destruction de la navette spatiale au-dessus du Texas et de la Louisiane, tuant les sept membres d'équipage.

[5] La navette spatiale américaine Challenger s'est désintégrée le 28 janvier 1986 lors du décollage, après 73 secondes de vol, causant la mort des sept membres d'équipage.

nombre d'industries en fonctionnement, leurs conséquences sont souvent beaucoup plus importantes. Cela peut s'expliquer par une concentration de processus dangereux, accompagné d'une augmentation de la population, et de la valeur des biens exposés. Cette évolution paradoxale laisse apparaître une asymétrie entre la maîtrise des risques de plus en plus en amont et la dimension de la crise en aval. Ces constats sur les limites actuelles de la progression de la sécurité ne peuvent être satisfaisants. Par conséquent, la problématique des nouvelles voies de progression se pose. En particulier, peut-on encore identifier dans l'analyse des différents accidents passés de nouvelles pistes d'amélioration ?

Le choix de l'étude de cas

Dans le domaine médical, les médecins se servent de la connaissance des pathologies pour reconnaitre les symptômes et sélectionner les mesures adaptées. De manière similaire, la voie proposée pour notre analyse est celle de l'étude d'accidents passés. L'objectif est de comprendre quelles ont été les faiblesses de la prévention des risques. De plus, les accidents majeurs sont mieux analysés et documentés, et permettent de révéler plus clairement des symptômes, qu'à travers l'analyse d'incidents ou de signaux faibles.

En outre, le choix du retour d'expérience comme données d'analyse se justifie au regard de plusieurs éléments. Premièrement, le retour d'expérience fournit une analyse globale des faits. Il permet de comprendre le phénomène accidentel, depuis la chaine causale des évènements, l'intégration des facteurs organisationnels, et jusqu'à la prise en compte des presqu'accidents et signaux faibles. En conséquence, lorsqu'elle est réalisée de manière méthodique, l'analyse d'accidents permet d'identifier des enseignements remarquables (Llory, 1999).

Deuxièmement, le retour d'expérience permet de comprendre les mécanismes accidentels mis en jeu. Il fournit une analyse précise des faits. A titre d'exemple, le retour d'expérience met en exergue deux grandes familles de causes. Tout d'abord, les causes directes, ou immédiates qui font références aux éléments dont la défaillance a initié ou contribué au déroulement de la chaine accidentelle (défaillance technique, comportement humain...), et les causes profondes, qui font références aux facteurs organisationnels sous-jacents, qui participent au processus de dégradation de la sécurité du système.

L'intérêt de cette démarche place aujourd'hui le processus de retour d'expérience au cœur des approches modernes de gestion des risques (Dien et al., 2004). A l'heure actuelle, la littérature propose presque autant de définitions qu'il existe de pratiques de REX (Gauthey, 2005). Une revue de ces définitions, et pratiques de REX, a été réalisée par la fondation pour une culture de sécurité industrielle (Mbaye, 2010).

Cependant, il est nécessaire de préciser que d'autres axes de recherche rejettent les analyses d'accident, et choisissent de se baser sur l'analyse du fonctionnement quotidien des organisations. Cela afin d'identifier des facteurs de fiabilité et de performance des organisations (HSE, 2011). D'autres spécialistes, tel que Perrow (2007), plaident pour une réduction de la complexité des organisations industrielles, et la réduction de la vulnérabilité des sociétés. Egalement, de nombreux travaux émergeants portent le concept d'organisations industrielles résilientes (Rigaud, 2011). Enfin, dans une perspective différente, d'autres pistes proposent la préparation à la gestion de crise en raison de l'occurrence inévitable des accidents (Lagadec, 2012), (Roux Dufort, 2000).

II.2 Démarche méthodologique adoptée

Notre analyse s'appuie sur la méthodologie de l'étude de cas. De manière générale, elle renvoie à une méthode d'investigation à visée d'analyse et de compréhension. Elle consiste à étudier en détail l'ensemble des caractéristiques d'un problème ou d'un phénomène restreint et précis, tel qu'il s'est déroulé dans une situation particulière, réelle ou reconstituée, et jugée représentative de l'objet à étudier (Albero, 2010). Plus précisément, l'étude de cas comme méthode de recherche est appropriée pour la description, l'explication, la prédiction et le contrôle de processus inhérents à divers phénomènes, que ces derniers soient individuels, de groupe ou d'une organisation (Woodside et al., 2003). Dans son ouvrage méthodologique, Gagnon (2005) cite l'intérêt et les limites de ce type de méthodes. Ceux-ci sont explicités dans le tableau 1.

Intérêts de l'étude de cas	*Limites de l'étude de cas*
• Permet l'analyse des systèmes complexes, tel que les systèmes humains et sociaux ; • Situe les cas visés dans leur contexte, et tient compte de leur histoire ; • Aborde les phénomènes dans leur globalité et leur profondeur ; • Apporte une description détaillée des évènements, et une compréhension des comportements et des interrelations entre les acteurs ; • Permet de répondre aux questions : qui, quoi, quand, et comment ? • Permet d'éclairer les paramètres difficilement mesurables par une analyse quantitative ; • Permet une forte validité interne des résultats ; • Permet d'appréhender une grande diversité de type de sources.	• Nécessite l'interprétation du chercheur, et peut donc être soumis à ses biais ; • N'atteint pas la représentativité statistique ; • La généralisation est difficilement réalisable sans recourir à une méthode quantitative complémentaire ; • La validité externe et la reproductibilité sont difficiles à obtenir ; • La méthode est onéreuse en temps.

Tableau 1 : Intérêts et limites de l'étude de cas, adapté de Gagnon (2005)

Le processus méthodologique adopté pour réaliser notre étude de cas est adapté de la démarche de réalisation de Gagnon (2005). Elle se décompose en plusieurs étapes, schématisées ci-dessous (Figure 3) :

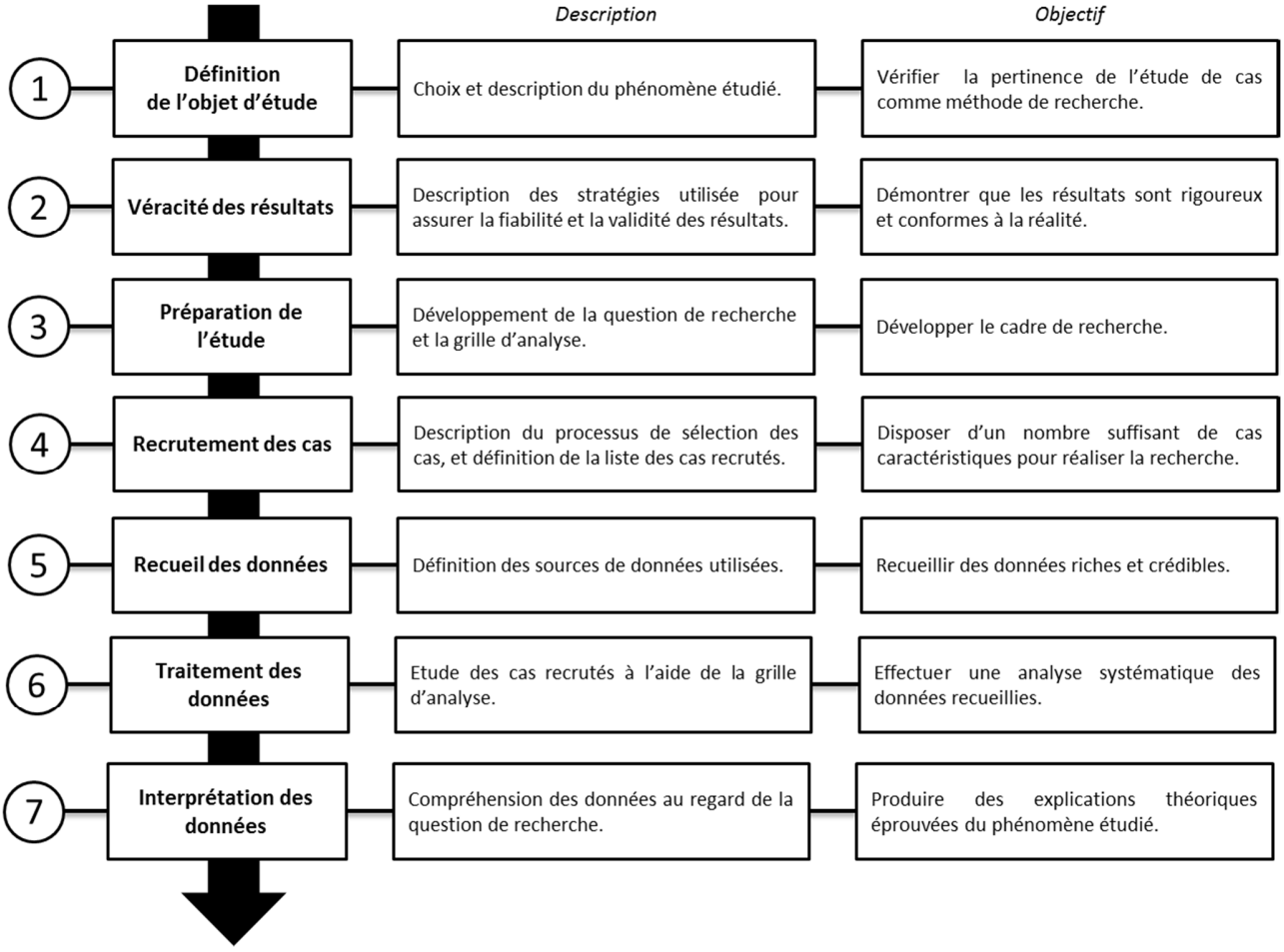


Figure 3 : Démarche de réalisation de l'étude de cas

Chaque étape du processus est explicitée dans les paragraphes suivants. Chaque étape est décrite et argumentée dans une transparence la plus complète possible, afin de montrer le suivi le plus méthodique possible du protocole de recherche, nécessaire à toute argumentation scientifique (Yin, 2003).

Etape 1 – Définition de l'objet d'étude

Cette étude porte sur les entreprises industrielles à hauts-risques pour la société. Ce type de système met en œuvre des processus technologiques qui ont comme particularité un niveau élevé de dangerosité. Leur perte de maitrise peut alors conduire à des conséquences catastrophiques : mortalité et morbidité humaine, pertes économiques, ou encore des pollutions environnementales de grande ampleur. Afin de maitriser ces risques, des stratégies de gestion sont mises en œuvre : analyse et outils techniques, facteurs humains, et approches organisationnelles réduisent la probabilité d'accident majeur.

Le sujet d'étude choisi ici est « l'accident industriel ». Le début de la démarche de recherche porte sur une question de départ très générale : « Quelles sont les faiblesses de la gestion des risques industriels ? ». Il s'agit de comprendre les mécanismes de l'accident industriel. Bien que cette étude corresponde à la seule première partie de ce travail doctoral, elle a pris une importance et une durée particulière.

Nous nous plaçons dans une perspective selon laquelle l'organisation est vue comme un système sociotechnique complexe, c'est-à-dire un « tout intégré ». Chaque composante de l'organisation, fonction, élément environnant joue un rôle dans les interactions organisationnelles. Dans ce cadre, l'accident industriel est la conclusion stratégique d'une suite d'évènements qui interagissent par une relation de cause / effet, mais également une complexité d'éléments de diverses natures en interaction, et issus de toutes les strates du système. Le choix d'une telle perspective oblige donc à comprendre quelles sont les relations entre les variables, et également pourquoi et comment ces relations existent. C'est-à-dire la description détaillée des acteurs, des relations, des fonctions, des situations et des évènements. La méthode d'étude de cas permet d'obtenir de tels résultats. Par son approche individualisée, elle permet de capturer la richesse de chaque situation personnalisée, comme peut l'être un accident industriel. Le choix de l'étude de cas n'est pas seulement un choix méthodologique, mais c'est également un choix relatif à l'objet d'étude.

Etape 2 – Véracité des résultats

L'utilisation de la méthode d'étude de cas impose de vérifier la validité et la fiabilité des résultats finaux (Gagnon, 2005). La notion de fiabilité renvoie à la constance et à la réplication des résultats. Selon cette exigence, des investigations répétées, et réalisées par d'autres chercheurs, doivent conduire à des résultats similaires.

La notion de validité renvoie à la justesse des résultats. Même si ceux-ci sont le fruit d'une méthode scientifique fiable et rigoureuse, ils doivent également faire preuve d'exactitude par rapport à la réalité. L'étude d'un accident industriel conduit à analyser des évènements par l'intermédiaire de données secondaires. Dans ce cadre, le chercheur est soumis à plusieurs biais d'analyse :

- **Le biais d'illusion holistique :** tendance à accorder aux éléments davantage de convergence qu'ils en ont en réalité, notamment en éliminant les éléments qui ne vont pas dans le même sens.
- **Le biais d'élite :** tendance à surestimer les éléments provenant d'informants qui énoncent clairement leur point de vue, et sous-estimer le point de vue d'autres moins bien clairement énoncés.
- **Le biais de surassimilation :** tendance à perdre sa propre vision et sa capacité d'analyse critique en devenant prisonnier des perceptions et des informations transmises par les intervenants locaux.
- **Le biais d'illusion rétrospective :** tendance à rationaliser après coup un événement imprévu et le considérer a posteriori comme plus probable ou prévisible qu'il n'était avant sa survenue.

Face à ces exigences de fiabilité et de validité des résultats, plusieurs garde-fous méthodologiques ont été fixés préalablement à l'étude. Concernant la fiabilité des résultats :

- **Position du chercheur :**

Dans le cadre de ce travail doctoral, l'éloignement géographique et temporel, dont les accidents industriels analysés font l'objet, assure une indépendance et l'absence de prise de partie entre les entreprises qui ont subies les accidents, et ce travail de recherche.

- **Sélection des sources :**

Rapports d'accident, publications scientifiques, bases de données, ouvrages, documents audiovisuels... Plusieurs types de sources de données sont disponibles. Elles délivrent des matériaux diverses, mêlant même parfois plusieurs types de matériaux : des faits, des analyses, des interprétations, ou encore des recommandations. Pour autant, ces sources ont

des origines variées, plus ou moins légitimes. Dans le cadre de ce travail, une classification des sources est réalisée, et décrite dans l'étape n°5. Cette catégorisation conduit, en fonction des caractéristiques de chaque type de sources, à accepter certains matériaux, et à en écarter d'autres.

- **Type des données recueillies :**

Le but de cette recherche est de comprendre le phénomène « accident industriel ». Pour cela, nous nous intéressons à décrire le fonctionnement du système industriel dans les moments précédant l'accident, ainsi que les éléments qui sont impliqués, ou qui ont contribué à la dynamique accidentelle. Pour atteindre cet objectif, nous avons porté notre attention, autant que possible sur les critères suivants :

  - Les faits : c'est la chaine accidentelle ;
  - Les causes immédiates et la chaine accidentelle ;
  - Les facteurs contributifs (aussi appelés « causes profondes ») ;
  - Les acteurs impliqués, et leurs relations ;
  - Les déterminants liés à l'environnement de l'organisation ;
  - Les processus et outils de gestion mis en œuvre.

Concernant la validité des résultats :

- **Nombre de cas étudiés :**

L'étude de cas est une méthodologie préparatoire à la conception d'une théorie généralisante. Cependant, un nombre élevé de cas étudiés permet d'accroitre la représentativité des résultats obtenus. Afin de satisfaire à cette exigence, un nombre représentatif de cas a été défini dans l'étape 3 : préparation de l'étude.

- **Sélection des cas étudiés :**

Afin de permettre une validité des résultats face à la problématique de recherche, un processus de sélection des cas étudiés est établi. Ce processus est décrit dans l'étape numéro quatre : recrutement des cas.

- **Effets de la présence de l'observateur :**

Lors du déroulement d'une enquête post-accidentelle, il existe un biais lié au recueil des données, provoqué par la menace de la sanction. Cependant, l'assermentation des témoignages liés au volet pénal de l'analyse, conduit généralement les témoins à ne pas divulguer de données, plutôt que de fournir des données volontairement erronées. C'est principalement la profondeur de l'analyse, et non sa validité, qui peut être impactée ici.

- **Particularités de chaque cas étudié :**

Chaque accident industriel possède ses propres spécificités. Cette particularité des cas est facilement descriptible, au regard des circonstances, des contextes environnementaux, des acteurs impliqués, ou encore du déroulement des évènements. Cependant, ce type de phénomène peut également présenter des similarités fortes entre les cas, et des items de comparaison peuvent émerger. C'est par exemple le cas en choisissant des descripteurs comme la technologie utilisée, le processus industriel mis en œuvre, ou encore le type d'évènement initiateur de la chaine accidentelle. Dans le cadre de ce travail, la construction de la grille d'analyse comparative des cas sera abordée dans l'étape numéro six : le traitement des données.

- **Existence d'explications rivales :**

Le phénomène « accident industriel » se prête facilement à la construction de théories explicatives rivales. Certains accidents industriels ont fait l'objet d'analyses contradictoires, que l'on peut qualifier de controverses, ou de polémiques. Un exemple récent est le cas de l'accident de l'usine AZF en 2001 (voir encadré de la page suivante). Dans le cas où plusieurs thèses seraient disponibles pour un même accident, le choix est fait de se référer aux principes de sélection des sources énoncées précédemment.

Exemple des principales théories rivales : l'explosion de l'usine AZF

L'usine AZF de Toulouse a été détruite le 21 septembre 2001 par l'explosion d'un stock de nitrate d'ammonium, causant 31 morts, plus de 2500 blessés, et d'importants dégâts matériels. A la suite de cet accident, plusieurs thèses explicatives ont émergé :

1 – La thèse officielle soutenue par les experts judiciaires fait état d'un accident chimique. La catastrophe aurait été provoquée par une erreur de manipulation, qui aurait conduit un employé d'une entreprise sous-traitante d'AZF à mélanger deux produits dangereusement incompatibles. Cela 15 minutes avant l'explosion. Les enquêteurs identifient ainsi des manquements dans la connaissance et la gestion du risque chimique sur le site (Barthelemy et al., 2001).

2 – Selon une seconde thèse, l'explosion aurait été l'effet domino d'une première explosion quelques secondes avant, et dont l'origine est extérieure à l'usine AZF. L'origine de cette première explosion serait la Société Nationale des Poudres et Explosifs, site de production à risques proche de l'usine AZF (Arnaudiès, 2005). Cette thèse de la double explosion est également soutenue par un rapport de l'Académie des Sciences (Menessier, 2009). La SNPE comme origine de cette première explosion est à nouveau évoquée (Valeurs Actuelles, 2003).

3 – D'autres thèses ont été évoquées à travers plusieurs médias : journaux, ou encore internet. Celles-ci ne font pas l'objet de sources valides, et ne sont donc citées qu'à titre d'illustration :

> Accident électromagnétique,
> Attentat Islamique,
> Tir de roquette en provenance d'une cité voisine,
> Fusée amateur,
> Chute de météorite,
> Chute d'avion,
> Ejection d'un filtre d'une tour de traitement sous l'effet d'un éclair...

Etape 3 – Préparation de l'étude

La préparation de l'étude a pour objectif de définir plusieurs éléments méthodologiques important. Le premier est la question de recherche qui pilotera l'étude. La portée de cette problématique conditionne ensuite la définition de l'échantillon étudié, ainsi que la construction de la grille d'analyse.

- **Définition de la question de recherche :**

Peut-on encore identifier dans l'analyse des différents accidents passés de nouvelles pistes d'amélioration ? Derrière cette question généralisant, notre objectif est l'identification de marqueurs récurrents dans l'ensemble des cas sélectionnés. La mise en perspective de plusieurs accidents passés doit permettre d'identifier des marqueurs récurrents de dysfonctionnement dans les activités de gestion des risques industriels.

Pour ce faire, la voie choisie est celle de la comparaison entre sécurité théorique, et sécurité opérationnelle réellement mise en œuvre. Nous postulons l'existence d'un décalage entre la représentation de la situation construite par le manager opérationnel, et la réalité du terrain. Cet écart serait alors un facteur contributif important de la réalisation de l'accident majeur.

En outre, il convient de délimiter le champ de notre travail. L'objectif de cette étude n'est pas de réaliser un nouveau retour d'expérience, pour en tirer un enseignement qui viendrait s'ajouter aux nombreux déjà existant. A titre d'exemple, l'accident de la raffinerie de Texas City renvoi à plusieurs centaines de références scientifiques, uniquement pour le bouquet *« Science Direct »*. Ce type de recherche nécessite une proximité de l'évènement, une grande disponibilité des données et des acteurs impliqués, ainsi qu'une grande quantité de ressources. De plus, ce travail ne vise bien entendu pas à discréditer les processus de retour d'expérience et d'analyses d'accidents déjà réalisés. Au contraire, leur impact a été considérable puisqu'ils ont permis d'améliorer notre connaissance des accidents, et a largement contribué à l'amélioration des performances de sécurité dans les industries à risques.

- **Définition de l'échantillon analysé :**

Un accident industriel est un phénomène susceptible de se reproduire dans une diversité de situations, dans des configurations propres à certaines variables récurrentes. Il s'agit ici de tirer des conclusions à partir d'un ensemble de cas. Pour cela, et avec l'objectif de fournir une étude valide et consolidée, au moins **dix cas seront analysés**. Le processus et les critères de sélection de ces cas sont expliqués dans l'étape suivante : étape 4 : le recrutement des cas.

- **Construction de la grille d'analyse :**

Comme indiqué précédemment, l'objectif de cette grille est la compréhension du déroulement et des causes des accidents sélectionnés. Il s'agit de mettre en lumière les écarts existant entre la sécurité théorique, et la réalité du terrain. Pour se faire, l'analyse portera sur la comparaison entre les règles, exprimées à travers le système de gestion de la sécurité, et la réalité du terrain, à travers les faits constatés par les enquêteurs. C'est une approche similaire à celle développée par les cyndiniciens. L'approche de la cyndinique est une démarche globale et systémique. Le but est de rendre intelligible les risques présents au sein d'un système, par la recherche d'écarts entre la situation telle qu'elle est perçue ou voulue, et la réalité (déficits systémiques cindynogènes) (Kervern, 1991).

Notre grille d'analyse comporte trois items :

1. ***Principales étapes de la chaine accidentelle :*** Cet item porte sur la dynamique de l'accident. Il s'agit ici de déterminer les principales étapes de la chaine accidentelle.
2. ***Description des faits :*** Il s'agit de lister les faits qui ont initié ou contribué au déroulement de la chaine accidentelle (défaillance technique, comportement humain...).
3. ***Ecart entre le système de gestion de la sécurité et la réalité :*** il s'agit de décrire les écarts de représentation entre les modes de gestion théoriques de la sécurité, et la réalité du terrain.

Une visualisation de la grille d'analyse complétée d'un exemple est présentée ci-dessous (Tableau 2) :

1. Principales étapes de la chaine accidentelle	**2. Description des faits**	**3. Ecart entre le système de gestion de la sécurité et la réalité**
Le *Blow-Out Preventer* n'a pas réussi à sceller le puit.	Plusieurs facteurs ont contribués à la défaillance du *Blow-Out Preventer :* • Le mode automatique de déclenchement a été défaillant.	Intégrité mécanique : des équipements d'urgence ont été défaillants. Ils n'ont pas su jouer leur rôle de mise en sécurité du process au moment le plus critique.
...	...	...

Tableau 2 : Modèle de grille d'analyse des accidents

Etape 4 – Sélection des cas

Deux contraintes imposent un processus de sélection des cas. La première est méthodologique. En effet, l'analyse de cas permet l'apport de conclusions qui répondent à une problématique de recherche. Il est donc nécessaire de sélectionner les cas en fonction de cette problématique. La seconde contrainte est capacitaire. Depuis l'explosion de la poudrière de Delft en 1654, le monde a enduré de nombreuses catastrophes industrielles. A titre d'image, la base ARIA, du BARPI, a déjà recensé plus de 40000 évènements (recherche réalisée dans la base ARIA le 1er mars 2014). Parmi eux, certains sont particulièrement remarquables. La gravité de leurs conséquences les place au rang d'accidents qui ont marqué les consciences. Les principaux évènements sont listés dans les tableaux suivants (Tableau 3 et 4) :

Date	Ville, Pays	Faits	Conséquences
16/04/1947	Texas City, Etats-Unis.	Explosion de nitrate d'ammonium.	581 morts et plus de 3000 blessés.
04/01/1966	Feyzin, France	Explosion dans un dépôt de GPL.	18 morts, 77 blessés.
10/07/1976	Seveso, Italie.	Surchauffe d'un réacteur chimique et libération d'un nuage toxique de dioxine.	200 personnes malades, contamination importante de l'environnement.
28/03/1979	Three Miles Island, Etats-Unis.	Fusion partielle du réacteur nucléaire.	Accident nucléaire catégorie 5, et faible relâchement dans l'atmosphère d'un nuage radioactif.
03/12/1984	Bhopal, Inde.	Relâchement de gaz toxique dans l'atmosphère.	10000 morts et 300000 malades.
26/04/1986	Tchernobyl, Ukraine.	Fusion du réacteur nucléaire.	Accident nucléaire catégorie 7, et relâchement dans l'atmosphère d'un nuage radioactif.
06/07/1988	Piper Alpha, Ecosse.	Explosion de la plateforme de gaz.	167 morts, et perte de la plateforme.
21/09/2001	Toulouse, France.	Explosion de nitrate d'ammonium.	31 morts, 2500 blessés.
23/03/2005	Texas City, Etats-Unis.	Explosion de la raffinerie.	15 morts, 170 blessés.
20/04/2010	Deepwater Horizon, Etats-Unis.	Explosion de la plateforme pétrolière.	11 morts, 17 blessés.
11/03/2011	Fukushima, Japon.	Surchauffe du cœur nucléaire consécutif à un tsunami.	Accident nucléaire catégorie 7.
17/04/2013	West, Etats-Unis	Explosion de nitrate d'ammonium.	15 morts, 160 blessés.
06/07/2013	Lac Megantic, Québec.	Explosion de wagons de matières dangereuses.	47 morts, destruction du centre-ville.

Tableau 3 : Principaux accidents industriels majeurs parmi les plus marquants depuis ces 50 dernières années

Date	Ville, Pays	Faits	Conséquences
27/03/1977	Tenerife, Iles Canaries.	Collision entre deux avions de ligne.	583 morts.
28/01/1986	Centre spatial Kennedy, Etats-Unis.	Désintégration de la navette spatiale Challenger lors du décollage.	7 morts, et interruption du programme spatial pendant 32 mois.
03/06/1998	Eschede, Allemagne.	Déraillement d'un train ICE.	101 morts, 100 blessés.
24/03/1999	Chamonix Mont Blanc, France.	Incendie du tunnel du Mont-Blanc.	39 morts, fermeture du tunnel pendant trois ans.
01/06/2009	Vol Paris/ Rio de Janeiro.	Abime en mer.	228 morts.
05/10/1999	Ladbroke Grove, Royaume-Uni.	Choc frontal entre deux trains.	31 morts, 520 blessés.
25/07/2000	Gonesse, France.	Ecrasement de l'avion supersonique Concorde après 2 minutes de vol.	113 morts.
01/02/2003	Navette Columbia.	Désintégration de la navette spatiale Columbia lors de la rentrée dans l'atmosphère.	7 morts.
12/07/2013	Brétigny sur Orge, France.	Déraillement.	7 morts, 30 blessés.
24/07/2013	Saint Jacques de Compostelle, Espagne.	Déraillement à grande vitesse.	79 morts et 140 blessés.

Tableau 4 : Principaux accidents de transport parmi les plus marquants depuis ces 50 dernières années

Appliqué à l'étude des accidents technologiques, le corpus d'évènements disponible peut être qualifié d'hétérogène. De plus, le fond documentaire est très important. Une première revue des évènements potentiellement intéressants permet d'isoler plusieurs critères de regroupement :

- **La date de l'accident** : l'occurrence d'accidents majeurs a accompagné le développement industriel, depuis les explosions de poudreries jusqu'aux industries actuelles.
- **Le domaine technologique** : les accidents répertoriés renvoient à des technologies diverses : production cyclique, production continue, transport de biens, transport de personnes, réseaux de matières dangereuses...
- **Les cultures industrielles mises en jeu :** les accidents ont lieu sur tous les continents développés, au sein de cultures du risque différentes. Sans rentrer dans une analyse culturelle du rapport de l'Homme au risque, ces aspects culturels peuvent peser sur la manière dont les risques sont gérés.

- **Les conséquences de l'accident :** les accidents revus ont généré des conséquences très variées en termes de conséquences humaines, économiques et environnementales, ainsi qu'en termes d'espace, de temps, et de désorganisation.

Ces quatre critères montrent toute la difficulté d'une tentative de rapprochement. Si cette diversité est une richesse, elle peut cependant poser des difficultés : difficulté à répondre à la problématique, difficulté à identifier les cas adaptés, et difficulté à compléter les items d'analyse choisis.

Cependant, il ne s'agit pas d'analyser à nouveau chaque accident en profondeur, mais plutôt d'identifier des marqueurs récurrents entre plusieurs accidents. Dans ce cadre, les critères sélectionnés ici sont le domaine technologique, la date d'occurrence, le lieu d'occurrence, et la gravité des conséquences. Ils sont fixés de la manière suivante :

- **Domaine technologique :** le domaine choisi est la chimie et la pétrochimie. Dans un objectif de représentativité, l'échantillon est limité à un seul domaine technologique.
- **Date d'occurrence :** les cas sélectionnés doivent être issus de périodes différentes et variées. A une date donnée, le niveau de connaissance et le développement technologique peut être similaire. Ces points communs peuvent constituer un biais d'analyse.
- **Lieu d'occurrence :** les cas sélectionnés doivent être originaires de territoires variés. Il s'agit ici de fixer au mieux un biais culturel relatif à des accidents issus d'une même zone géographique.
- **Gravité des conséquences :** les cas sélectionnés doivent être à l'origine de conséquences majeures. C'est-à-dire des impacts graves sur les personnes, les biens et l'environnement, ou encore être la cible d'un accident qui remet en cause la survie du système. Il ne s'agit pas ici d'analyse des presqu'accidents, ou encore des incidents mineurs.

Au regard des critères de sélection présentés précédemment, la liste des cas retenus est décrite dans le tableau suivant (Tableau 5) :

N°	Référence du cas	Domaine technologique	Lieu d'occurrence de l'accident	Date d'occurrence de l'accident	Gravité des conséquences
1	Delft 1654	Poudrerie	Delft, Pays-Bas	12/10/1654	Une centaine de morts
2	Grenelle 1794	Poudrerie	Grenelle, France	31/08/1794	Plus de 1000 morts
3	Oppau 1921	Chimie	Oppau, Allemagne	21/09/1921	561 morts, 1 952 blessés et 7 500 personnes sans-abris
4	Texas City 1947	Stockage pétrolier	Texas City, EUA	16/04/1947	581 morts, 3000 blessés environs
5	Feyzin 1966	Stockage pétrolier	Feyzin, France	04/01/1966	18 morts, 77 blessés
6	Bhopal 1984	Chimie	Bhopal, Inde	03/12/1984	10000 morts, 30000 malades environs
7	Piper Alpha 1988	Extraction pétrolière	Mer du nord	06/07/1988	167 morts, perte de la station
8	Institute 2008	Chimie	Institute, EUA	28/08/2008	2 morts, 8 blessés, 40000 personnes confinées pendant 3 heures.
9	Texas City 2005	Raffinage	Texas City, EUA	23/03/2005	15 morts, 170 blessés
10	Deepwater Horizon 2010	Exploration pétrolière	Golfe du Mexique	20/04/2010	11 morts, 17 blessés, pollution maritime de grande ampleur

Tableau 5 : Description de l'échantillon d'accidents sélectionnés pour l'analyse

Une illustration des cas sélectionnés est proposée page suivante (Figure 4).

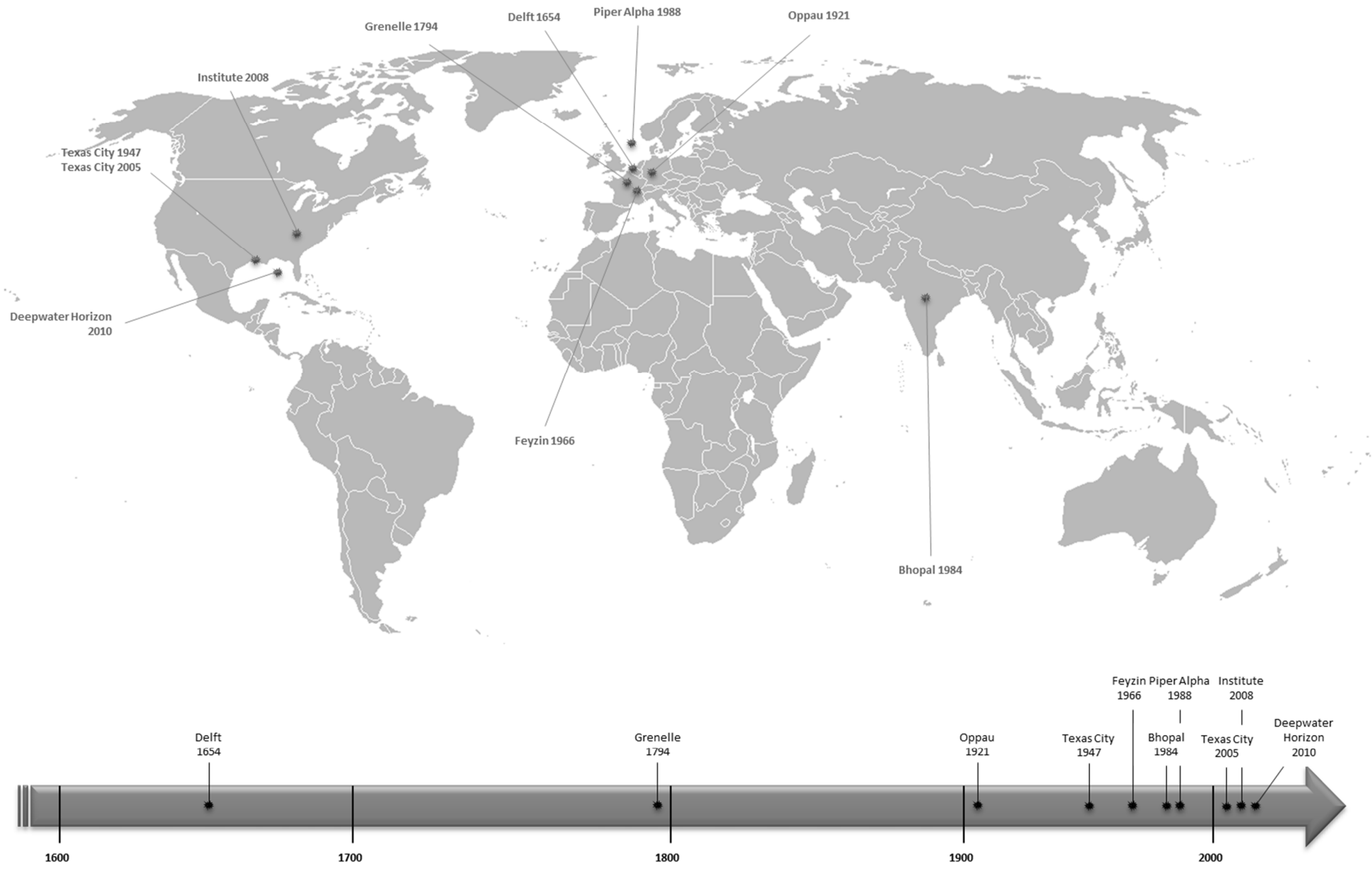


Figure 4 : Répartition spatiale et temporelle des cas sélectionnés pour l'analyse

Etape 5 – Collecte des données

Pour réaliser cette étude, plusieurs sources de données sont disponibles, selon la typologie suivante.

Tout d'abord, les principaux matériaux utilisés sont les **rapports officiels d'enquête post-accidentelle**. Ces documents s'appuient sur des faits constatés par les enquêteurs. De plus, ils ont été rédigés par des auteurs qui ont fait l'objet d'un processus d'indépendance et de légitimation lié au statut « d'enquêteur mandaté ».

La seconde source d'informations utilisée est les **publications scientifiques**. La logique de ce type de source est d'utiliser certains faits et de les interpréter dans un objectif de démonstration particulier. Il est donc légitime de s'interroger sur la fiabilité de ce type de source, notamment dans le cas où l'objectif de la publication n'est pas celui de cette étude. En outre, les publications utilisées ont toutes fait l'objet d'un processus de sélection thématique, de relecture par les pairs, avant la diffusion de leurs résultats dans la recherche.

Les **ouvrages** portant sur certains accidents industriels constituent la troisième catégorie de source utilisée. Les théories qu'ils véhiculent apportent un éclairage particulier qui permet d'améliorer la compréhension des accidents étudiés. Egalement, les ouvrages sélectionnées portent des théories qui ont largement fait l'objet de discutions scientifiques critiques dans leur communauté.

Les **documentations techniques** et les **bases de données** sont également utilisées. La validité des informations émises est garantie par le choix de sources adossées à des instituts de recherche et d'expertise dans le domaine du risque et de l'accidentologie industrielle.

La dernière catégorie de sources utilisées est composée de **documents audiovisuels** (enregistrement audio, vidéo...) et **de documents issus de sources non scientifiques** (revues, sites internet...). Ces types de documents peuvent faire l'objet d'un manque de fiabilité, dû à certaines limites méthodologiques possibles : les auteurs ne sont pas reconnus par la communauté scientifique, les argumentations ne s'appuient pas sur des faits établis, ou encore les résultats n'ont pas fait l'objet d'un processus de relecture par les pairs, et de diffusion de la recherche. Face à ces réserves, ce type de sources n'a pas été utilisé pour

corroborer des faits ou en apporter de nouveaux. Ces documents ont uniquement servi à identifier et écarter des théories rivales.

II.3 Analyse de 10 accidents industriels majeurs passés

En premier lieu, notre analyse des accidents sélectionnés démontre les limites des démarches classiques de gestion des risques. En effet, la sécurisation des systèmes technologique s'appuie historiquement sur trois axes d'action : technique, humain, et organisation (Figure 5).

Figure 5 : Types d'action mis en œuvre pour la sécurisation des systèmes technologiques

La catégorie « organisation » renvoie aux moyens de prévention relatifs à l'organisation du travail. On parle d'organisation lorsque deux conditions sont remplies. Lorsqu'il existe tout d'abord une division des tâches entre plusieurs personnes. Ensuite lorsqu'une coordination des tâches est nécessaire pour accomplir l'objectif final. On trouve généralement dans cette catégorie des mesures relatives aux procédures de travail, procédures de sécurité, au rythme de travail, aux systèmes de gestion existants (EPI, formations, retour d'expérience, respect des normes...).

La catégorie « humaine » renvoie aux moyens de prévention relatifs aux ressources humaines. On y trouve généralement les mesures associées :

- au recrutement (compétences, certification, adéquation au poste de travail…),
- à la formation du personnel (formation sécurité, permis spécifiques…), à l'information du personnel (affichage de sécurité…),
- au suivi médical (visite médicale d'embauche, surveillance renforcée…), à l'environnement de travail (température, éclairage, ergonomie du poste de travail…),
- aux relations sociales (bien être, charges mentales…).

Enfin, la catégorie « technique » renvoie aux moyens de prévention relatifs aux ressources techniques. Elle regroupe l'ensemble des outils et équipements permettant aussi bien la détection (capteur…) que la protection (carter…).

Cette approche de la sécurité a servi de découpage conceptuel à de nombreuses méthodologies de gestion des risques. On peut citer à titre d'exemple la méthode ATHOS (Le Coze et al., 2002).

Les limites de l'approche Technique / Humain / Organisation

Cette conception de la sécurité repose sur l'hypothèse que la maitrise de manière indépendante, individuelle, et ponctuelle, des causes relatives à chacun des trois champs permettent globalement d'éviter l'occurrence d'un accident. Notre étude remet en cause cette hypothèse. En effet, l'analyse des différentes causes contributives des accidents étudiés met en exergue la nature systémique de l'accident industriel. Des causes de natures variées, issus de toutes les dimensions du système, et parfois dissimulées au cœur de la vie quotidienne, se combinent pour former une chaine accidentelle. Défaillance technique, écart à la procédure, test non réalisé, sous-dimensionnement de composant, absence de communication... La chaine accidentelle nécessite l'inaction de l'ensemble des barrières de sécurité prévues pour faire face à la complexité des process industriels à hauts-risques. L'accident n'est pas seulement technique, humain, ou organisationnel, il est l'ensemble des trois. Il est le fruit de multiples facteurs. Notre étude comparative a permis d'identifier une

typologie de douze grandes familles récurrentes. Le schéma suivant illustre toute la dimension systémique de l'accident industriel (Figure 6). Chacun de ces facteurs est décrit dans l'annexe n°2.

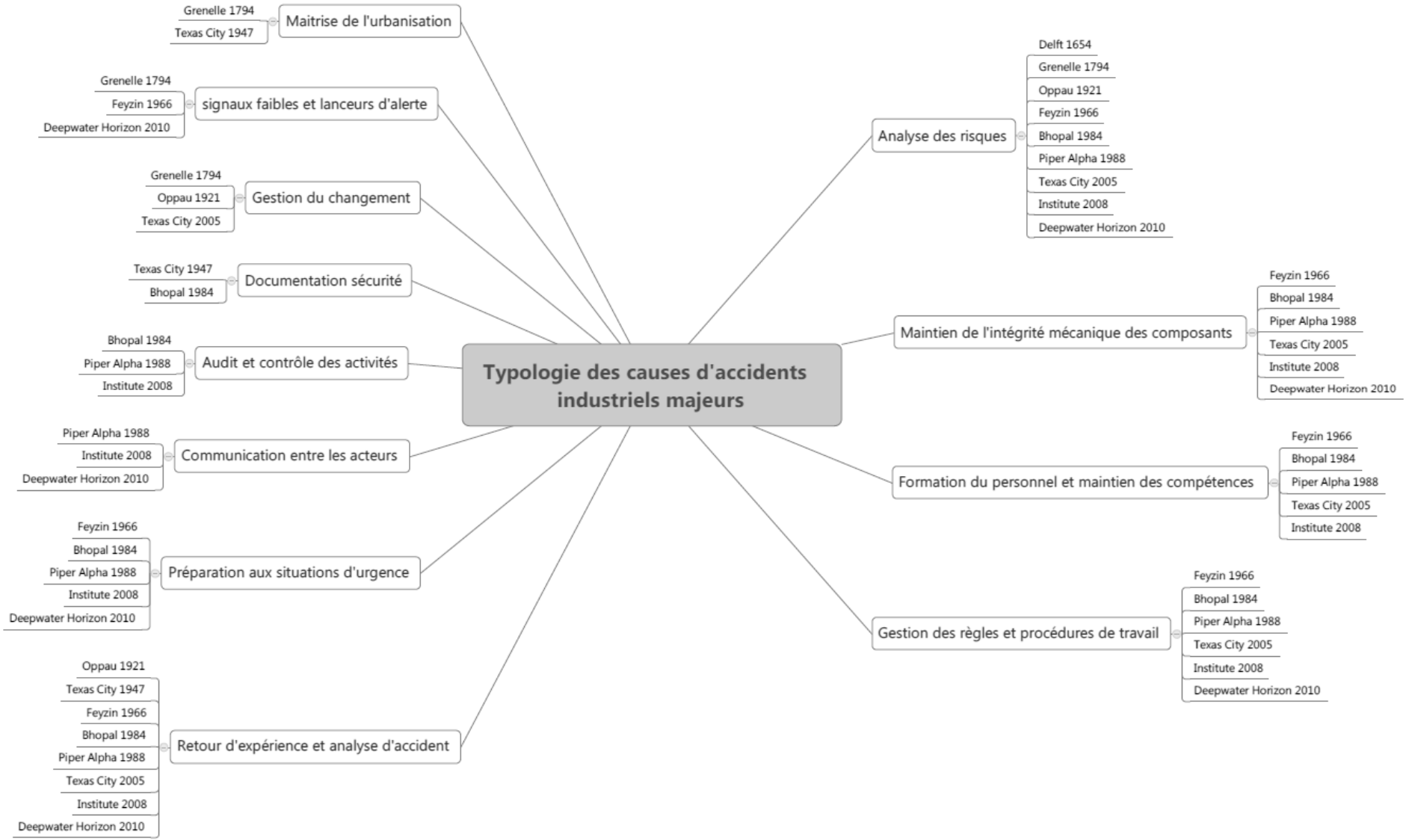


Figure 6 : Familles de causes des accidents industriels majeurs

Egalement, la vision systémique du phénomène accidentel est renforcée par l'identification de plusieurs constats sur la construction des accidents, et notamment leurs causes. Cependant, le modèle classique Organisation/technique/Humain, n'en permet pas l'analyse. Trois phases peuvent être identifiées.

Dans une première phase, les causes impliquent tous les services et toutes les strates du système industriel : direction de production, ingénierie, ressources humaines, administration, achats... Pour illustrer ces propos, on peut considérer l'ensemble des acteurs et relations de l'entreprise nécessaire au recrutement d'un simple opérateur. Celui-ci a été recruté, formé, peut être averti des difficultés, rappelé à la règle, ou encore autorisé à des écarts. Egalement, le manager a été engagé, a reçu des objectifs, des ressources, un pouvoir décisionnel, et une autorité. De nombreux acteurs peuvent être impliqués dans toutes ces tâches (direction, management intermédiaire, ressources humaines, services supports...). L'opérateur et le manager appartiennent donc à plusieurs réseaux complexes, imbriqués, qui influent leurs représentations, leurs décisions, et leurs comportements. Ainsi, la cause de l'accident n'est pas seulement le comportement de l'opérateur, ou encore la défaillance du composant, mais est également à rechercher dans l'ensemble des services, et à tous les niveaux du système.

A titre d'exemple, l'analyse de l'accident de Feyzin (en 1966) a montré la contribution de plusieurs strates du système. Tout d'abord, la conception du système occasionnait un givrage presque simultané des vannes lors de la détente de gaz, permettant le blocage en position ouverte. Egalement, le management a émis une demande d'intervention, alors que les conditions environnementales ne respectaient pas les conditions opératoires. Enfin, les opérateurs n'ont pas respectés les procédures de travail pour la manœuvre des vannes.

A Bhopal en 1984, le top management de l'entreprise a fortement réduit le personnel pour faire face à ses difficultés financières. Egalement, le management opérationnel était absent lors de la phase accidentelle. Les opérateurs n'ont pas respectés les procédures à mettre en œuvre en cas d'accident. Enfin, le personnel médical de la ville n'était pas informé de la dangerosité des produits, et de la manière de traiter leurs effets sur l'Homme.

A Texas City, en 2005, les experts ont sous-estimés le niveau de risque associé au placement des baraquements temporaires au plus près du process industriel. L'enquête a également dénoncé la politique de réduction des moyens alloués à la sécurité mise en place par le top management, et le manque important de supervision des activités par le management opérationnel.

Dans une deuxième phase, il apparait que les causes sont dissimulées au cœur des activités quotidiennes. La vie d'une entreprise industrielle est faite de situations informelles. La plupart des interactions et des informations échangées ne sont pas formalisées (c'est par exemple le cas de l'avalisation d'un écart par un manager entre deux réunions). Les contraintes de production imposent des ajustements quotidiens et des prises de décision immédiates (comme la non réalisation d'une procédure de vérification). L'automatisation des process et des systèmes de mesures conduit à une confiance totale en la machine, et neutralisant le doute et le questionnement (c'est par exemple le cas de la déportation des systèmes de contrôle, qui conduit à créer des représentations qui ne sont pas celles souhaitées par l'opérateur, mais celles imposées par le concepteur. Ce repositionnement de l'opérateur en marge du process le conduit à porter une confiance totale à ses indicateurs et aux alarmes préprogrammées). Les actions de sécurité semblent parfois incompatibles avec la tenue des objectifs de production, et sont alors réalisées avec un minimum de ressources, et uniquement dans un but de satisfaction administrative ou hiérarchique (c'est par exemple le cas lors de validation systématique de check-list sans application réelle de la procédure). La surcharge procédurale et organisationnelle conduit à la mise en place de stratégie d'évitement de situations bloquantes pour l'opérateur (c'est par exemple le non signalement d'un évènement de sécurité, qui bloquera le processus de production). La plupart de ces modes de contournement des règles sont invisibles et non détectables.

A titre d'exemple, avant l'accident de la plateforme Piper Alpha (en 1988), les carnets de bord des équipes de conduite ne faisaient pas l'objet d'un remplissage précis des évènements rencontrés. Le démontage des vannes n'était pas consigné, les procédures d'allocation des permis feu n'étaient pas respectées. Ainsi, l'équipe montante ne possédait pas les informations nécessaires à la conduite du process en sécurité.

Concernant l'explosion de l'usine d'Institute (en 2008), l'interface de contrôle des installations a été modifiée sans questionnement associé à la compétence des opérateurs. Le nouveau système était fondé sur une représentation différente du processus de production. Cela n'a pas permis à l'opérateur d'avoir une vision précise de l'état réel des installations.

Sur la plateforme Deepwater Horizon, des équipements de sécurité, tels que des alarmes, étaient quotidiennement déconnectés, afin de ne pas entraver le bon déroulement des activités de production.

Et dans une troisième phase, nous pouvons conclure que les causes concernent l'ensemble du cycle de vie du système industriel. La sécurité d'un système est comprise à travers toutes les phases de son cycle de vie. La première phase est relative à la conception du système. Les choix de formes, de matériaux, de technologies, et d'assemblages, ainsi que les spécifications d'exploitation conditionneront le niveau de complexité et les modes de défaillances du système. Le niveau de sécurité dépend également de sa fabrication à travers la qualité des matériaux, des méthodes, et des normes de travail utilisés lors de l'assemblage des éléments du système. Enfin, c'est pendant les phases d'exploitation que le niveau de sécurité est maintenu dans le temps. Au-delà de ces trois phases, théoriques, le système industriel est amené à évoluer. Les process de production se complexifient, avec davantage de fonctions, davantage de composants, et davantage de combinaisons possibles dans les scénarios accidentels. Ainsi, de nouveaux évènements de sécurité sont possibles, alors même qu'ils n'ont pas été prévus dans l'analyse des risques initiale. Ainsi, le choix des hypothèses d'analyse des risques, la sélection des technologies, et les pratiques de gestion peuvent se conjuguer en scénarios accidentels, pré-identifiés ou non, et prennent racines dans toutes les étapes de cycle de vie du système industriel.

A titre d'exemple, à Oppau, dans les mois précédant l'accident, des modifications ont été apportées au procédé de fabrication, facilitant l'explosivité du mélange. Des tests auraient dû être réalisés sur le nouveau mélange, afin de s'assurer d'un niveau de stabilité minimal nécessaire. Mais ces tests n'ont pas été réalisés.

A l'origine conçue pour l'exploitation pétrolière, l'activité de la plateforme Piper Alpha a été réorientée vers l'extraction de gaz. Le principal risque n'était plus l'incendie, mais l'explosion en cas de fuite de gaz. Le soir de l'accident, les protections pare-feu n'ont pas été efficaces face aux explosions de gaz.

A la raffinerie de Texas City, en 2005, certains équipements de protection étaient sous-dimensionnés, ou manquant. L'augmentation du potentiel de danger du process n'a pas été prise en compte par une mise à jour de l'analyse des risques. Ainsi, du fait de l'évolution de l'activité de la raffinerie, les scénarios accidentels identifiés ne correspondaient plus à ceux concrètement possibles, et les équipements de sécurité associés étaient obsolètes et inefficaces.

L'existence de symptômes systémiques

Le caractère systémique de l'accident fait émerger des symptômes transverses qui nécessitent d'aborder la sécurité dans une approche globale. Notre étude a permis d'identifier plusieurs phénomènes : la migration des pratiques, la dérive du comportement global, et la phase de résistance.

Le premier symptôme transverse est celui de la migration des pratiques du système. Dans la littérature scientifique, le terme de « migration » s'inscrit dans les travaux d'Amalberti (2013), portant sur la création d'un modèle de migration typique des pratiques professionnelles. Selon cet auteur, les pressions de production entrainent les opérateurs vers une zone de productivité accrue. Mais c'est également une zone opérationnelle dégradée par rapport au modèle initial, où les situations dangereuses vont se multiplier, et s'amplifier, créant ainsi des risques majeurs de perte de contrôle du process industriel.

Au départ, les process industriels font l'objet d'une conception très prudente. Des barrières techniques (composants redondants, diversifiés) et organisationnelles (procédures de travail, règles d'exploitation) sont prévues pour assurer un niveau de sécurité optimal. Mais peu à peu, les conditions vont être modifiées par les acteurs du système, afin de gagner en performance et en confort de travail. Deux phénomènes sont à l'origine de ces dérives. Le premier concerne la propension des opérateurs à s'approprier et modifier la manière dont ils réalisent leurs tâches. L'évolution des contraintes de production, l'augmentation des performances demandées, ou encore la réduction des ressources allouées, obligent les opérateurs à réaliser des écarts aux règles, et des ajustements qui compromettent peu à peu le niveau de sécurité. On peut par exemple demander aux opérateurs de faire davantage avec moins de personnel et de matériels. En conséquence, des équipements de sécurité ne sont pas installés, ou encore des contrôles et des vérifications sont supprimés, afin de gagner du temps. Ces écarts, notamment lorsqu'ils ont un effet positif sur les performances, ne conduisent généralement à aucune sanction managériale. Ils deviennent alors des nouveaux standards de communauté, illégaux, mais tout à fait normaux dans la vie quotidienne de l'entreprise. Le second phénomène concerne la période que l'on pourrait appeler « de rodage » du système industriel. L'analyse théorique de sûreté de fonctionnement réalisée lors de la phase de conception conduit à la définition de barrières de sécurité nécessaires à une mise en œuvre dans des risques calculés et assumés. Cependant, le système de départ fait l'objet d'une complexification croissante. A titre

d'exemple, la superposition de multiples règles et équipements réduisent théoriquement le risque, mais sont parfois difficilement réalisables concrètement. C'est notamment le cas lorsque les systèmes sont conçus ou modifiés sans prise en compte du point de vue des opérateurs qui interviendront quotidiennement.

L'écart entre théorie et pratique émerge également lorsque le process subit des modifications, sans qu'aucune mise à jour de l'analyse des risques, et des barrières de sécurité, ne soit réalisée. Bien qu'initialement adaptées au process, les mesures de sécurité ne permettent plus d'assurer une protection suffisante en cas de situation anormale. Ces dérives des pratiques professionnelles vont créer un décalage entre les règles d'exploitation théoriques, et les activités réellement mises en œuvre. C'est ainsi que le système fait l'objet d'une migration progressive, vers un état où les barrières de sécurité sont inefficaces, et le risque non maitrisé.

De nombreux exemples montrent l'existence de migration des pratiques. Avant l'explosion de la poudrière de Delft, des sources d'inflammation étaient régulièrement introduites sans mesures particulières, et ce malgré la dangerosité des produits chimiques utilisés.

Sur la plateforme Piper Alpha en 1988, les modules de formation des opérateurs à la gestion des situations d'urgence étaient hâtifs, partiellement suivis, et régulièrement annulés.

A l'usine agro-pharmaceutique d'Institute, les opérateurs contournaient régulièrement les dispositifs de sécurité lors du remplissage des réservoirs, à l'encontre des procédures écrites, et avec l'accord de l'agent de maitrise.

Le deuxième symptôme systémique est celui de la dérive du comportement global du système. L'idée de dérive des pratiques a également été développée par Rasmussen et al. (2000). Selon l'auteur, les accidents industriels majeurs sont le résultat d'une dérive systématique du comportement global de l'organisation vers l'accident. Ce mouvement est impulsé par une pression, une contrainte en faveur du rapport coût / efficacité dans un environnement très compétitif. Dans ce contexte, les pressions de production sont directement reportées sur les différents acteurs du système, dans leur contexte habituel de travail. Chacun a de larges chances de subir la même tension liée à la compétitivité, et prend alors, dans sa propre vision incomplète du système, le risque d'un écart aux règles. Cette action est réalisée afin de maximiser sa performance, en considérant toujours que les

parades et défenses prises par les autres sont encore pleinement efficaces. Dans cette situation, la limite d'un comportement dit « sûr » d'un acteur en particulier, dépend des écarts possiblement réalisés par les autres acteurs. Une variation habituelle du comportement, même si celle-ci est acceptable dans le mode de gestion « normal », peut conduire à un dysfonctionnement grave et non-prévisible. La période de migration des pratiques professionnelles vers un état du système propice au développement d'un accident industriel majeur a été autrement formulée par Turner et al. (1978), sous le terme de période d'incubation. Ces travaux ont été repris dans un autre contexte, celui des établissements hospitaliers, par Bignell et al. (1984). L'idée principale est qu'une incubation plus ou moins longue est nécessaire à l'occurrence d'un accident industriel majeur. La dynamique de l'accident, formalisée par la chaine accidentelle, et initiée par un évènement déclencheur, intervient en fin de cycle. Elle est d'une durée relativement courte. Dans sa globalité, le cycle d'incubation peut se prolonger pendant des mois, ou même des années. Cette période se caractérise par une dégradation progressive plus ou moins marquée de la sécurité, une prise de conscience apparente limitée de cette dégradation par les opérateurs et le management, et une minimisation de cette dégradation. Constatée dans la plupart des accidents industriels majeurs, la reconnaissance de l'existence de cette période d'incubation est un enjeu majeur pour l'anticipation des accidents, là où, dans son déroulement, « l'accumulation d'un ensemble d'évènements qui ne sont pas remarqués car ils sont en contradiction avec les croyances partagées sur les risques et la manière de les éviter ». Llory et al. (2010).

Globalement, la dérive du comportement peut être observée à travers différents aspects du système. A Bhopal en 1984 avant l'accident, les travaux de recherche ont montré plusieurs dynamiques concomitantes : une absence de contrôle des autorités, une baisse importante du personnel qualifié, des modifications dans les procédures de sécurité vers moins de surveillance, la suppression ou l'arrêt de dispositifs de sécurité, la réduction de la maintenance des équipements, et l'absence du personnel d'encadrement.

A Texas City en 2005, l'enquête post accidentelle a montré de nombreux écarts entre les règles et les opérations telles qu'elles furent mises en œuvre : l'application erronée du modèle de calcul du risque, conduisant à une sous-estimation, l'application partielle des consignes de sécurité, le sous-effectif du personnel de production, la réduction des budgets de formation, ou encore des écarts nombreux récurrents, et acceptés aux procédures de travail.

Sur la plateforme Deepwater Horizon, en 2010, a été constaté la suppression de dispositif de surveillance (capteur de flux), la modification du matériel de contrôle de puit, en contradiction avec les règles, l'absence de procédures opérationnelles critiques (pour la mise en œuvre des tests d'étanchéités), la déconnection des barrières de sécurité (court-circuit du capteur de flux, alarme générale en sourdine), ou encore l'absence de vérification des équipements d'urgence.

Enfin, le troisième symptôme transverse est celui de la phase de résistance du système, matérialisée par des signaux faibles. Dans des conditions de dégradation progressive du niveau de sécurité, certaines phases particulières d'exploitation ne peuvent plus être contenues. C'est par exemple le cas de périodes transitoires, d'arrêt de maintenance, ou encore de reprise d'activité. Des signaux, symptômes de la dérive du système, émergent alors à un niveau individuel. Ils émergent à plusieurs niveaux, du niveau opérationnel au managérial. Ils émergent également de manière plus ou moins précoce, c'est-à-dire de plusieurs semaines avant l'évènement, jusqu'au début de la chaine accidentelle.

Dans la littérature actuelle, ces signaux font l'objet d'un champ sémantique riche. Les termes « signaux faibles », « signal d'alarme », « signal avant-coureur », « signal précoce » sont parfois utilisés de manière interchangeable, ou sans distinction de sens (Saltmarsh et al., 2012). Dès 1975, Ansoff formule l'idée selon laquelle il existe dans le présent des symptômes de changements possibles dans le futur. Il utilise alors l'expression de « signal faible » pour désigner des informations précoces et imprécises indiquant l'imminence d'évènements impactant (Ansoff, 1975). Selon Vaughan, un signal faible est un signal difficile à décoder, ou un signal qui, après analyse, paraît si improbable que les opérateurs considèrent qu'il a peu de chances de se reproduire (Vaughan, 2001). Pour Hiltunen (2008b), un signal faible est un avertissement précoce, dont la force grandit en se combinant à d'autres signaux. Mevel conclut que les signaux faibles s'apparentent à des «bruits» dont la valeur n'est perçue qu'après un traitement approprié, qu'il soit individuel ou collectif (Mevel, 2004). Les précurseurs regroupent les conditions, évènements, qui précèdent et conduisent à un accident (Phimister et al., 2003). Pour le United State Nuclear Regulatory, un précurseur fait référence à un évènement ou des conditions opérationnelles qui sont des éléments d'une séquence accidentelle postulée (Keller et al., 2005). Pour Carroll et al. (2011), un précurseur est un évènement nécessaire à l'occurrence d'un accident dans un scénario donné.

Dans le domaine de la gestion des risques industriels, la notion de « signaux précurseurs » a émergé de l'analyse de grands accidents technologiques, tels que Challenger, Columbia, ou encore Texas City. En 1978, Turner propose l'hypothèse des précurseurs. La plupart des accidents sont liés à des enchainements d'erreurs et de défauts, parfois complexes, mais presque toujours détectables au cours d'une période dite d'incubation (Turner et al., 1978). Vaughan (1996) reprend l'idée que des signaux précurseurs sont disponibles dans l'organisation mais que ceux-ci ne sont pas traités. Elle appelle cette dynamique de l'organisation jusqu'à l'accident «normalisation de la déviance». Le mouvement des organisations hautement fiables a également mis en avant l'importance de la prise en compte des signaux faibles dans la sécurité des systèmes. Le maintien des opérateurs à un niveau élevé de vigilance, appelé «conscience situationnelle», permet de détecter les problèmes naissant et d'apporter des ajustements immédiats, ce qui évite potentiellement la génération de situations indésirables plus impactantes (Weick et al., 2008).

Si la question des signaux faibles fait l'objet d'une intellectualisation abondante récente, ceux-ci ont été identifiés dans de nombreux accidents industriels majeurs. A Grenelle en 1794, de nombreuses alertes avaient été émises par une autorité scientifique sur les risques associés à la poudrière, et notamment l'impact d'un changement rapide de rythme de travail sur la maitrise de la stabilité des produits.

A Feyzin, en 1966, les difficultés d'intervention liées à la conception dangereuse des installations avaient été soulevées à plusieurs reprises par des membres du personnel. Les demandes de modification issues des opérateurs n'ont pas été prises en compte, manquant ainsi une opportunité d'améliorer le niveau de sécurité du système.

Sur la plateforme Deepwater Horizon, dans les semaines qui ont précédées l'accident, le personnel a été confronté à plusieurs changements d'organisation. Ces modifications fonctionnelles et hiérarchiques, en impactant les rôles et responsabilités de plusieurs managers, ont profondément affecté le système de management. Ces difficultés ont fait l'objet de nombreuses alertes orales et écrites sur les tensions dans l'équipe, et la difficulté à atteindre les objectifs demandés.

Au regard de notre analyse, la sécurisation classique par une approche de sureté de fonctionnement, à laquelle s'ajoute une prise en compte de plus en plus effective des facteurs humains et organisationnels, est nécessaire pour assurer la maitrise du système industriel. Pourtant, cette vision a des limites. La gestion disciplinaire de chaque type de cause possible ne permet pas d'empêcher les accidents industriels majeurs. Dans la

profondeur du système, des symptômes transverses émergent. Ces défis systémiques sont difficilement appréhendables par le modèle « Technique / Humain / Organisation », et nécessite une approche globale du système.

III – L'évolution de l'environnement décisionnel du manager opérationnel

Depuis une trentaine d'années, le volet managérial de la maitrise des risques industriels est devenu un élément central de l'attention scientifique et normative (Hale, 2003). Avec cette nouvelle dimension, la société entre dans le troisième âge de la sécurité (Hale et al., 1998).

L'évolution des modèles de production de sécurité a conduit à modifier notre perception de l'accident industriel majeur. Les facteurs humains et organisationnels sont également contributeurs de l'évènement accidentel. En outre, malgré ces schémas d'actions poussés, notre étude a montré l'existence de faiblesses rémanentes dans la pluparts des organisations qui ont subi un accident : la dimension systémique de l'accident, la dérive des pratiques de l'entreprise, et la prise en compte des périodes de résistance.

De multiples rapports d'accidents (Challenger, Texas City, Deepwater Horizon...) ont questionné l'absence de décision de prudence, et ont donc indirectement critiqué la non prise d'initiative. Pour permettre la prise de décision d'anticipation, trois défis sont à lever par le manager :

- ***La complexité :*** c'est le défi de la compréhension du système, de ses mécanismes, de son fonctionnement, et de son évolution.
- ***L'érosion du temps :*** c'est le défi de l'instantanéité du monde actuel. Il s'agit de réinscrire la gestion dans la durée de long terme de la vie d'un système industriel.
- ***La décision :*** rassembler les conditions d'émergence de la phase de décision, afin de passer du choix imposé par l'environnement, et répondre au défi de l'initiative.

III.1 Le défi de la complexité

Est complexe ce qui ne peut pas se ramener à une loi ni se réduire à une idée simple (Morin, 2011). Selon Morin, la pensée complexe est la pensée qui va accepter la complexité, c'est-à-dire la contradiction. La complexité n'est pas un refus de la simplicité, mais une ouverture sur l'inconcevable. En ce sens, la complexité de Morin est le « principe de la pensée qui considère le monde et non pas (…) le principe révélateur de l'essence du monde », (Introduction à la pensée complexe, p. 138). C'est une pensée qui cherche à la fois à respecter la spécificité de chaque champ du savoir, tout en préservant le lien entre toutes les disciplines allant de la philosophie à la physique, en passant par la sociologie, la biologie ou la psychologie. La complexité correspond à ce projet d'interprétation des différents savoirs en vue de préserver l'autonomie de chaque discipline tout en mettant en lumière leur interdépendance essentielle.

La notion de complexité fait référence à un système que l'on tient pour irréductible à un modèle fini quelle que soit sa taille, le nombre de ses composants, et l'intensité de leur interaction. Pour un observateur, il est complexe parce qu'il tient pour certain l'imprévisibilité potentielle des comportements. La complexité est une propriété attribuée au phénomène observé par l'acteur du fait des représentations qu'il s'en fait. Or le phénomène peut juste s'avérer compliqué, juste compliqué puisque déterminé et réductible à un modèle unique et complètement calculable. Mais si les systèmes complexes ne peuvent être réduits à des modèles explicatifs, ils n'en sont pas moins compréhensibles.

La complexité d'un système industriel est visible à travers l'étude des accidents majeurs. Notre analyse a permis d'identifier deux aspects de complexité. Le premier aspect concerne les causes des accidents. Celles-ci concernent toutes les fonctions (achats, communication, ingénierie, production, formation...), et toutes les strates du système (opérateurs, management opérationnel, top management). Elles concernent toutes les activités quotidiennes liées aux opérations, de la défaillance complète d'une barrière, au simple ajustement ponctuel de procédure. Enfin, elles concernent toutes les étapes du cycle de vie du système (conception, production, maintenance...). L'analyse des causes constitue une « photo » de l'accident. C'est un scénario parmi de nombreux possibles, qui adopte une conjonction particulière de différents éléments du système.

Le second aspect de la complexité est rendu visible avec l'existence de symptômes systémiques. La migration des pratiques, la dérive globale du système, et l'émergence

d'une période de résistance, matérialisée par des signaux faibles, sont des phénomènes qui font partie intégrante de la dynamique accidentelle. Elles sont les signes de comportements émergeants, non-prévus, ou non pris en compte par le système.

Ancrage théorique de la complexité au sein des systèmes industriels de production

Plusieurs auteurs ont formalisé la notion de complexité au sein de systèmes de production industrielle. Et l'approche de la complexité a évolué au cours des développements scientifiques. Perrow (1984) décrit que la complexité d'un système dépend du nombre d'éléments qui composent ce système et le nombre d'interactions et de couplages entre ces éléments. Un processus industriel nécessite la mise en œuvre d'une grande quantité d'éléments. Cette complexité technologique interagit avec cinq autres types de composantes du système : les procédures, des opérateurs, des matériaux et fournitures, et un environnement nécessaire à l'exploitation du système. La multiplicité des interactions possibles entre les composantes ne permet plus au concepteur du système, ou à ceux qui l'exploitent, de comprendre, et d'imaginer l'ensemble des comportements possibles de ce système. Cette limite est renforcée par l'impossibilité des acteurs à regarder directement le processus de transformation industriel. Non seulement les opérateurs ne peuvent anticiper l'ensemble des comportements du système, mais ils ne peuvent suivre son état réel qu'à travers un prisme de mesures et d'indicateurs indirects. Selon l'auteur, la plupart des accidents industriels ne sont donc pas dus aux seules erreurs ou défaillances d'éléments du système, mais à la combinaison brutale et non anticipée d'échecs de ces 6 composantes du système. Ainsi à chaque fois que le système croît en complexité, la probabilité d'un accident industriel majeur augmente. L'auteur conclut alors que les systèmes industriels peuvent générer des accidents normaux :

« Si la complexité interactive et le couplage étroit – caractéristiques des systèmes – produisent inévitablement un accident, je crois qu'il est juste de parler d'accident normal ou d'accident de système. Le terme singulier, accident normal, veut signaler que, compte tenu des caractéristiques du système, des interactions d'échecs multiples et inattendus sont inévitables. C'est la traduction d'un trait inhérent des systèmes et non l'expression d'une fréquence. » Perrow (1984) p5.

Dans leur ouvrage, Rasmussen et Svedung (2000) abordent la complexité avec l'angle des évolutions sociétales. De profonds et globaux changements affectent la société actuelle. Les

conditions stables du passé ont fait place à une société dynamique. Cette tendance nouvelle affecte en profondeur les modes de gestion des risques industriels majeurs. Plusieurs déterminants caractérisent ces changements sociétaux :

- **Accélération des changements technologiques :** des changements technologiques ont lieu dans tous les domaines industriels, tels que les process industriels, les transports ferroviaires, maritimes... Si ces évolutions ont toujours existé, leur rythme s'est accéléré. La rapidité avec laquelle les nouveaux procédés techniques sont mis en œuvre ne permettent pas aux modes de gestion adaptés d'émerger. Une distorsion se créé entre ce que l'on est capable de faire, et ce que l'on est capable de gérer. De cette faille grandissante s'élèvent de nouvelles problématiques de gestion des risques (nanotechnologie, biotechnologie...), dont le principe de précaution est un aboutissement.

- **Augmentation des capacités industrielles :** les capacités de production des organismes industriels augmentent continuellement, avec un potentiel de risques d'accident majeur correspondant. La gravité des conséquences augmente, mais la probabilité d'un accident diminue, permettant l'acceptation de la société pour un risque « calculé ». En conséquence, les modèles d'analyse ne doivent plus seulement se baser sur une performance normale, ou moyenne, mais également prendre en compte des scénarios extrêmement rares, mais catastrophiques.

- **Haut degré d'intégration :** les développements rapides des systèmes de transport, d'énergies, et d'informations, associés à des exigences de production « en flux tendu » ont conduit à un haut niveau d'intégration et de couplage des systèmes entre eux. Dans ce contexte, une seule décision peut se propager rapidement et largement, et avoir des conséquences dramatiques sur la société dans son ensemble. Cette interdépendance forte n'est pas sans rappeler le fonctionnement du système financier mondial, ou encore des réseaux internet. En conséquence, il devient de plus en plus difficile de construire des modèles capables d'appréhender cette complexité.

- **Un environnement économique compétitif et agressif :** la compétition accrue polarise les décideurs sur des critères financiers à court terme, plutôt que sur des critères de long terme qui concernent la sécurité, ou encore les impacts environnementaux.

Ces tendances ont un effet important sur la manière d'aborder la question de la gestion des risques. La modélisation des systèmes basée sur une décomposition structurelle est alors challengée par l'abstraction fonctionnelle, et la coopération multidisciplinaire (Rasmussen et Svedung, 2000). Les auteurs proposent alors une modélisation du système socio-technique complexe (Figure 7). La gestion des risques est assurée par une organisation sociale composée de nombreux niveaux décisionnels hiérarchisés. La maitrise des risques dépend alors de la qualité de la coordination entre ces niveaux, issus de disciplines scientifiques multiples.

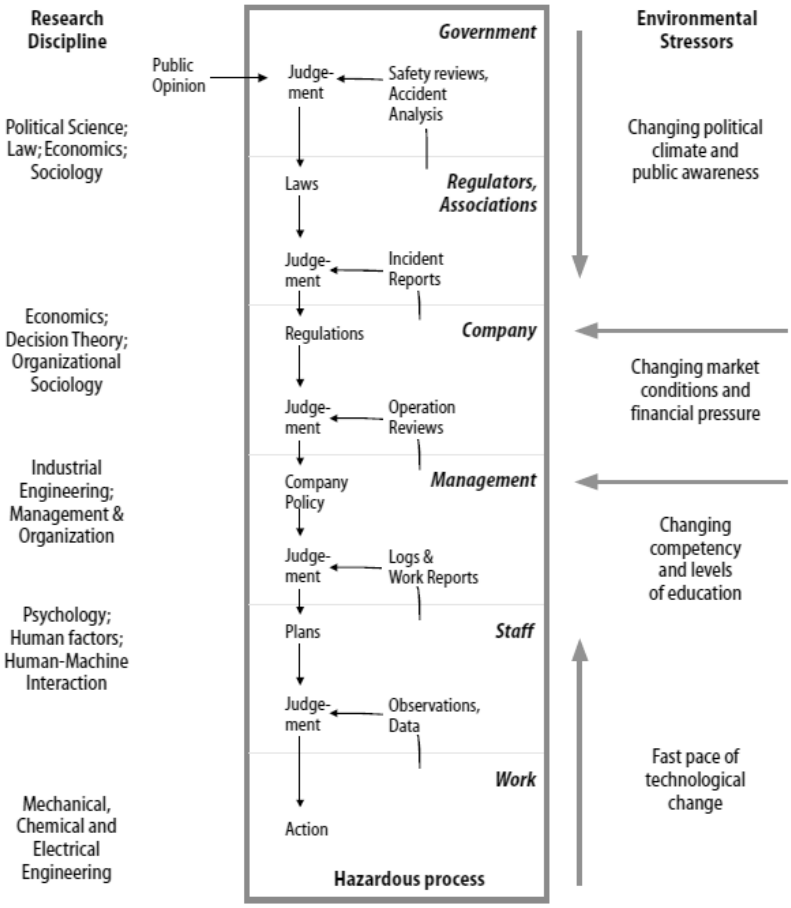


Figure 7 : Modélisation d'un système sociotechnique complexe, tiré de Rasmussen et al. (2000)

A travers cette représentation, les auteurs définissent plusieurs niveaux décisionnels impliqués dans la gestion des risques, et la réglementation des activités à risques. Cette vision prend en charge un rôle important des multiples acteurs, et de l'environnement.

Enfin, selon Journé et al. (2012), un certain nombre de principes communs permettent de saisir la complexité. Sans les aborder, nous pouvons citer le principe hologrammatique, le principe de récursivité, et le rôle du temps et du contexte. Ces principes doivent permettre d'affronter la complexité, s'ils s'appuient sur une pensée dialogique, c'est-à-dire la capacité à faire dialoguer les contraires, et prendre en compte les jeux ago-antagonistes (délibéré / émergent, identité / altérité, hiérarchie / réseaux, formel/informel...). Ainsi, la pensée complexe peut se caractériser par quatre points principaux :

1. La complexité est liée à une surcharge informationnelle, à une difficulté à identifier l'ensemble des scénarios possibles, de nombreuses situations ambiguës, équivoques, mal structurées, et à la difficulté de décider entre plusieurs options possibles.

2. La complexité est marquée par la multiplicité grandissante des parties prenantes, et l'urgence temporelle.

3. La complexité doit être abordée par les pratiques quotidiennes des acteurs, c'est-à-dire les activités ordinaires des managers, autant que des managés.

4. La complexité est marquée par la difficulté pour l'action managériale, une fois saisie dans les dynamiques organisationnelles, de rester dans les cadres de son intention initiale. La volonté de contrôle, de rationalisation, de normalisation des comportements, appliquée aux systèmes complexes, renforce paradoxalement leur ingouvernabilité, en occultant les tensions, désordres, et interactions nécessaires à leur fonctionnement (Thiétart, 2000).

Ces trois définitions de la complexité, selon Perrow (1984), Rasmussen et Svedung (2000), et Journé et al. (2012), la complexité d'un système tient au moins à trois séries de facteurs :

- **Les facteurs liés à l'anatomie du système :** sa composition, aux nombres et aux caractéristiques de ses composants, et les liaisons, formalisées et non formalisées, qui existent entre les composants. Les systèmes complexes sont généralement constitués d'un grand nombre de composants. Ils sont souvent de plusieurs types et possèdent une structure interne qui ne peut être négligée. Les éléments sont reliés par des interactions non linéaires, et de natures variées.

- **Les facteurs liés à l'environnement du système :** ce sont les aléas et les incertitudes propres à son environnement. Le système est soumis à des influences extérieures, différentes échelles. Le système modifie son environnement, qui en retour va le contraindre et modifier ses états ou comportements possibles. L'environnement peut donc avoir un effet positif ou négatif sur le système, c'est-à-dire stabilisateur, ou encore déstabilisateur.

- **Les facteurs liés au comportement du système :** et l'existence de rapports ambigus entre les liens de causalité déterministes, et le hasard apparent des évènements qui surviennent. Le comportement d'un système complexe fait état d'une causalité circulaire. Il existe des rétroactions des comportements collectifs et des propriétés émergentes sur le comportement des éléments composants le système.

L'analyse des accidents nous a montré toutes les facettes de la complexité et l'évolution des situations décisionnelles rencontrées par le manager. La première facette est celle de la coordination des acteurs. Les organisations humaines composées d'acteurs multiples en interaction, dont les conséquences sont rarement directes et instantanées. Ces acteurs ont des agendas, des comportements, des valeurs, et des cadres de références diversifiés. Ils poursuivent des buts différents, parfois contradictoires. Chaque acteur ne possède que des informations partielles sur les moyens de parvenir à un résultat d'intérêt commun. Il existe des effets pervers de coordination, où les résultats réels de l'action sont contraires aux finalités attendus.

La deuxième facette est liée à la compréhension du système. Il existe une multitude de règles de fonctionnement dans le système (procédures, ordres…). De nombreux outils permettent d'avoir un regard sur le système, et de l'évaluer (documents réglementaires, analyse des risques, outils comptables, indicateurs de production, indicateurs RH…). Ils alimentent une représentation symbolique du système. Cependant, ils dépassent les capacités cognitives des acteurs. Personne n'a les moyens et les ressources nécessaires pour appréhender l'ensemble de ces documents. Ces limites sont renforcées dans les situations d'urgence, où le temps est limité et les conditions stressantes. Chacun construit ses propres documents de suivis, plus efficaces, mais moins standardisés.

La troisième facette est liée aux actions tacites dans le système. A l'organisation formelle s'ajoute une organisation informelle en parallèle, masquée. Les acteurs mettent en œuvre un

certain nombre de compétences qui ne sont pas fournies par l'organisation. Ils ne sont pas formalisables et explicitables à travers des documents, ou encore des outils.

Ces différentes facettes de la complexité de gestion sont des facteurs de stabilité et d'instabilité du système. Ils sont liés à l'existence de boucles de rétroaction, comme par exemple le retour attendu après la mise en œuvre d'une décision ; à l'interdépendance du système avec son environnement, tel que le lien commercial ; aux incertitudes associées aux prises de décision, et aux phénomènes émergents dans l'entreprise : nouveau leadership, nouveaux comportements, nouveaux risques. Certains facteurs poussent le système vers l'instabilité et le désordre, tel que l'innovation, les initiatives individuelles, les expérimentations… D'autres facteurs cherchent à ramener le système vers un état d'équilibre : la planification, le contrôle, la structure… Ces facteurs d'équilibre de l'organisation génèrent une fluctuation continue du niveau de risque. Le risque ici est un risque de perte de maitrise, et donc d'inefficacité, des actions de gestion. Et ce risque gestionnaire se répercute sur le process industriel, en termes de risque opérationnel. C'est par exemple le cas de la non réalisation du processus de formation, qui contribue à un comportement inadéquat de l'opérateur. Ces difficultés à décrire et expliquer le fonctionnement quotidien de la gestion a été mis en avant lors d'accidents technologiques récents, tels que la perte de la navette Columbia, l'explosion de la raffinerie de Texas City, et l'accident nucléaire de Fukushima.

Fort de notre analyse, et des définitions précédentes, le défi de la complexité se décline selon deux problématiques :

1. **L'inventaire de l'ensemble des interactions qui caractérisent un système :** le caractère socio-technique des systèmes industriels ne permet pas de connaitre la qualité et l'intégralité des interactions existantes.
2. **L'identification des propriétés émergentes :** les modèles de sécurisation classique n'intègrent pas les phénomènes systémiques présents dans la dynamique accidentelle.

III.2 Le défi de l'érosion du temps

Notre étude a montré que l'accident industriel majeur nécessitait l'accumulation de défaillance à tous les niveaux du système. Si cette détérioration générale est nécessaire, la présence de symptômes transverses comme la migration des pratiques, et la dérive globale montre l'importance de la dimension temporelle dans cette accumulation. Pourtant, la sécurité des systèmes industriels à risques est majoritairement construite sur le principe de défense en profondeur. Plusieurs couches de barrières de sécurité viennent s'interposer à la dynamique accidentelle. Ce sont des garde-fous qui assurent un retour à un état stable lors d'une perte de maitrise du processus de production. L'émergence de l'état accidentogène du système est le résultat d'une évolution, une érosion du temps.

Des facteurs d'érosion du temps

L'étude de plusieurs accidents passés a permis d'identifier plusieurs facteurs d'érosion.

Le premier facteur est lié à la durée de vie des installations. Un système industriel est généralement conçu pour un fonctionnement sur un temps long, c'est-à-dire plusieurs dizaines d'années. Or l'utilisation répétée de composants techniques impose une fatigue structurelle. Les infrastructures vieillissent, certains composants s'érodent, et leur obsolescence les rend difficile à maintenir à long terme.

Un deuxième facteur d'érosion concerne l'adaptation des pratiques par les opérateurs de production. En effet, dans un espace de liberté d'action défini, l'opérateur a tendance à adapter la manière de réaliser ses tâches, vers un mode de réalisation maximisant le confort et l'efficacité de production. Sous la pression des résultats, des ajustements quotidiens assurent le niveau de productivité requis. Face à ces tendances, les conditions réelles de fonctionnement ne sont plus celles qui ont été prises en compte lors de l'analyse des risques initiale. Sans incidents graves, le système peut être perçu comme aussi sûr que lors de son fonctionnement nominal initial, et la sécurité devient routinière.

Cette tendance est renforcée par la répétition d'écarts consentis aux procédures, et sans conséquences apparentes. C'est par exemple le cas du court-circuitage d'un dispositif de sécurité. De plus en plus de procédures sont durablement enfreintes, sans que cela fasse débat. Des situations où l'on aurait autrefois arrêté la production sont tolérées. L'écart s'est

creusé entre les messages managériaux descendants et la réalité de ce que vivent les personnels d'exploitation.

Un troisième facteur est celui des changements de finalité. Lors de la vie du système, les conditions d'exploitation sont parfois amenées à changer. Par exemple, de nouveaux produits sont demandés par les clients. Les exigences de productivité augmentent, et les objectifs à court terme se trouvent parfois localement contradictoires avec les exigences de sécurité à long terme. Les organisations sont modifiées en conséquence. Des couches supplémentaires de procédures sont ajoutées à celles définies initialement. Le formalisme lié à la qualité ou à la sécurité est accru, réduisant d'autant les marges temporelles de réalisation effective des opérations de production ou de maintenance.

Une gestion soumise à des ruptures

Enfin, l'érosion est le résultat de l'immédiateté du temps présent, sans continuité ou transmission de la mémoire. La gestion d'une entreprise industrielle est soumise à de nombreuses ruptures. Celles-ci sont de plusieurs natures différentes, et concernent des fonctions critiques du système de gestion :

- **Ruptures de connaissance du système :** celles-ci sont particulièrement présentes à deux types de moment de la vie du système. La première rupture concerne le changement d'équipe de travail. La continuité d'activité impose une rotation des opérateurs sans l'arrêt des activités. La transmission des informations, par l'intermédiaire de briefing, ou encore de carnet de bord, est critique pour la sécurité opérationnelle du process. La seconde rupture de connaissance a lieu lors du turn-over du personnel. Un opérateur, ou un manager, quittant l'entreprise, emporte avec lui la connaissance précise du fonctionnement du système, des ajustements réalisées, et de leurs justifications. La gestion des passations de poste est donc importante pour garder cette connaissance dans le système, et permettre de développer une culture sécurité à long terme.

- **Rupture dans les activités du système :** la mise en œuvre d'un processus de production comporte de nombreuses phases d'activités aux objectifs différents. Parmi elles, les phases d'arrêt pour maintenance, contrôle, ou encore de démarrage sont critiques. En effet, elles ne correspondent pas à un mode de fonctionnement

stabilisé et nominal du process. Ces étapes associent généralement des risques accrus, une moins bonne maitrise des opérations, du fait de leur plus rare fréquence, et le recours à du personnel supplémentaire, peu habitué aux installations. La maitrise des phases transitoires est donc un levier de sécurité important à prendre en compte.

- **Ruptures liées à l'environnement du système :** elles sont issues de l'environnement direct, et génèrent une remise en cause de l'existence du système. Elles peuvent être d'origine médiatique. L'incident de l'usine Lubrizol est un exemple où la crise médiatique dépasse largement la crise opérationnelle. Elles peuvent également être d'origine économique, ou commerciale, comme ce fut par exemple le cas à Bhopal, en 1984.

Tous ces facteurs modifient le niveau global de risques. Au sein d'un système sociotechnique complexe, le défi de l'érosion du temps peut alors être décrit comme la problématique de prise en compte des effets cumulés d'évènements a priori indépendants, mais pouvant, par effet cumulatif, générer des conséquences importantes. Celles-ci peuvent être l'élévation du niveau de risque, jusqu'à la réalisation de conditions fortement accidentogènes.

III.3 Le défi de la décision

Au sein d'un système caractérisé de sociotechnique et de complexe, l'espace décisionnel du manager se trouve imbriqué à l'interface de plusieurs strates de l'organisation. Il peut être schématisé par la Figure 8.

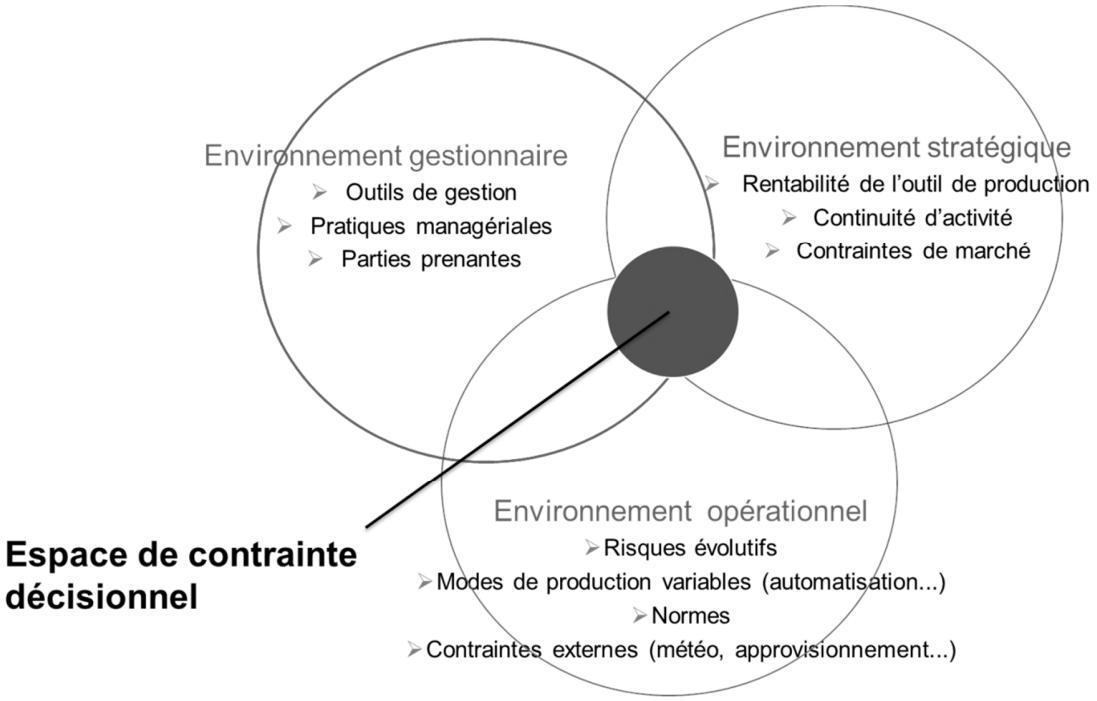


Figure 8 : Identification de l'espace de contrainte décisionnel du manager opérationnel

L'espace décisionnel du manager se situe à l'interface de trois environnements distincts. Il peut être qualifié de très contraignant :

1. **Un environnement opérationnel :** constitué de l'ensemble des matériels, équipements et infrastructures liés aux processus de production, de l'organisation et des rythmes de travail, des modes de production, des normes techniques liés au produit et au process, des sous-traitants, et de contraintes externes.

2. **Un environnement stratégique :** constitué d'activités stratégiques, de schémas directeurs, d'objectifs de rentabilité, de contraintes économiques, de lois du marché, et continuité d'activité.

3. **Un environnement gestionnaire :** constitué d'outils de gestion, de systèmes d'information, de pratiques managériales, de compromis entre demande et capacité de réalisation, et de parties prenantes.

Si l'ensemble de la production est réfléchie globalement et s'articule autour de processus généralement clairs, chacun de ces facteurs est potentiellement déstabilisateur, voire bloquant. C'est par exemple le cas lors d'un changement d'équipe mal réalisé, de restrictions budgétaires, ou encore d'atteinte médiatique liée à l'image de l'entreprise. En effets, plusieurs caractéristiques définissent la complexité de l'écosystème décisionnel du manager :

- **Un environnement mouvant et incertain :** le caractère non isolé des organisations à risques oblige le décideur à prendre en compte les évolutions de son environnement, et ses effets sur l'organisation. C'est par exemple le cas des normes, des contraintes de marché, de l'opinion publique…
- **La présence d'enjeux internes :** les moyens de gestion limités, et la présence de sous-groupes aux objectifs opposables peut générer des décisions qui correspondent non pas à la meilleure option possible, mais à un choix de compromis, en partie déconnecté du problème initial.
- **Une complexité liée à la nature même des organisations :** les interactions entre systèmes techniques et systèmes sociaux de l'organisation font émerger des comportements inattendus, et non anticipables.
- **Une abondance d'informations :** la superposition des systèmes de reporting apportent au décideur une grande quantité d'information, nécessaire à la compréhension de la situation. Cependant, ce flux d'information peut avoir deux limites. Le découplage entre logique d'information et processus décisionnel peut augmenter l'incertitude des options étudiées. De plus, la quantité d'information disponible dépasse les capacités d'analyse du décideur.

De tels contextes placent le décideur dans un carcan qui mêle équivocité de la situation, contraintes de l'action, incertitude des conséquences, et responsabilité des effets. Dans le cas des systèmes à risques, des décisions erronées peuvent s'ajouter à d'autres facteurs accidentogènes, et conduire à des catastrophes industrielles majeures. Dans la plupart des situations décisionnelles, le manager identifie avec succès l'option la plus adéquate face au

problème rencontré. Cependant, il existe au moins deux cas pour lesquels le manager doit être soutenu par une aide à la décision.

Cas n°1 : situations pour lesquelles aucune option ne se dégage naturellement de la construction du problème. Dans cette situation, le manager a besoin d'une démarche structurée, objectivée et consolidée qui lui permette d'aboutir à une voie d'action satisfaisante. C'est par exemple le cas lors du constat d'évènements inquiétants, mais inexplicables, par l'intermédiaire de signaux faibles. Le manager est alors en recherche d'une méthode d'enquête, qui permette une meilleure compréhension de la situation, c'est-à-dire suffisante à déclencher l'action.

Cas n°2 : situations pour lesquelles le manager doit justifier un point de vue, ou défendre une prise de position. Il a alors besoin de construire une argumentation convaincante, qui ne repose pas sur des considérations intuitives. Par exemple, l'arrêt d'un réacteur chimique, peut engendrer des pertes importantes. Cette décision doit alors être justifiée, pour une hiérarchie qui met en balance d'autres considérations (production, finance, délais de remise en route).

Dans un contexte où les processus sont dynamiques et l'information continue, face à des conflits de gestion entre sécurité et production, et devant le dilemme de l'action, le manager est à l'image d'un pilote d'avion. Celui-ci a besoin de stratégies globales guidant ses décisions. Les outils de gestion restent nécessaires et importants, mais leur utilisation hors de cadres définis peut contribuer à les rendre inefficace.

Ainsi, le défi de l'initiative de la décision se décline selon deux problématiques :

1. **Conforter le décideur dans ses choix :** il s'agit de lui permettre de construire une représentation actualisée de la situation, et l'aider à résoudre les dilemmes auxquels il fait face dans son activité de management.

2. **Construire une argumentation solide et convaincante hors de la hiérarchie :** il s'agit de faire reposer la décision sur une réflexion structurée et objective. Celle-ci n'est plus seulement à l'initiative du manager, elle est également le résultat d'un processus logique d'analyse.

Focalisation sur le manager opérationnel

Dans ce cadre, le choix que nous avons adopté pour le positionnement du cadre organisationnel est le suivant (Figure 9) :

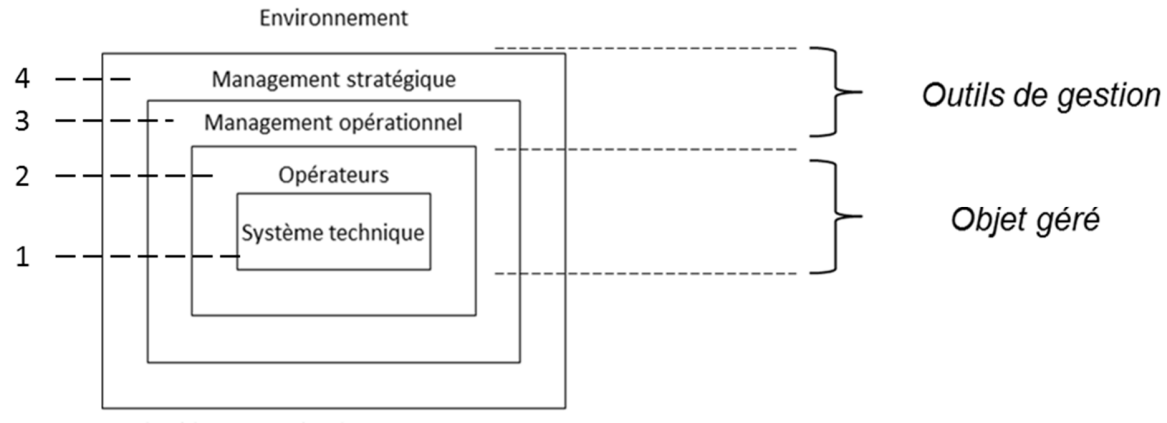


Figure 9 : Les multiples niveaux hiérarchiques d'un système industriel

Chaque niveau peut être décrit de la manière suivante :

1. A la base du modèle, est représenté le processus technique : il s'agit de composants, logiciels, flux de matières, d'énergie.... Les problématiques associées à ce niveau concernent essentiellement la sureté de fonctionnement du process.
2. Le niveau suivant est relatif aux opérateurs : il s'agit de l'ensemble des individus qui interagissent avec le process technique. Ils le contrôlent, le supervisent, et en assurent la maintenance. Les problématiques associées à ce niveau concernent essentiellement l'ergonomie des situations de travail. Les questionnements du niveau « processus technique » et « opérateurs » sont similaires, et portent sur la performance opérationnelle : « comment fait-on pour réaliser telle tâche ? ».
3. Le niveau suivant est celui du management opérationnel : il constitue le focus central de ce travail. A ce niveau sont conçues et coordonnées les règles de gestion relatives à la mise en œuvre du couple processus technique / opérateur. Les problématiques associées au management opérationnel concernent l'adéquation entre des objectifs de production, des ressources, des contraintes réglementaires, mais aussi les possibilités et le comportement des niveaux opérationnels (capacité de production, compétence, comportement face au risque, climat social...). Le questionnement associé porte sur la création et la mise en œuvre de règles de gestion : « Comment fait-on faire ? ».
4. Le niveau suivant porte sur le management stratégique de l'entreprise. Il s'agit ici pour une équipe de direction généralement restreinte de prendre les décisions structurantes de l'activité de l'organisme. La stratégie de l'entreprise est définie, et les ressources allouées aux niveaux inférieurs. Les problématiques de ce niveau portent sur la compréhension de l'environnement du système, son positionnement stratégique. Le questionnement associé porte sur l'objet de l'outil industriel mis en œuvre : « Pourquoi fait-on faire ? ».

La place du manager opérationnel au sein de systèmes sociotechniques complexes est alors intéressante au regard de trois paramètres :

1. **Son environnement informationnel :** Sa position centrale, la place dans un écosystème décisionnel d'abondance et de diversité des informations.

2. **Ses outils de contrôle :** il a à sa disposition les outils de gestion permettant le traitement des informations et la représentation de l'état du système pour l'aide à la décision (par exemple le système de gestion de la sécurité).

3. **Sa latitude décisionnelle :** Depuis les développements de Mintzberg (1984), la fonction de manager est mieux définie. Parmi les dix rôles du cadre définis par Mintzberg, il est ceux de concevoir les règles de gestion, et d'assurer un rôle décisionnel au sein de l'entité qu'il anime.

Dans ce cadre organisationnel contraint et structuré, le manager opérationnel doit remplir son rôle. À l'interface entre considérations stratégiques et réalisation opérationnelle, son rôle est primordial dans l'anticipation des accidents industriels majeurs.

Conclusion de la Première Partie

Les limites de l'étude de cas

Afin de garantir des résultats fiables et valides, des stratégies, décrites dans l'étape 2, ont été définies et mises en œuvre. Pourtant, après s'être attelé à une analyse approfondie, et obtenu des résultats intéressants, le choix de l'objet d'étude « accident industriel » peut être remis en question. Celui-ci est porté par la question de recherche : « Quelles sont les faiblesses dans la gestion des risques industriels ? ». Si ce choix permet de répondre à la problématique posée, un autre choix aurait également été pertinent au regard du résultat recherché : l'anticipation des accidents industriels majeurs. Ce second objet d'étude porterait sur des organisations industrielles à risques placés dans une dynamique accidentelle, mais qui ont tenu. Il aurait permis d'identifier non pas les facteurs d'échecs seulement, mais également les facteurs de succès. Choisir « l'industrie qui a tenu » comme objet n'a pas été possible, pour plusieurs raisons. Tout d'abord, il existe assez peu de retours d'expérience disponibles. De plus, il est difficile de faire la part des choses entre les facteurs qui ont été contributifs au succès, et les éléments aléatoires du système. Et enfin, ce type de question demande une analyse très détaillées des cas, et donc beaucoup de temps et de ressources, incompatibles avec ce travail doctoral.

Les défis du manager opérationnel

L'industrie à hauts-risques est un système complexe. Et son évolution créée de nouvelles vulnérabilités que les approches disciplinaires et techniques n'arrivent pas à fixer. Les facteurs de déstabilisation sont nombreux. Citons les leviers exogènes : ruptures technologiques, mondialisation de la compétitivité, contraintes normatives, nouveaux traitements médiatiques... et les leviers endogènes : pression budgétaire, nouvelles méthodes de management, érosion des équipements et infrastructures... Le risque industriel est devenu organisationnel. Dynamique, erratique et diffus, il nécessite une approche différente, qui replace l'Homme au cœur du système.

Cette première partie permet de préciser la problématique rencontrée par le manager opérationnel. Premièrement, la sécurité est un processus actif, conduite par le manager

opérationnel. Il a la charge de son efficacité. Deuxièmement, l'accident industriel revêt un caractère nouveau, qui dépasse les voies de sécurisation classique. Des faiblesses rémanentes dans la gestion opérationnelles des systèmes ont été identifiées : la dimension systémique de l'accident, la dérive des pratiques de l'entreprise, et la prise en compte des périodes de résistance. Pour déclencher la décision d'anticipation, le manager doit faire face à trois défis :

- *La complexité :* c'est le défi de la compréhension du système, de ses mécanismes, de son fonctionnement, et de son évolution.
- *L'érosion du temps :* c'est le défi de l'instantanéité du monde actuel. Il s'agit de réinscrire la gestion dans la durée de long terme de la vie d'un système industriel.
- *La décision :* rassembler les conditions d'émergence de la phase de décision, afin de passer du choix imposé par l'environnement, au défi de la prise de risque d'initiative.

Dans ce cadre, la problématique de recherche est celle de l'anticipation des accidents industriels majeurs. Elle est la suivante :

- ***Quelle aide à la décision pour le manager opérationnel, au sein de systèmes sociotechniques complexes ?***

A l'opposé de toute querelle d'existence disciplinaire, et dans un clair but d'anticipation, il s'agit d'échanger entre des horizons opérationnels et conceptuels différents et multiples, en évitant les syndromes de capharnaüm et « d'usine à gaz », pour, si possible, décider à temps.

Résumé de la Première Partie

Depuis une cinquantaine d'années, les modèles de maitrise des risques (sureté de fonctionnement, facteurs humains et organisationnels...) sont associées à des pratiques éthiques, normatives, et politiques. Ils ont permis d'élever très significativement le niveau de sécurité des organisations industrielles à risques. Pourtant, des accidents industriels récents, tel que le naufrage de la plateforme Deepwater Horizon, ou encore l'explosion de Lac Mégantic, remettent en cause ce plan de maitrise des risques. Au cours de cette première partie, nous nous intéressons au rôle du management opérationnel dans l'anticipation des accidents industriels majeurs. Pour répondre à cette problématique, nous analyserons les accidents industriels majeurs passés. Sur une période de 300 ans, cette étude des accidents les plus marquants nous a permis de préciser selon trois aspects différents la problématique rencontrée par le manager opérationnel :

1. La sécurité est un processus actif, dont le manager opérationnel est le pilote. Il est en charge de son efficacité, et doit également être capable de déclencher des situations d'initiative lorsque c'est nécessaire.
2. L'accident industriel revêt un caractère nouveau, qui dépasse les voies de sécurisation classique. Des faiblesses rémanentes dans la gestion opérationnelles des systèmes ont été identifiées : la dimension systémique de l'accident, la dérive des pratiques de l'entreprise, et la prise en compte des périodes de résistance.
3. Pour passer de la réaction à la décision d'anticipation, le manager doit faire face à trois défis :
   - *La complexité :* c'est le défi de la compréhension du système, de ses mécanismes, de son fonctionnement, et de son évolution.
   - *L'érosion du temps :* c'est le défi de l'instantanéité du monde actuel. Il s'agit de réinscrire la gestion dans la durée de long terme de la vie d'un système industriel.
   - *La décision :* Défi par la nature même de l'initiative. Il s'agit de rassembler les conditions d'émergence de la phase de décision, afin de passer du choix imposé par l'environnement, à la prise de risque d'initiative.

On comprend alors le rôle du manager opérationnel dans l'anticipation des accidents industriels majeurs. Sa position d'initiative, à l'interface entre considérations stratégiques et réalisation opérationnelle, sa place dans un écosystème décisionnel ou l'abondance et la diversité des informations qui lui parviennent nécessitent des outils d'aide à la gestion. Ainsi, c'est dans la sphère managériale que se trouvent un des leviers de progrès important en matière de gestion des risques industriels.

Deuxième Partie

De l’accident industriel à la rupture managériale

Sous-table des matières #2

Sous-table des matières #2 89

Introduction de la Deuxième Partie 91

I – Principales contributions à l'explication de la dynamique accidentelle 93

I.1 La construction de la sécurité industrielle au XX^{ème} siècle.....93

I.2 Positionnement scientifique des principaux courants théoriques.....108

II – Analyse des principaux modèles de production de sécurité 113

II.1 Présentation des principaux modèles théoriques existants.....113

II.2 Analyse des modèles théoriques retenus.....170

III – Nécessité d'un nouveau regard sur l'accident industriel 190

Conclusion de la Deuxième Partie 197

Résumé de la Deuxième Partie 199

Introduction de la Deuxième Partie

L'analyse de plusieurs accidents industriels majeurs nous a permis de souligner toute l'importance prise par les phases séquentielles des évènements. Dans la plupart des accidents industriels majeurs, la catastrophe aurait pu être évitée. Le phénomène est certes difficile à décrypter.

La sécurité est un processus actif du système. Son maintien nécessite la mise en œuvre de stratégies, et de moyens, pour garantir la rentabilité et la pérennité de l'entreprise. Au cœur du système, le manager opérationnel a la charge du pilotage des activités, dans des cadres prévus de productivité et de sécurité.

Cependant, l'analyse de multiples accidents industriels passés a mis en lumière des pistes d'amélioration de la gestion opérationnelles des systèmes. Dimension systémique de l'accident, dérive des pratiques de gestion, et périodes de résistance sont autant de phénomènes qui affectent la maitrise des activités.

De ces constats, nous posons la problématique suivante. Quelles sont les capacités des principaux modèles de production de sécurité, à prendre en compte, et répondre, aux trois défis identifiés pour le manager opérationnel ?

Pour pouvoir répondre, il faut tout d'abord procéder à une revue des principales contributions scientifiques à l'explication du phénomène accidentel. Cette première partie sera suivie d'une analyse comparative des principaux modèles retenus aux trois défis du manager opérationnel. Enfin, cette deuxième sous-partie nous permettra de préciser les besoins en aide à la décision du manager opérationnel.

I – Principales contributions à l'explication de la dynamique accidentelle

L'objectif de cette sous-partie est de décrire le développement de la construction de la sécurité industrielle au XXème siècle. Celle-ci nous permettra ensuite de réaliser un positionnement scientifique des courants théoriques, dans le but d'identifier les principaux modèles de production de sécurité.

I.1 La construction de la sécurité industrielle au XX^{ème} siècle

La sécurité industrielle s'inscrit initialement dans une longue tradition technique. Les sciences de l'ingénieur développent de nouveaux concepts dans le but d'augmenter la fiabilité des composants et des assemblages. En parallèle, de nouveaux accidents technologiques bouleversent l'ordre établi, et interpellent une fois encore la question de la sécurité. Face à la difficulté à expliquer les causes de ces nouveaux évènements, des évolutions dans la manière de comprendre les accidents étaient nécessaires. De nouveaux champs scientifiques se structurent alors. La sureté de fonctionnement est complétée par l'étude de l'Homme au travail. La prise en compte des facteurs humains apparaitrait comme un facteur de fiabilité intéressant. Mais elle ne suffit pas. En effet, les modèles d'accidents permettent de constater la répétition d'erreurs. De plus, des accidents ont lieu, alors qu'aucune erreur flagrante ne semble s'être produite. A la suite de grandes catastrophes industrielles des années 80, l'accent est mis sur l'étude des facteurs organisationnels qui prennent une nouvelle dimension. Au-delà de la panne et de l'erreur, c'est dans l'organisation elle-même que les causes de l'accident sont recherchées. Enfin, dans les années 2000, avec la complexité des systèmes, une nouvelle dimension est prise en compte : résilience. Dans ce contexte, l'évolution par la continuité s'impose pour améliorer la gestion du risque. Ce discours rassurant prend le pas et la résilience ouvre une ère qui nous propose l'analyse de la contrainte sur les modèles mis en place. En conséquence, le système doit s'adapter à toutes les perturbations qui s'imposent à lui. Ces grandes tendances scientifiques du XXème siècle sont reprises dans le schéma suivant (Figure 10).

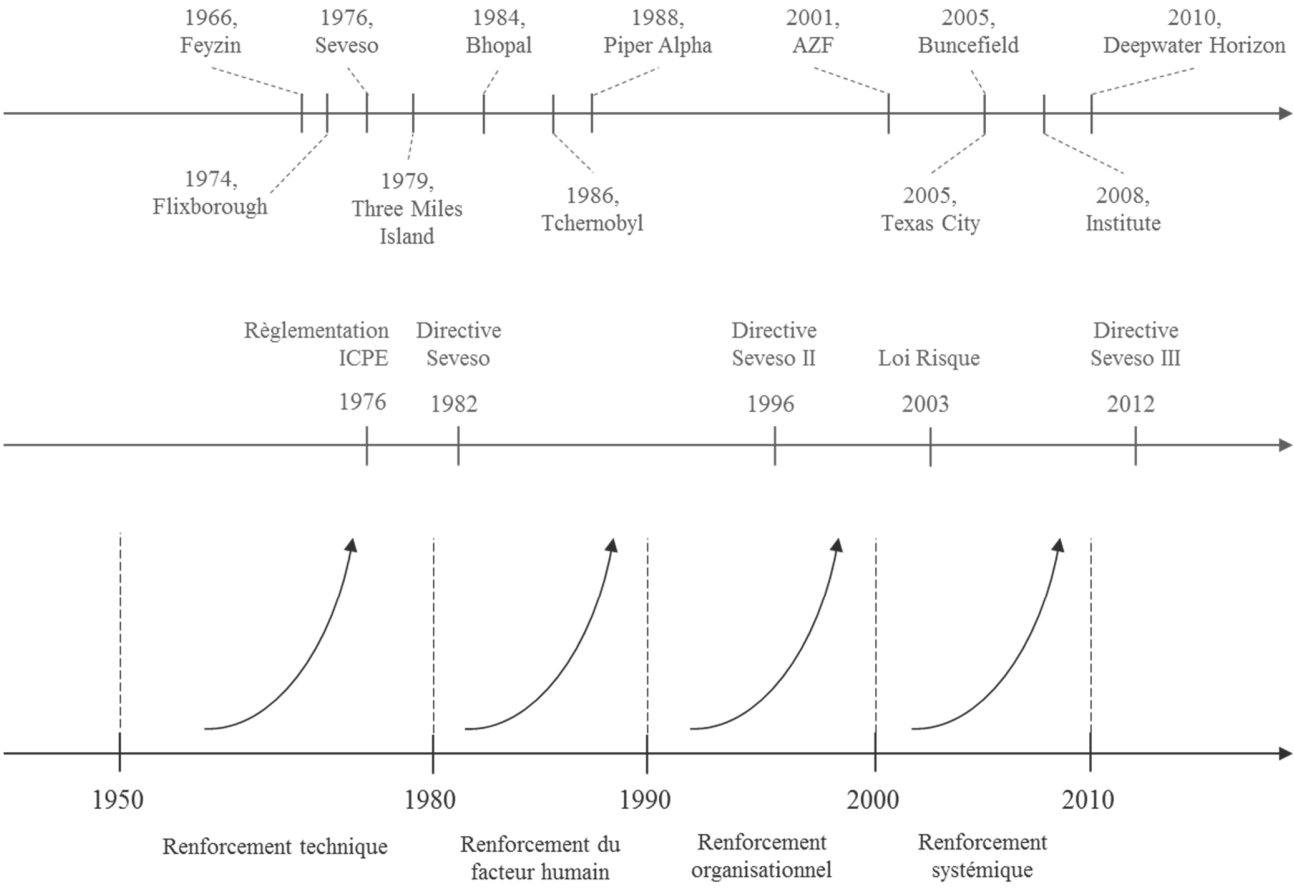


Figure 10 : Correspondance entre développements scientifiques, réglementaires, et les accidents industriels

Les quatre développements principaux, énoncés précédemment, sont décrits dans les paragraphes suivants.

Un développement technique

Jusqu'au début du XXème siècle, les méthodes de production s'inscrivent dans une culture artisanale. Les pièces sont fabriquées à la main. Le niveau de fiabilité de chaque produit dépend davantage des compétences et de l'habileté des artisans, que de la conjonction des fiabilités des diverses pièces. L'arrivée de l'ère industrielle modifie le rythme et les méthodes de production. Tout s'accélère ! Les besoins et les attentes de l'économie de consommation s'imposent peu à peu dans une classe ouvrière qui commence à consommer.

Dans ce processus, une nouvelle catégorie émerge, une classe intermédiaire. L'approche artisanale n'est pas suffisante pour alimenter et répondre, et les nouveaux secteurs industriels apparaissent pour produire dans la quantité et la qualité. L'automatisation s'intègre dans le processus du travail humain, et les pièces sont standardisées et fabriquées en masse. Quel meilleur exemple pour affirmer ce turn-over permanent que le cas des roulements à billes, nécessaire à l'expansion du chemin de fer. On retrouve ce processus lié au mouvement dans toutes les industries. Avec le mouvement permanent basé sur la quantité, la production de qualité unique s'affirme aussi comme une valeur commerciale. En effet, toutes les pièces sont à l'identique, et les éléments défectueux sont détectés au cours du processus de production, grâce à des tests de vérification. La fiabilité est garantie par l'application de procédures spécifiques de contrôle qualité. Le développement de l'électricité est aussi une source de progrès. La volonté de rendre plus fiable cette source d'énergie est à l'origine de nouvelles méthodes, telles que la mise en parallèle des transformateurs et lignes de transport, et l'interconnexion des lignes à haute tension. Des avancées importances sont dues à la mise en redondance et à l'amélioration des matériels.

L'arrivée du transport aérien fait apparaitre de nouveaux aspects de la fiabilité. Le recueil d'informations statistiques sur la fréquence des pannes de pièces d'avions, notamment sur les moteurs, permet la création de nouveaux modèles de fiabilité. Ces approches statistiques sont à l'origine des premières améliorations orientées et des premiers objectifs de sécurité à atteindre. Ainsi, *l'Aeronautical Research Council* de Londres demande que le taux d'accident d'un avion ne dépasse pas 10^{-5} par heure, dont 10^{-7} par heure pour les causes liées à la structure de l'avion (Villemeur, 1988).

Jusqu'aux années 1940, les approches qualitatives de la fiabilité et de la sécurité sont peu prises en compte par les concepteurs, et généralement de manière subjective. Elles se limitent à l'expérience acquise lors d'accidents précédents. Ce manque méthodologique a été identifié dans un nombre de catastrophes industrielles du XXème siècle. Le plus bel exemple est certainement le naufrage du Titanic. Ce fleuron technique de l'époque est équipé d'un système de cloisonnement automatique qui divise la coque en compartiments. Cependant, les cloisons ne sont pas assez hautes pour fermer hermétiquement chaque compartiment. Les concepteurs pensaient que l'équipage aurait le temps d'intervenir avant que l'eau ne se déverse dans le compartiment voisin. Cet excès de confiance s'est également manifesté lors de la décision de se diriger à pleines vapeurs vers une zone connue pour sa dangerosité à cette période de l'année. Après avec percuté un iceberg, le

navire sombre très rapidement, entrainant la mort de 1500 personnes (British Government Report, 1912).

Les années 40 et la seconde guerre mondiale sont à l'origine de nouvelles interrogations sur la fiabilité des systèmes. L'idée générale de la fiabilité introduite par Midgley et Pierce (1926) ne permet pas d'expliquer les nombreux échecs rencontrés lors de la fabrication des missiles. Selon les auteurs, un système technique est considéré comme une chaine. La fiabilité d'un système est égale à celle de son maillon le moins fiable. Dans cette optique, les ingénieurs cherchent à renforcer les pièces qu'ils pensent être les plus critiques. Cependant, les tests montrent que certains composants sont parfois fiables, parfois défaillants. L'idée du maillon faible de la chaine est alors remise en cause. La fiabilité d'un système n'est pas celle de son maillon le plus faible, mais est liée aux fiabilités de l'ensemble des composants. Les ingénieurs cherchent alors à prévoir et mesurer la fiabilité du système, dès sa conception.

Les années 50 connaissent de nouvelles exigences. La complexification des composants, et l'arrivée de l'électronique, introduisent des dimensions et des paramètres de plus en plus variables. Le manque de fiabilité des équipements militaires entrainent des disponibilités grandement réduites et une augmentation des coûts de maintenance. Devant le besoin d'une véritable ingénierie de la fiabilité, le *Department of Defense* américain fonde l'*Advisory Group on Reliability of electronic Equipment AGREE,* avec pour but d'intégrer la fiabilité dès les processus de conception des composants. Les premières techniques de conception de composants à haute fiabilité sont apparues. Elles sont reprises ensuite par la NASA. Les domaines de l'aéronautique et du nucléaire américains accordent également une importance croissante aux problèmes de sécurité.

C'est également à cette époque que sont entrepris les premiers efforts pour comprendre les erreurs humaines qui contribuent aux défaillances des systèmes, et des moyens pour s'en prémunir.

Avec l'arrivée de la micro-informatique, de nouvelles ressources sont alors disponibles. Les temps et coûts nécessaires au recueil et au traitement des données d'incident sont divisés par dix. Les options de tri permettent le classement en mode de défaillances, ce qui permet une meilleure évaluation de la fiabilité que les taux génériques. Les premières bases de données sur les taux de défaillance sont créées dans les années 60. On peut citer les bases de l'*United Kingdom Atomic Energy Authority UKAEA, Royal Radar Establishment RRE, Rome Air Development Corporation.*

Face à la complexité des systèmes mis en œuvre, de nouvelles techniques de fiabilité et méthodes d'application viennent compléter celles existantes. La méthode d'analyse des modes de défaillances, et de leurs effets, AMDE, a été inventée en 1949 par l'armée américaine (Villemeur, 1988). *Bell Telephone Laboratories* conçoit en 1961 la méthode de l'arbre de défauts, pour évaluer la sécurité du système de contrôle de lancement du missile *Minuteman*. *Boeing* développe également la méthode de construction de l'arbre des causes. La *Société Nationale des Industries Aéronautiques et Spatiales SNIAS* introduit la méthode des combinaisons de pannes pour ses projets Concorde et Airbus.

Le recours aux méthodes d'analyse prévisionnelle de la fiabilité et de la sécurité se généralise dans l'industrie aéronautique. Les différentes normes sorties aux Etats-Unis, en Angleterre, et en France sont harmonisées grâce aux travaux de la *Commission Electrotechnique Internationale CEI*.

Vers 1965, la caractéristique de « maintenabilité[6] » du système est introduite. Les matériels, notamment électroniques, deviennent de plus nombreux et complexes. Les ingénieurs s'intéressent à réduire les coûts engendrés par les dépenses annuelles de maintenance, ainsi que ceux engendrés par l'indisponibilité de ces matériels lorsqu'ils ne sont plus en mesure d'assurer les services attendus (Guyot, 1969).

Au début des années 70, Rasmussen, de *l'US Nuclear Regulatory Commission*, réalise la première caractérisation du risque nucléaire par l'évaluation complète du risque lié à une installation nucléaire américaine. Le but était d'apprécier le risque que faisait courir l'industrie nucléaire à la population, dans un contexte de montée des mouvements écologiques aux Etat-Unis (Villemeur, 1988). Le risque était caractérisé par la probabilité annuelle de décès d'une personne des populations environnantes à la suite d'un accident conduisant à la dispersion de produits radioactifs.

De fortes inquiétudes relatives au manque de contrôle réglementaire officiel sur les activités susceptibles de provoquer des accidents aux conséquences grave pour la sécurité publique, se font jour dans le milieu des années 70. Les accidents de Flixborough en 1974, et de Seveso en 1976 provoquent une forte sensibilisation de la population et des pouvoirs publics. La réglementation Seveso voit le jour. Dans le même temps, les techniques quantitatives se développent. Celles-ci ont deux objectifs : améliorer la disponibilité des

[6] C'est la capacité pour des composants à être maintenus, de manière cohérente et à moindre coût, en état de fonctionnement.

systèmes, afin de réduire le coût des défaillances matérielles, et évaluer les risques, afin de réduire les possibilités d'accidents industriels.

Depuis les années 80, les études de risques et l'utilisation des techniques de fiabilité se sont généralisées dans le domaine nucléaire. L'accident de *Three Miles Island*, en 1979, a contribué à faire évoluer les méthodes de sureté de fonctionnement. Dans ses conclusions, la Commission d'enquête présidentielle (1979) recommande l'utilisation croissante des méthodes d'analyse probabiliste des risques. Ces techniques se sont également exportées dans d'autres branches industrielles, telles que le domaine pétrolier, la chimie, les transports ferroviaires, ou encore l'industrie automobile.

Un développement de la prise en compte des facteurs humains

La notion de facteur humain est apparue dans les années 1930 dans le domaine militaire. Des travaux sur les activités cognitives telles que la mémoire, la perception, l'attention et le sommeil ont permis la conception de critères pour la sélection des soldats devant participer à des missions pour lesquelles les défaillances de ces capacités sont critiques (Chapanis, 1963). Dans le domaine industriel, le développement des premières approches scientifiques du travail (Taylor, Ford), fait apparaitre une dichotomie homme / machine. Cette séparation conduit à une classification des accidents selon deux facteurs : facteur technique et facteur humain. Cette période voit également le développement d'un courant de recherche, porté par la médecine et la psychologie, qui s'intéresse à l'homme au travail comme objet d'étude. Ces travaux cherchent à mettre en évidence le rôle de facteurs psychologiques et sociologiques dans les accidents. C'est l'émergence de la notion de prédisposition aux accidents liées à des variables individuelles (âge, sexe, fatigabilité, intelligence, type de personnalité, aptitude à l'égard du risque…) et contextuelles (environnement familial, professionnel, social…).

Plusieurs modèles d'analyse émergent au cours de cette période. En 1931, Heinrich constate que 88% des accidents sont causés par des gestes humains, 10% par des actes dangereux, et 2% par le hasard (Heinrich, 1931). L'auteur propose alors la théorie des dominos. Selon ce modèle, les évènements conduisant à un accident constituent une série de dominos : l'environnement social, l'erreur humaine, des actes dangereux, l'accident, et les blessures. Cette théorie est le premier modèle qui met l'accent sur un accident dû à l'erreur humaine (Hollnagel, 2004). Dans cette approche de modélisation, l'Homme est

intégré aux outils classiques d'évaluation de la fiabilité comme un composant, auxquels est associé un taux de défaillance. Les erreurs humaines s'expliquent généralement par un manque de formation, de rigueur et de discipline. Pour d'autres auteurs, tels que Raymon (1952), la conjonction des facteurs techniques et humains est indispensable pour qu'il y ait accident. Contrairement à Heinrich, cette vision de l'accident ne prend pas en compte les éléments de la situation de travail (technique et social).

Les années 1950 sont sources d'une structuration des travaux de recherche autour de trois approches : l'ingénierie de fiabilité, le management des risques, et l'approche « human engineering ». L'ingénierie de fiabilité cherche à réduire le nombre de défaillances et de pannes des systèmes technologiques. Parallèlement, le management des risques cherche à identifier les facteurs organisationnels qui contribuent à la maitrise des risques. Enfin, devant l'insuffisance des critères de sélection des individus, l'approche « human engineering » s'intéresse à la compréhension de l'homme au travail. Les premiers travaux, issus des domaines du nucléaire, du charbonnage et de la sidérurgie, se focalisent sur l'aspect psychologique du travail. Ce sont les débuts des démarches ergonomiques. L'accident s'explique par le couplage existant entre l'opérateur et son environnement direct de travail. Plusieurs paramètres caractérisent la possibilité pour l'homme de commettre des erreurs, mais également ses capacités de rattrapages : le niveau de stress, la charge de travail, les capacités cognitives, les facteurs environnementaux… On parle alors de fiabilité homme machine.

Les années 1970 se caractérisent par des évolutions technologiques. L'automatisation et l'informatisation modifient en profondeur les processus de production. Il en résulte une complexification des systèmes, et une redéfinition du positionnement de l'Homme vers des activités de contrôle, de surveillance et de maintenance. Le perfectionnement des études quantitatives de fiabilité permet également un renforcement de la sécurisation des systèmes. C'est la notion de défense en profondeur, et de l'ajout de nombreuses barrières de sécurité. Paradoxalement, ces barrières constituent de nouveaux points faibles qui fragilisent le système. Celui-ci devient de plus en plus difficile à comprendre, et donc plus difficilement maitrisable pour les personnes chargées de le gérer. Dans son fonctionnement automatisé normal, le système ne requiert pas l'action de l'Homme. Cependant, certains dysfonctionnements, souvent rares, vont exiger une intervention humaine. La méconnaissance du déroulement des évènements antérieurs, le haut niveau d'expertise demandé, et des processus de décisions sous incertitude et contraintes temporelles vont alors favoriser l'apparition d'une erreur humaine. Cette période voit alors le développement

de travaux sur la fiabilité humaine et la notion d'interface homme machine. La manière dont sont agencées les informations pour l'opérateur joue un rôle dans la fiabilisation des interactions entre l'Homme et la machine qu'il conduit. Plusieurs théories explicatives sur les origines de l'erreur : Théorie de la détection du signal (Tanner et al., 1954), Théorie de l'information de Shannon (1948), Théorie de l'image opérative d'Ochamine (1978) ou de la représentation fonctionnelle de Leplat (1985), Théorie de l'homéostasie du risque du Wilde (1982) sont publiées. Des outils d'évaluation de la fiabilité humaine, fondés sur des approches quantitatives sont également disponibles. C'est le cas de la méthode TESEO[7], et THERP[8].

Dans la même période, un certain nombre d'accidents industriels font apparaitre l'Homme comme facteur d'infiabilité. L'un des plus connus est certainement l'accident nucléaire de Three Miles Island, aux Etats-Unis, en 1979. Cette nuit-là, plusieurs défaillances techniques ont provoqué une fuite du circuit primaire d'un réacteur de la centrale, conduisant à un début de fusion du cœur et à un relâchement d'une grande quantité de radioactivité autour de la centrale. L'enquête post accidentelle met en avant l'incapacité des opérateurs de conduite à comprendre l'enchainement des évènements et à reprendre le contrôle du système. Si la quantité d'informations est disponible, elle ne permet pas toujours aux opérateurs de se construire une représentation juste de la situation, telle qu'elle se déroulait en cœur du réacteur. Plusieurs facteurs explicatifs sont mis en avant, comme la complexité du système, la conception de la salle de contrôle et des interfaces homme / machines, les procédures d'urgences, l'apparition d'effet tunnel et la redondance organisationnelle (Llory, 1999).

A la suite de l'accident de Three Miles Island, les années 1980 voient la nécessité de la prise en compte du facteur humain dès la conception des outils de gestion des processus de production. La notion d'homme / machine laisse place à la notion d'homme / tâche. Les sciences cognitives abordent les problèmes d'aménagement des tâches au regard des fonctionnements cognitifs et des représentations mentales. L'erreur est placée dans les phases de raisonnement. Ces travaux permettent une meilleure compréhension des facteurs qui concourent à l'erreur humaine : les circonstances de production, la qualité de définition de la tâche, les conditions externes et internes de réalisation… Plusieurs domaines de spécialisation font leur apparition, comme l'ergonomie des logiciels, l'intelligence artificielle, et les systèmes experts. Des outils plus précis d'évaluation de la fiabilité

[7] Une revue des différentes méthodes d'évaluation de la fiabilité humaine a été réalisée par le *Health and safety Laboratory* (Bell et al., 2009).

humaine sont également développés. Les méthodes SLIM[8], et MAUD[8] se basent sur un relevé des erreurs les plus fréquentes à partir de l'analyse des tâches et des facteurs d'influence. La méthode SHERPA[8] intègre les mécanismes psychologiques d'erreur décrits dans le modèle de traitement de l'information de Rasmussen (1983) et la modélisation de l'erreur de Reason (1990). La méthode HEART[8] prend en compte les conditions techniques, organisationnelles et environnementales de la tâche. Enfin, la méthode GEMS[8] s'appuie sur les mécanismes de gestion de l'information et des justifications psychologiques de l'erreur. Depuis les années 2000, l'homme est considéré comme un acteur à part entière de la maitrise des risques. Les nouvelles approches du facteur humain se focalisent sur la connaissance et l'apprentissage des activités.

Un développement de la prise en compte des facteurs organisationnels

Les évolutions organisationnelles de la fin du XXème siècle sont marquées par des ruptures, à la suite de grandes catastrophes industrielles. Jusque dans les années 1970, la sécurité s'appuie sur la fiabilité des composants, et la prise en compte des facteurs humains dans les processus de production. Les années 80 ont fait l'objet de plusieurs accidents technologiques marquants. L'analyse de ces nouveaux évènements montre que la défaillance technique et l'erreur humaine ne suffisent plus à expliquer l'occurrence de l'accident. Plusieurs raisons peuvent expliquer ce modèle fondé sur l'humain (Daniellou et al., 2010) :

- La focalisation sur les erreurs humaines pousse à ignorer la totalité des régulations effectuées par l'Homme. Seuls les évènements non désirés sont pris en compte.
- La plupart des erreurs sont rattrapées par l'individu. En outre celles-ci sont très nombreuses, et ne peuvent toutes être détectées.
- Une même erreur peut avoir des conséquences différentes selon le contexte dans lequel elle se produit. Analyser les erreurs isolément ne permet pas de comprendre l'accident.
- Il n'est pas possible de définir l'ensemble des tâches à réaliser dans une journée de travail. Un même geste peuvent donc être considéré ou non comme une erreur, selon s'il a été prévu ou non.

- Les analyses d'accidents ont souvent fait l'hypothèse d'une capacité cognitive infinie. Dans la rapidité des évènements, il n'est parfois pas possible de faire appel calmement à ses connaissances, et à une capacité de réflexion approfondie.

- L'analyse d'accidents prenait difficilement en compte la conception du système lors d'une analyse d'erreur lors de l'exploitation du système.

Face à ces limites, plusieurs champs scientifiques liés aux facteurs organisationnels ont pris en charge les questions de sécurité industrielle. Elles manifestent une volonté d'agir sur le comportement des organisations. L'accident est par essence multicausal. De nombreux concepts émergent alors : la culture de sécurité, les organisations hautement fiables... L'accident organisationnel remet en cause l'entreprise dans son ensemble, à l'échelle locale, ainsi qu'à celle de ses parties prenantes (autorités, sous-traitants, actionnaires...). Cette approche de l'organisation est complétée depuis une vingtaine d'années principalement par une vision systémique et résiliente sur le système industriel. En outre, ces approches récentes sont encore peu développées au regard des autres développements énoncés.

Une sécurité de réaction et ses effets

Les développements cités précédemment constituent l'héritage du XXème siècle. Deux caractéristiques principales sont identifiables. Premièrement, c'est une sécurité réactive. Elle est décalée, retardée, non synchronisée aux évènements industriels. C'est une sécurité par à-coup, en réaction aux catastrophes. En effet, et comme le montre le graphique suivant (Figure 11), les développements ont été insufflés par l'occurrence de plusieurs drames industriels.

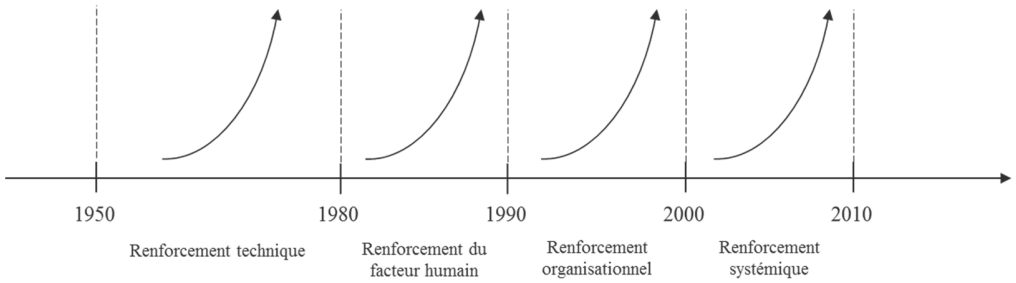


Figure 11 : Les grands développements scientifiques du XXème siècle, relatifs à la sécurité industrielle

l'environnement, ainsi qu'à la directive européenne du 24 juin 1982 concernant les risques d'accidents majeurs de certaines activités industrielles, dite directive « Seveso ». L'accident de la centrale de Three miles Island est un tournant dans les réflexions portant sur les interfaces Homme / machine, et plus largement sur la place et le rôle de l'Homme au sein du processus industriel. Les accidents de Bhopal, de Flixborough, de Tchernobyl, et de Piper Alpha, ont contribués aux réflexions portant sur le versant organisationnel de la sécurité. Ils ont également été déclencheurs de la directive européenne du 9 décembre 96 concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses, dite directive « Seveso II ». L'explosion de l'usine AZF a alimenté de larges questionnements relatifs à l'urbanisation autour des sites industriels, et au rôle de la société civile dans la maitrise des risques industriels. Elle est principalement à l'origine de la loi du 30 juillet 2003 relative à la prévention des risques technologiques et naturels et à la réparation des dommages. Enfin, les récents accidents de Buncefield, de Texas City, de Deepwater Horizon, et de Fukushima, ont fait émerger de nouvelles attentions sur le fonctionnement et l'évolution globale des systèmes industriels.

La deuxième caractéristique concerne la motivation sur laquelle repose cette sécurité. C'est une construction fondée sur l'angoisse. Sans rentrer dans l'approche psychologique, il convient de noter la dureté des effets d'un accident industriel majeur. La règlementation s'articule notamment sur la volonté de ne plus revivre des conséquences insupportables.

Afin d'illustrer ce propos, le tableau suivant (Tableau 6) décrit l'étendue des conséquences imposées par les principaux accidents.

Accident	Date	Conséquences
Feyzin	04/01/1966	18 morts, 77 blessés.
Flixborough	01/06/1974	28 morts, 36 blessés.
Seveso	10/07/1976	200 personnes malades, contamination importante de l'environnement.
Three Miles Island	28/03/1979	Accident nucléaire catégorie 5, et faible relâchement dans l'atmosphère d'un nuage radioactif.
Bhopal	03/12/1984	10000 morts et 300000 malades
Tchernobyl	26/04/1986	Accident nucléaire catégorie 7, et relâchement dans l'atmosphère d'un nuage radioactif.
Piper Alpha	06/07/1988	167 morts, et perte de la plateforme.
AZF	21/09/2001	31 morts, 2500 blessés.
Texas City	23/03/2005	15 morts, 170 blessés.
Buncefield	11/12/2005	43 blessés, 2000 personnes évacuées.
Institute	28/08/2008	2 morts, 8 blessés, 40000 personnes confinées pendant 3 heures.
Deepwater Horizon	20/04/2010	11 morts, 17 blessés, pollution maritime de grande ampleur

Tableau 6 : Description des conséquences des principaux accidents majeurs

Le contexte économique joue également un rôle dans la construction de la sécurité industrielle. Celle-ci a pris place dans une tendance d'industrialisation. C'est un monde de temps long, qui évolue peu. Le mouvement des entreprises est alors caractérisé par plusieurs dominantes :

- ✓ Une confiance dans le progrès technologique. Elle s'est formalisée par exemple à travers les différentes expositions universelles, ou encore la conquête de l'espace.

- ✓ Une large ouverture des marchés. Héritage de l'époque coloniale, et amélioration des moyens de production, ont permis la création de nouvelles opportunités commerciales.

- ✓ Un développement de nouvelles énergies. L'essor du pétrole donne naissance à la pétrochimie. Celle-ci est ensuite complétée par l'électronucléaire.

Dans ce contexte, la recherche de la performance et de la continuité pousse les entreprises à se transformer, en automatisant les procédés. Un haut niveau de productivité est recherché. Les ressources, les moyens de production, et les énergies sont imbriqués et concentrés. La production s'effectue de manière centralisée, et en grande série. Les processus sont rationnalisés. Il s'agit de gérer les ressources de la manière la plus efficace possible. L'organisation du travail se développe, et s'articule autour des procédures, des normes et des standards.

En parallèle, la sécurité doit s'intégrer dans les évolutions, permettant de poursuivre les transformations. Au cours de cycles de complexification, des progrès dans la manière de maitriser les risques sont réalisés, en couplant simultanément baisse du niveau de risque global, et augmentation de la productivité.

Le niveau de complexification atteint aujourd'hui soulève de nouvelles problématiques. Tout d'abord, l'entreprise est de nos jours placée face à une situation de saturation réglementaire. Dans le domaine de la gestion des risques, celle-ci est placée face à une obligation de moyens et de résultats. La transposition de chaque nouveau risque en norme ferme davantage les possibilités d'action.

Egalement, le niveau de risque stagne. S'il n'a jamais été aussi bas, les efforts entrepris pour abaisser les niveaux de risque semblent ne plus porter leurs fruits. De nouveaux accidents majeurs arrivent encore. Ces évènements ont un caractère paradoxal, dans la mesure où la connaissance nécessaire à expliquer leur survenue existe, et est utilisée lors des enquêtes. Pour autant, cette connaissance n'a pas permis d'éviter les dits accidents.

De plus, les systèmes industriels font l'objet d'une calcification. C'est une situation paradoxale dans laquelle on assiste à un découplage entre les règles de gestion et les effets. L'accident ferroviaire de Brétigny sur Orge, en 2013, en est un exemple. Les enquêteurs ont constaté le délabrement général du réseau ferroviaire, alors même que les plans de maintenance sont de plus en plus conséquents.

Une sécurité industrielle construite sur l'expérience et la mémoire

L'évolution des méthodes de travail a toujours été associée au travail lui-même. Que ce soit l'artisan qui améliore ses outils, le chef cuisinier qui modifie ses recettes, en encore l'enseignant qui adapte sa pédagogie, chaque personne cherche à comprendre la motivation et le déroulement de son travail, pour en améliorer l'efficacité. Plusieurs leviers sont moteurs de ces évolutions. On peut identifier la recherche de rentabilité (réaliser la même tâche, avec moins de ressources), les bonnes et mauvaises expériences passées (occurrence d'un incident, ou réussite inespérée), le progrès technologique (l'automatisation permet de réaliser de nouvelles tâches), les évolutions réglementaires (apparition d'une nouvelle norme, restriction du temps de travail...), et enfin le levier de la mémoire de l'accident subie, fondée sur une émotion collective marquante pour la société.

L'évolution des méthodes de travail s'est faite de différentes manières. Deux voies principales peuvent être identifiées. La première voie est celle de la transformation. Il s'agit de modifier des usages pour les rendre plus adaptés à la situation actuelle. C'est par exemple le cas pour le massage cardiaque. Le progrès dans les connaissances du fonctionnement du corps humain a permis de rendre cette technique de réanimation plus efficace. La seconde voie est celle de l'accumulation. Aux pratiques existantes sont ajoutées de nouvelles pratiques, généralement plus contraignantes pour l'opérateur, mais dont le sens importe pour le système dans sa globalité. C'est par exemple le cas lors d'ajouts de règles de traçabilité, de sécurité, ou de protection individuelle. Or, le paragraphe précédent a montré que la modèle de sécurité du XXIème siècle était celui de l'expérience et de la mémoire. Plusieurs développements sont venus au fil des accidents, compléter la manière dont les risques industriels sont gérés. Apprendre des expériences, tel a été la base de l'évolution de la sécurité des systèmes industriels. L'accumulation possède également un avantage important. Elle s'appuie sur les règles antérieures, et permet de conserver une certaine stabilité du système. Une phase transitoire existe entre les anciennes règles et les nouvelles. La rupture est amortie par la superposition temporaire entre deux systèmes. C'est ici tout l'enjeu de la sécurité du XXIème siècle. Il s'agit de trouver le point d'équilibre existant entre la nécessité d'évolution, et le besoin de stabilité du système. En outre, l'accumulation a également des limites. Sans les expliquer à nouveau, on peut citer l'abondance de réglementations contraignantes, la stagnation du niveau de risque, ou encore la calcification du système industriel.

En outre, l'accumulation des barrières de prévention des risques a effacé la crise de l'accident industriel. Le risque s'est substitué à la catastrophe. L'attention est focalisée sur

l'analyse du risque, et la construction de barrières de prévention. L'accident majeur est devenu l'exceptionnel, l'improbable. Il ne peut plus arriver. Le système se trouve dans une posture ou l'accident devient une surprise. Le choc fait place à l'incompréhension. La sursécurisation du risque en a fait oublier les conséquences. L'exceptionnel devient préoccupant et anxiogène.

L'accident de l'usine AZF en 2001, a remis en cause cet état de fait. L'explosion d'un stock de nitrate d'ammonium, a entrainé la mort de 31 personnes, faisant 2 500 blessés et de lourds dégâts matériels. A l'instar des précédents accidents, la réponse étatique a été normative, et technique. Premièrement, en 2003, la loi du 30 juillet 2003 relative à la prévention des risques technologiques et naturels et à la réparation des dommages est promulguée. Cette loi comporte quatre points importants : l'obligation d'informer les riverains, la sensibilisation des salariés et des sous-traitants, la maîtrise de l'urbanisation par la définition de zones à risques, la reconnaissance de la notion de risques technologiques. Deuxièmement, les établissements mettant en œuvre des processus à hauts risques industriels doivent faire l'objet d'un plan de prévention des risques technologiques. Leur objectif est de résoudre les situations difficiles en matière d'urbanisme héritées du passé et, mieux encadrer l'urbanisation future. C'était un retour en arrière intéressant dans le sens où l'accident reprend une place dans la politique de gestion des risques. Celle-ci est modifiée. L'accident devient un aléa technologique. Et l'anticipation de la crise doit être réalisée aussi au niveau de la population. L'occurrence d'un accident doit être pensé et prévu dans la société. 10 ans après l'entrée en vigueur de la loi "Risques", le bilan des PPRT est le suivant. Ils concernent 407 bassins industriels et plus de 800 communes et 99% d'entre eux sont désormais prescrits et 73 % approuvés (site du ministère de l'écologie, du développement durable, et de l'énergie). Si la phase de rédaction des plans connait un relatif succès, leur mise en œuvre concrète semble être plus difficile. La complexité technique du sujet, l'importance des enjeux de sécurité, et les coûts associés au PPRT en font un outil difficile à mettre en œuvre. Au-delà de l'approche financière des dommages, la loi Risque apparait comme un outil de tranquillisation des populations par rapport à un risque oublié.

I.2 Positionnement scientifique des principaux courants théoriques

Tel que cela est décrit dans la première partie, l'étude des accidents s'inscrit dans une longue tradition technique et scientifique. Différentes communautés scientifiques et professionnelles se sont intéressées aux questions de sécurité des systèmes industriels et aux processus accidentels : psychologues, sociologues, ingénieurs (de multiples disciplines), chercheurs en management en sciences de gestion.... Egalement, des enquêteurs, avocats, décideurs, et législateurs ont été confrontés aux questions de compréhension de l'accident industriel. La diversité de ces sources et leurs origines hétérogènes ont formé une littérature vaste, mais fragmentée. Et plusieurs auteurs ont cherché à identifier une structure dans l'évolution des idées relatives aux approches de modélisation des systèmes industriels, à partir de l'accident.

Selon Lheto et Salvendy (1991), les modèles d'accidents disponibles diffèrent sur de nombreux critères. Ils diffèrent selon leur champ d'application (industrie, transport, application générique...), leur finalité (descriptive ou prescriptive, générique ou spécifique...), leur structure (mathématique, logique, verbale, séquentielle...), leur objet d'étude (Homme, processus industriel, produit...), et leurs données d'entrée et de sortie (danger, erreur, probabilités, causes ou solutions). Les auteurs se sont appuyés sur l'étude de 54 modèles pour développer une taxinomie des modèles d'accidents (Figure 12).

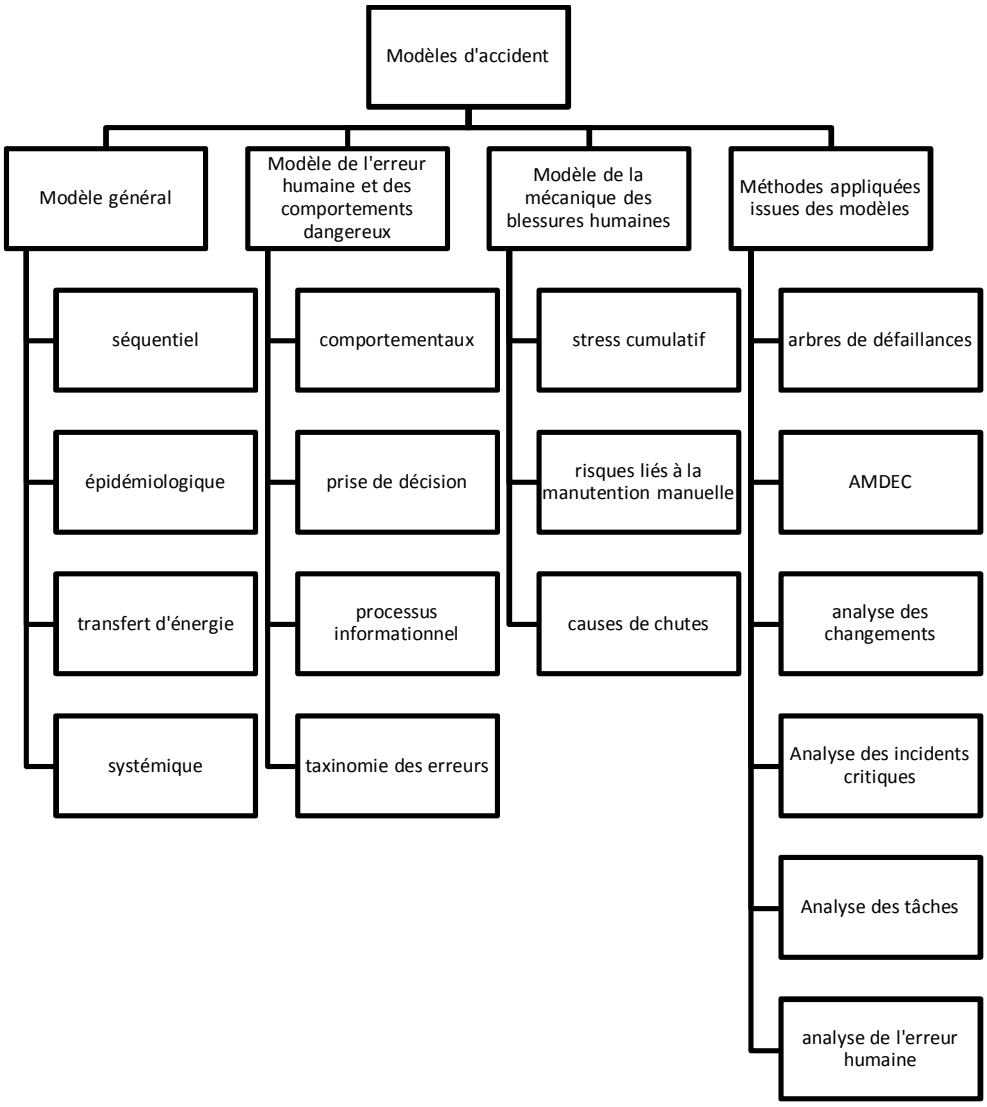


Figure 12 : Taxinomie des modèles d'accidents selon Lheto et al. (1991)

Wilpert et Fahlbruch (1997) avancent une vision différente de l'évolution de la recherche dans le domaine nucléaire. Le déplacement de l'objet d'étude de la défaillance technique vers l'erreur humaine, puis l'organisation, et enfin l'organisation dans son contexte, montre une volonté de rendre le phénomène plus intelligible, par une prise de recul et une prise en compte de la dynamique du système (Figure 13). L'approche devient systémique, et implique une considération globale du système, ses interactions internes (opérateurs, managers, directeurs…) et externes (contraintes de marché, autorités, opinion publique…).

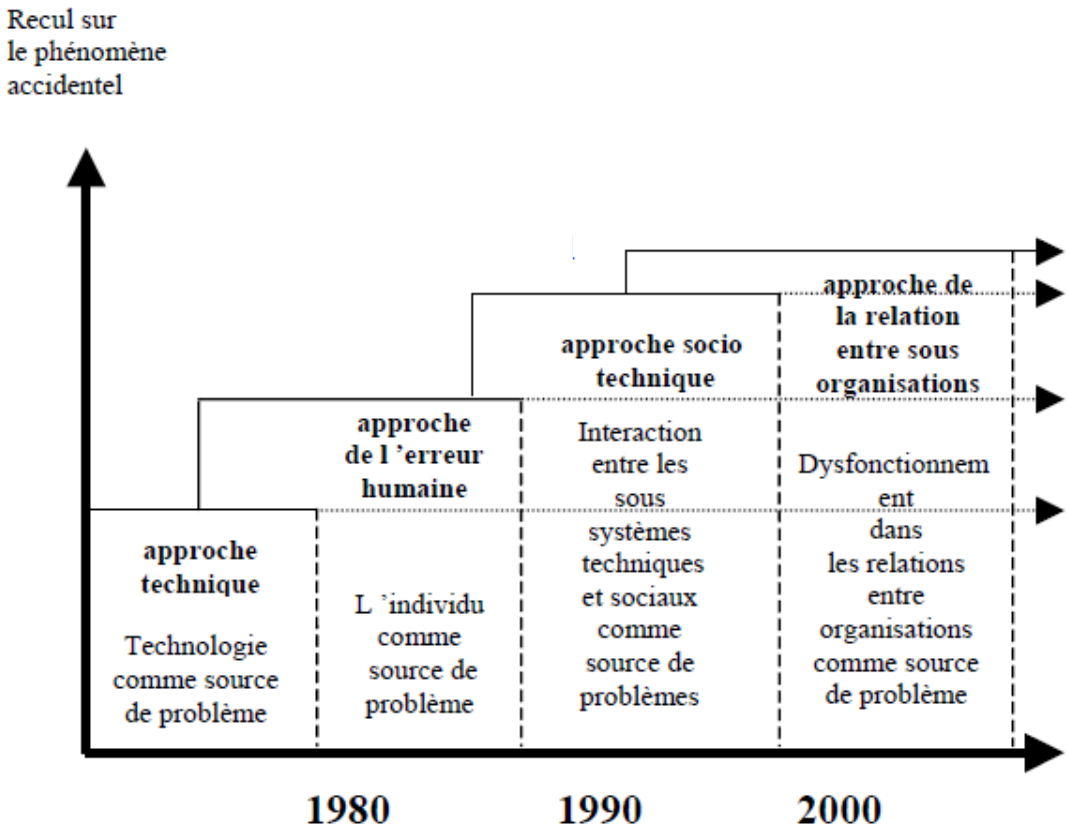


Figure 13 : Evolution de la recherche dans le nucléaire, selon Fahlburgh et al. (1997)

Sklet (2004) argue que l'absence de définitions et de concepts communs provoque une confusion des idées. C'est par exemple le cas sur la notion de causes, lors d'analyses post-accidentelles. Certains auteurs se concentrent sur les facteurs causaux, d'autres sur les facteurs déterminants, les facteurs contributeurs, les causes racines, ou les défaillances actives et les conditions latentes. En outre, bien que les termes utilisés par les enquêteurs soient différents, leurs conclusions sur les faits, et les recommandations proposées pour éviter qu'un autre accident ne se produise, sont généralement similaires.

D'autres auteurs ont cherché à classifier les modèles d'accidents disponibles dans la littérature. Laflamme (1990) a proposé une représentation fondée sur quatre approches différentes : décisionnelle, séquentielle, dynamique et séquentielle, et organisationnelle.

Kjellen (2000) a décrit cinq catégories de modèles : cause-conséquence, process, énergie, arbre logique et management Hygiène, Sécurité et Environnement. Hollnagel (2002), classe les modèles d'accidents en trois groupes : séquentiel, épidémiologique et systémiques. Cette même classification a été reprise par Qureshi (2007). Katsakiori et al. (2009) proposent une classification des modèles orientée vers l'individu, en trois groupes majeurs : les modèles séquentiels (terme repris d'Hollnagel, 2002), qui décrivent les accidents comme une séquence d'évènements dans un ordre spécifique ; les modèles focalisés sur le traitement de l'information par l'homme (d'après Lheto et Salvendy, 1991), qui analysent l'accident en terme de comportements humains ; et enfin les modèles systémiques (également d'après Hollnagel, 2002), qui incluent les facteurs organisationnels et décrivent les performances du système global. Saleh et al. (2010) proposent une nomenclature des modèles d'accident et de sécurité des systèmes fondée sur quatre groupes majeurs d'idées (Figure 14). Le premier groupe inclue les travaux de Turner et al. (1978), Perrow (1984), et Vaughan (1996). Le second groupe fait référence aux modèles d'arbres de défaillances, et d'analyse probabiliste des risques. Le troisième regroupe les modèles de défense en profondeur et de barrières de protection. Enfin, le dernier groupe reprend les approches de la sécurité par les théories de contrôle et systémiques.

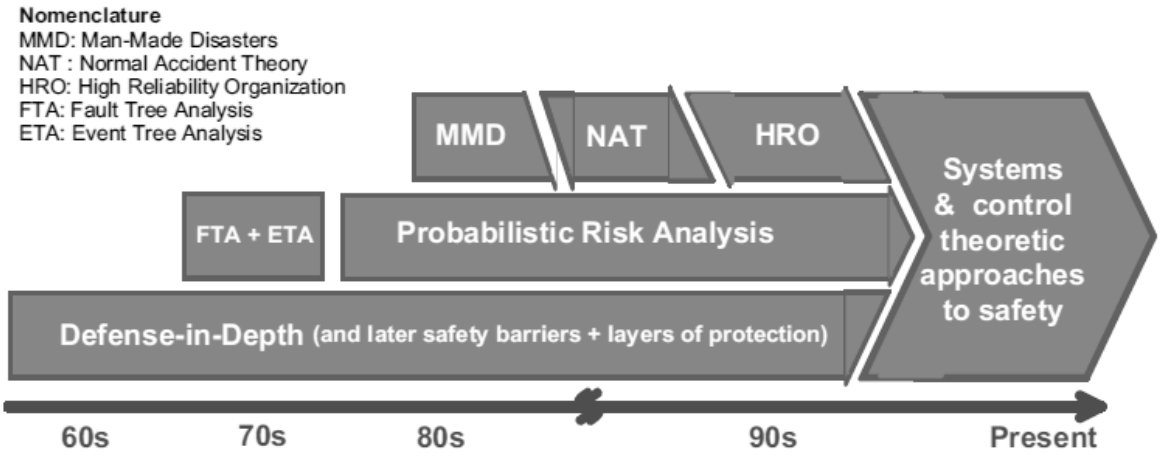


Figure 14 : Evolution des idées relatives aux modèles d'accident, selon Saleh et al., (2010)

Depuis les premières explications sommaires d'accident, jusqu'aux modèles récents plus élaborés, les cas de notre étude ont fait l'objet d'analyse fondée sur des modèles construits à partir de niveaux de connaissances différents. Pour mieux faire, il aurait été nécessaire de

choisir un modèle descriptif de l'accident industriel, et d'analyser chaque cas à l'aide de cet unique modèle, pour ensuite les comparer. Cette approche de la comparaison très difficilement réalisable, pour au moins deux raisons. La première est liée à l'existence même des modèles. Comme le montre les graphiques précédents, la tendance en matière de modélisation a été d'intégrer de plus en plus d'éléments du système analysés. Les périmètres d'analyse actuels sont beaucoup plus étendus que ceux du XVIII^{ème} siècle. Ainsi, les données nécessaires à la construction des modèles d'aujourd'hui n'étaient pas collectées, car considérées comme peu importantes. Il existe donc un déficit de données, mais ce manque n'est visible que de notre point de vue de contemporain.

II – Analyse des principaux modèles de production de sécurité

Après avoir diagnostiqué les défis lancés au manager opérationnel, nous proposons dans cette deuxième partie une revue de différents modèles sécuritaires.

Pour atteindre cet objectif, nous avons décomposé la réflexion en deux étapes. Tout d'abord, nous abordons les cinq principaux modèles retenus, et à partir des défis, nous en proposons une analyse. L'objectif est d'identifier la capacité de chaque modèle à répondre aux défis managériaux.

II.1 Présentation des principaux modèles théoriques existants

Dans un premier temps, il convient de retenir les modèles les plus représentatifs pour notre analyse. Nous avons choisi les modèles ci-dessous (Tableau 7) pour les raisons suivantes :

1. Compte tenu des ressources disponibles pour ce travail d'analyse, seulement cinq modèles peuvent être sélectionnés.
2. Les modèles sélectionnés sont ceux majoritairement mentionnés dans les rapports d'accident.
3. Ces références sont également majoritairement reconnues par la littérature comme des modèles canoniques, structurant les développements scientifiques relatifs à la sécurité industrielle (cf. partie I.2 de la deuxième partie).

Nom	Date	Auteur(s)
Gérer les risques d'accidents organisationnels	1997	James Reason
Les organisations hautement fiables	2011	Kathleen M. Sutcliffe
La migration des activités du système	1997	Jens Rasmussen
La gestion de la sécurité dans les systèmes de production	2003	Andrew R. Hale
L'ingénierie de la résilience en pratique	2010	Erik Hollnagel, Jean Pariès, David W. Woods, John Wreathall

Tableau 7 : Liste des principaux modèles de production de sécurité sélectionnés

Afin de réaliser au mieux nos analyses, nous avons choisi un processus de lecture analogue fondé sur les deux points présentés ci-dessous. Ce processus a l'avantage d'être une revue méthodique de la principale littérature pertinente. Chaque théorie est étudiée selon la même trame méthodologique. Cependant, ce processus à l'inconvénient de rester à l'état d'étude bibliographique. Chaque théorie ne peut être analysée en profondeur.

Le processus est le suivant :

1. Premièrement, la partie II.1 propose une présentation détaillée des modèles sélectionnés, en plusieurs paragraphes, et selon la disposition suivante :

Titre du modèle **Auteur**

SYNTHESE

Synthèse en quelques lignes des principales idées décrites par le modèle.

CONTEXTE

Description des éléments contextuels avancés par l'auteur.

HYPOTHESES DU MODELE

Description des hypothèses sur lesquelles repose le modèle.

DESCRIPTION DU MODELE

Description des phénomènes menant à l'accident industriel.

LA PRODUCTION DE SECURITE

Description de l'apport de l'auteur relatif à la production de sécurité.

CRITIQUE DU MODELE

Synthèse des principales critiques publiées dans littérature scientifique.

2. Deuxièmement, chaque modèle est analysé au prisme des défis managériaux, tels qu'ils ont été formalisés en fin de première partie. Cette analyse est formalisée dans la partie II.2, et selon la disposition suivante :

Titre du modèle **Auteur**

<u>Le défi de la complexité :</u> faire l'inventaire des interactions qui caractérisent le système, identifier les propriétés émergentes.
Analyse du modèle au prisme du défi de la complexité.

<u>Le défi de l'érosion du temps :</u> prise en compte des effets cumulés d'évènements, et l'anticipation de rupture dans la continuité de fonctionnement du système.
Analyse du modèle au prisme de l'érosion du temps.

<u>Le défi de la décision :</u> construire une représentation actualisée de la situation, et une argumentation convaincante.
Analyse du modèle au prisme du défi de la décision.

Gérer les risques d'accident organisationnel
J. Reason (1997)

SYNTHESE

Selon Reason, l'accident organisationnel est le résultat de la dégradation des barrières de défense mises en place dans le système. Cette dégradation créée des trous dans les couches de défense. Une dégradation trop importante rend alors possible des trajectoires accidentelles. Selon Reason, l'apparition de trous est due à l'inefficacité des processus organisationnels sous-jacents au processus de production primaire. Pour maintenir un haut niveau de sécurité, il s'agit pour le management de surveiller ces processus organisationnels, afin de réduire au minimum les actes dangereux, et les conditions latentes accidentogènes.

CONTEXTE

Psychologue, J. Reason s'est d'abord intéressé à la psychologie cognitive des erreurs humaines. A travers l'étude de plusieurs accidents technologiques, l'auteur porte son travail sur la place de l'homme dans la supervision des systèmes technologiques. En effet, l'automatisation grandissante des systèmes de production n'a pas pour autant supprimé l'Homme du processus. Selon l'auteur, la raison principale de son maintien dans des systèmes essentiellement contrôlés par des ordinateurs « intelligents » est le traitement nécessaire des situations d'urgence non prévues au moment de la conception. Les concepteurs ne sont pas capables d'anticiper l'ensemble des scénarios possibles de défaillance, et par conséquent, ne sont pas capables de prévoir des dispositifs de sécurité pour chaque éventualité. Le recours à l'Homme est alors nécessaire, du fait de sa capacité inégalée à procéder à des résolutions de problèmes, en temps réel, et sur des situations nouvelles. En outre, cette capacité est principalement limitée, mis à part quelques exceptions (Apollo 13 par exemple), par l'effet du stress. Donc si l'opérateur a un apport positif pour la sécurité du système, il commet également des erreurs. Ce sont ces erreurs, ajoutées à la complexité du système, qui génèrent des accidents majeurs. De cette première vision de l'accident organisationnel a émergé une série de travaux sur le management de la sécurité dans les systèmes sociotechniques complexes.

Dans son dernier ouvrage, Reason (1997) oppose les accidents individuels aux accidents organisationnels. Les premiers sont les plus courants, et dont les effets n'impactent qu'un

ou plusieurs opérateurs, sans menacer de populations ou d'infrastructures externes au système. De plus, l'opérateur est généralement l'agent et la victime de l'accident. C'est le second type d'accident qui intéresse Reason : les accidents organisationnels. Ils sont rares, comparativement aux premiers, et souvent catastrophiques. Ils ont de multiples causes, et impliques de nombreux acteurs à tous les niveaux de l'entreprise. Le questionnement central de Reason porte sur la genèse des accidents organisationnels : quelles sont les origines de la rupture des défenses du système ?

HYPOTHESES DU MODELE

Le modèle de Reason repose sur plusieurs hypothèses :

1. **Un modèle expliquant les causes d'un accident doit comporter trois éléments basiques :** des dangers, des barrières de défense, et des pertes potentielles (Figure 15). L'accident est le résultat de la perte de maitrise du potentiel de danger, par les barrières de défense, et occasionne des pertes importantes.

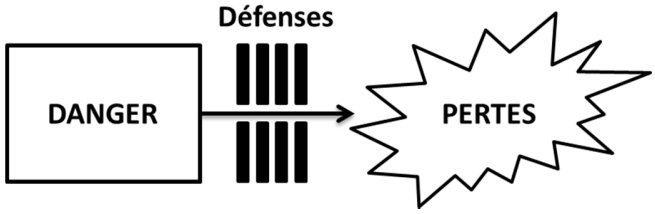


Figure 15 : Relation entre le danger, les défenses, et les pertes, traduit de Reason (1997)

2. **La gouvernance de tout système technologique par deux processus universels :** la production et la protection. Ces deux processus constituent une zone au sein de laquelle le système évolue (Figure 16). Cette zone opérationnelle est bordée par deux extrêmes dangereux. Lorsque la protection consomme les ressources du système de manière excessive vis-à-vis du potentiel de danger, le système sur sécurisé rentre dans une zone de faillite potentielle. A l'opposé, l'excès de pression productive, et la dégradation des barrières défenses, conduit à une zone à hauts risques d'accident

majeur. L'éloignement de ces deux zones de fonctionnement nécessite la recherche de l'équilibre entre les processus de production et de protection.

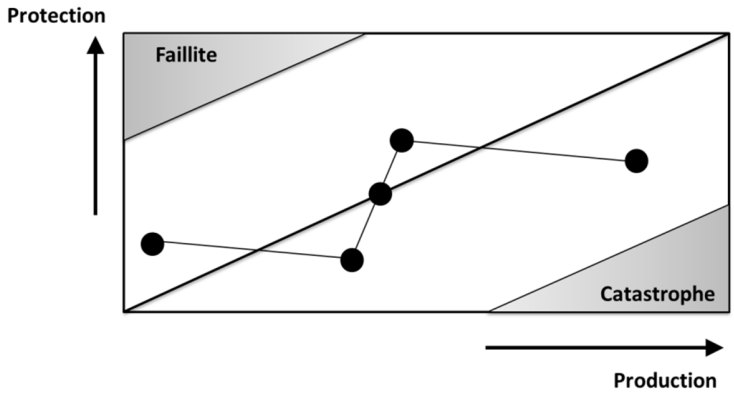


Figure 16 : Durée de vie d'une organisation hypothétique, dans l'espace production protection, traduit de Reason (1997)

3. **La dégradation de barrières de défense :** selon l'auteur, les accidents organisationnels naissent de l'affaiblissement simultané des barrières de défense du système. Dans un monde idéal, ces barrières sont pleinement efficaces, et bloquent l'ensemble des séquences accidentelles. En réalité, celles-ci sont constituées de faiblesses (panne, erreur de conception...). Ce sont les « trous dans le fromage ». Tous ces trous sont autant de fenêtres d'opportunité pour une séquence accidentelle.
4. **La culpabilité de l'Homme, qui fait des erreurs :** ce sont les actes dangereux, dont les effets se font ressentir immédiatement (erreurs actives). Elles sont généralement associées à l'activité des opérateurs qui sont en première ligne (opérateur de ligne, de salle de contrôle…).
5. **L'existence de conditions latentes accidentogènes :** dont les conséquences restent en sommeil dans le système, et ne se manifestent qu'en se combinant avec d'autres facteurs. Elles ont tendance à se développer à partir des activités de ceux qui sont éloignés de l'interface de contrôle direct, à la fois dans le temps et l'espace (concepteurs, managers…). Elles représentent la menace la plus importante sur la sécurité d'un système.

DESCRIPTION DU MODELE : L'ACCIDENT ORGANISATIONNEL

Les défenses du système

Les systèmes technologiques sont composés de nombreuses barrières de défense. Selon Reason, elles peuvent être catégorisées selon leurs fonctions. Bien que la fonction de défense soit partagée par toutes les barrières, leurs modes d'application varient. L'auteur propose la typologie suivante :

- Générer la connaissance et la conscience du potentiel de danger.
- Donner une claire indication de la manière d'opérer en sécurité.
- Fournir des alarmes et alertes lorsque le danger est imminent.
- Restaurer le système à un état sécurisé dans les situations anormales.
- Interposer des barrières de sécurité entre le potentiel de danger et les pertes possibles.
- Contenir et éliminer le potentiel de danger qui échapperait à ces barrières.
- Fournir le moyen d'échapper et d'être secouru lors d'une perte de confinement du potentiel de danger.

Ces défenses constituent des tranches successives de protection, chacune couvrant la défaillance de la suivante. C'est la multiplicité, l'imbrication, et l'interconnexion entre ces défenses qui rend les systèmes technologiques complexes. Selon Reason, ces différentes couches sont constituées de point de faiblesses, de trous, qui rendent possible les trajectoires accidentelles. Ces trous ont deux origines : les défaillances actives, et les conditions latentes. Les défaillances actives sont les contributions directes de l'Homme. Ce sont des actes dangereux, qui se matérialisent par des erreurs, ou encore des violations de règles de sécurité. Elles sont directement identifiables, et ont un effet direct sur le niveau de sécurité du système. Au sein de systèmes complexes, les défaillances actives sont considérées comme la conséquence de conditions latentes. Conception erronée, manque de supervision, procédure infaisable, défaut de maintenance... Les conditions latentes peuvent être présentent depuis plusieurs années dans le système. Elles émergent des niveaux décisionnels les plus élevés (régulateur, concepteur, managers stratégiques...) et impactent l'ensemble des décisions prises dans l'organisation. Si les défaillances actives sont uniques à un évènement spécifique, les mêmes conditions latentes peuvent contribuer à plusieurs incidents. Elles augmentent les probabilités des défaillances actives, par la création de facteurs locaux favorisant les erreurs ou les violations. Elles peuvent également en agréger

les conséquences. Compte tenu de la dynamique du système, les trous sont donc à géométrie et position variable au sein de la tranche.

La dynamique accidentelle

Selon Reason, la condition nécessaire à un accident organisationnel est la conjonction rare d'un jeu de trous dans les défenses successives, autorisant le potentiel de danger à porter atteinte aux cibles (Hommes et infrastructures). C'est le modèle du fromage suisse (Figure 17).

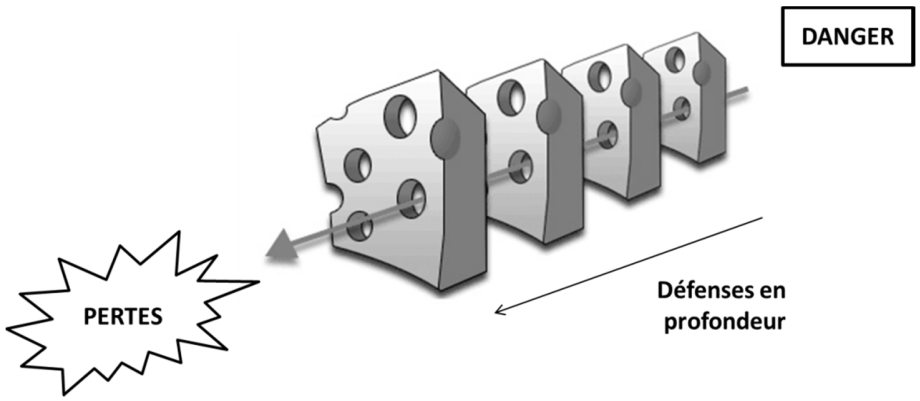


Figure 17 : Trajectoire accidentelle traversant les barrières de défense, adapté de Reason (1997)

Cette fenêtre d'opportunité est un évènement rare, du fait de la multiplicité des couches de défense, et de la mobilité des trous. Ainsi, l'accident organisationnel est rendu possible par la conjonction de trous issus de défaillances actives, et/ou de conditions latentes. Reason décrit plusieurs étapes successives dans la dynamique accidentelle (Figure 18). La première étape est la contribution de facteurs organisationnels : décisions stratégiques, allocations de ressources, management, communication... Ces facteurs négatifs sont le résultat d'un déséquilibre entre les processus de production et de protection décrits précédemment. Les conséquences de ces activités se déclinent aux différents postes de travail (salle de contrôle, poste de pilotage...), et se formalisent par des facteurs locaux qui influent sur le travail : pression de production, sous-formation, personnel réduit... Enfin, la troisième étape est l'apparition d'actes risqués. Les facteurs locaux, combinés à la tendance naturelle des

Hommes à faire des erreurs ou des violations, génère des trous dans les défenses. Finalement, si les trous s'alignent avec ceux créés par les conditions latentes, une fenêtre d'opportunité se créé pour une trajectoire accidentelle.

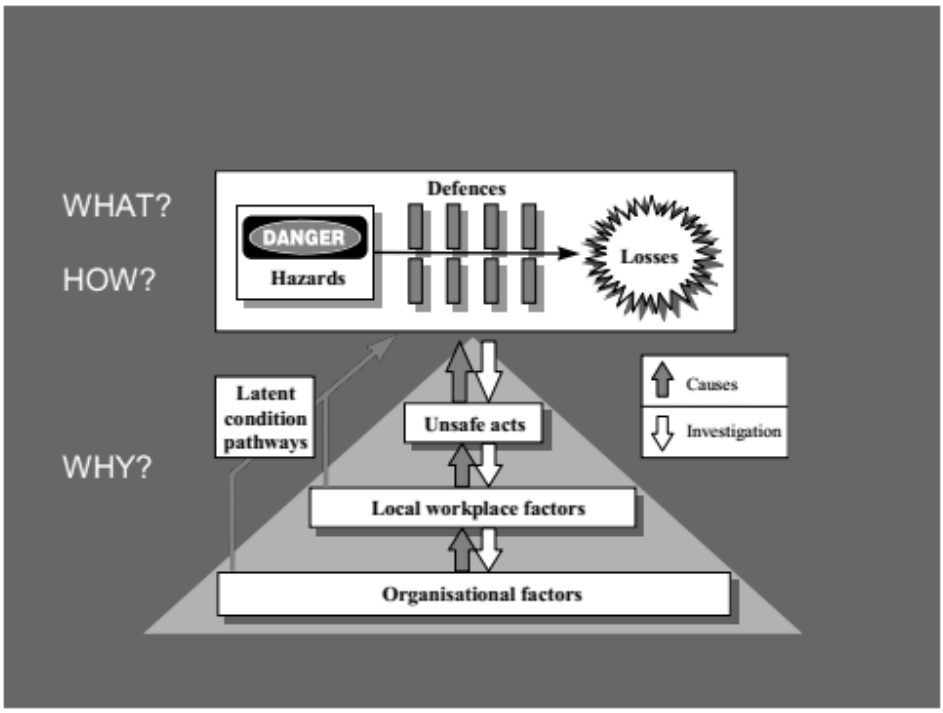


Figure 18 : Etapes dans le développement et l'enquête d'un accident organisationnel, tiré de Reason, (1997)

LA PRODUCTION DE SECURITE : L'ESPACE DE SECURITE

Selon Reason, au regard de leur nature, les accidents ne sont pas directement contrôlables. Et de ce fait, fixer des objectifs de réduction du nombre d'accident, ou d'incident, n'est pas pertinent. Le système ne peut pas supprimer les dangers, qui sont liés au processus de production, mais ne peut que chercher à se protéger contre une perte de contrôle. De même, il ne peut pas supprimer les actes dangereux, il ne peut que chercher à les diminuer.

L'espace de sécurité

Reason modélise le niveau de sécurité d'un système à travers son positionnement dans un espace de sécurité. C'est un espace conceptuel défini par deux notions opposées : la résistance et la vulnérabilité. Ainsi, la position du système dans cet espace est déterminée par la qualité du processus utilisé pour combattre et confiner les dangers associés au process de production. Cette localisation est donc fonction de l'étendue et de l'intégrité des défenses. Du fait des évolutions du système, de son environnement, et de ses barrières de défense, la position du système évolue dans cet espace, entre une zone de forte résistance, et une zone de forte vulnérabilité, accidentogène. Un management de la sécurité efficace doit donc chercher à fixer le système dans une zone de résistance maximum, et maintenir cette position. Pour réaliser cela, les managers doivent comprendre la nature des forces qui influencent le système, et le type d'information nécessaire pour maintenir la position (Figure 19). Reason définit deux types de forces : les forces agissant pour la sécurisation du système, et augmentant sa résistance (formation, procédures de vérification...), et celles réduisant la sécurité et augmentant sa vulnérabilité (turn-over, baisse de la maintenance...) Selon l'auteur, deux éléments sont nécessaires pour cela : un « moteur » interne pour piloter le système dans la bonne direction, et un « système de navigation » pour identifier les progrès.

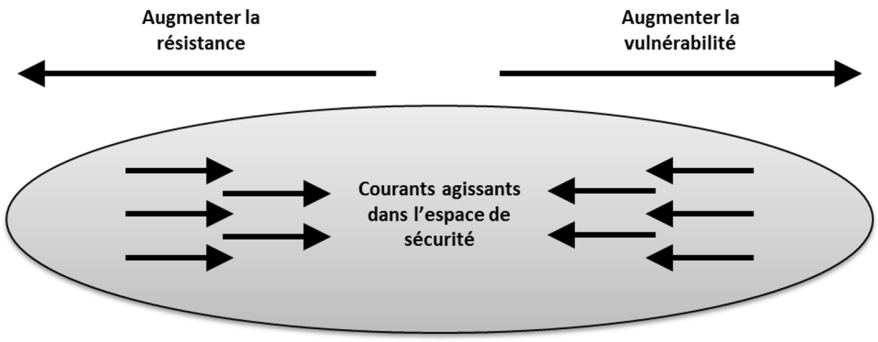


Figure 19 : Courants agissant dans l'espace de sécurité, traduit de Reason (1997)

Le moteur de la sécurité

Reason définit trois ingrédients vitaux pour piloter la sécurité. Ces forces stratégiques sont l'engagement, la compétence, et la conscience. L'auteur les définit de la manière suivante :

- **L'engagement :** il a deux composantes principales : les motivations et les ressources. La motivation fait référence au comportement des acteurs du système. Recherchent-t-ils un modèle de bonnes pratiques, où se contentent-t-ils de respecter la réglementation ? Les ressources font références aux efforts alloués par le système pour atteindre des objectifs de sécurité. Ceux-ci font références à toutes les sources de progrès : investissement financier, compétences, responsabilisation, valorisation... Un haut niveau d'engagement est difficile à obtenir et à maintenir, du fait par exemple du turn-over des cadres, ou encore des changements de priorités imposées par le marché. L'engagement est le résultat d'une forte culture de sécurité.
- **Les compétences :** atteindre des objectifs de sécurité nécessite de posséder les compétences techniques adaptées à la mise en œuvre du processus de sécurité. Et notamment, posséder les bonnes informations à travers un système d'information sécurité efficace.
- **La conscience :** c'est le fait de garder à l'esprit l'existence des dangers qui menacent les opérations. Deux caractéristiques sont symptomatiques des systèmes qui n'ont pas le niveau nécessaire de conscience. La première est un paradoxe positionnel. C'est le fait que le top management, qui possède le plus large degré décisionnel, règle la plupart de ses problèmes de sécurité en blâmant les opérateurs, qui ne font que suivre les procédures imposées, avec le matériel fourni. Le second symptôme est le phénomène du « savon », et concerne principalement les managers opérationnels en charge des questions de sécurité. Ils considèrent les mesures de sécurité comme un équipement. Ils les mettent en place, et ne comprennent pas une absence de résultats. Mais la sécurité est davantage un processus actif, qu'un équipement. Simplement les activer ne suffit pas. Il est nécessaire de les surveiller, les ajuster... Un système conscient de sa sécurité se renforce constamment.

Système d'aide à la navigation et espace de sécurité

Selon Reason, une notion clé pour naviguer dans l'espace de sécurité réside dans l'appréciation de ce qui est gérable et de ce qui ne l'est pas. La majorité des entreprises considèrent la sécurité comme un processus de production négatif. Les tâches associées sont la réduction des accidents, du temps d'arrêt de travail... A l'inverse, l'auteur considère le management de la sécurité comme un processus essentiel et complètement intégré au

processus de production. Au lieu d'exercer en vain un contrôle direct sur le nombre d'incidents et d'accidents, les managers doivent mesurer et améliorer en permanence les processus de production : conception, construction, formation, procédures, maintenances, budgétisation, planification, communication, gestion des conflits... C'est le processus de management qui détermine la santé du système de sécurité. Dans ce cadre, le seul objectif atteignable en terme de gestion de la sécurité n'est pas le zéro accident, mais l'atteinte d'une zone de résistance maximale, et d'y maintenir le système. Et cela nécessite un système d'aide à la navigation. Plus précisément, cela nécessite un système d'information sécurité qui ne révèle pas seulement les conclusions sur l'état passé (mesures réactives), mais qui facilite une vérification de l'état de santé des processus organisationnels (mesures proactives). Les principales composantes de ce système de navigation sont décrites dans la figure suivante (Figure 20).

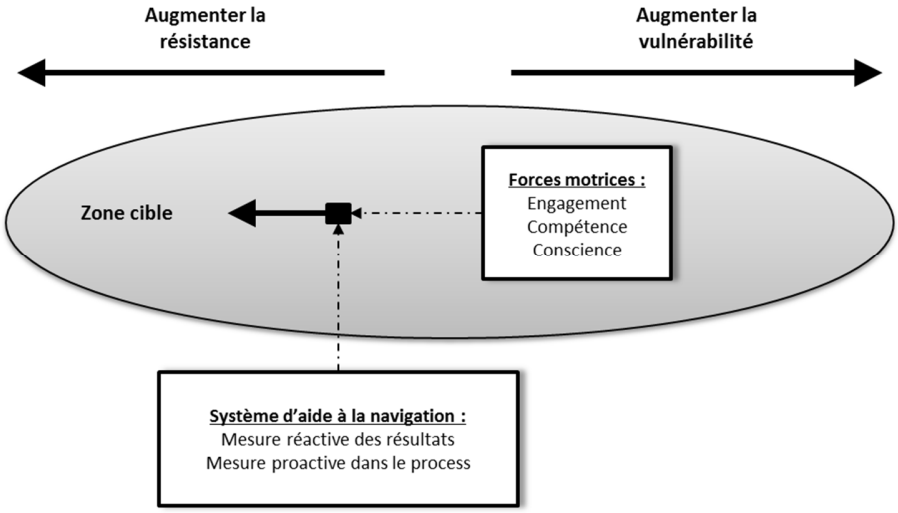


Figure 20 : Résumé des principaux facteurs impliqués pour la navigation dans l'espace de sécurité, traduit de Reason (1997)

Le système d'aide à la navigation doit répondre à deux objectifs :

1. Permettre l'apprentissage des leçons des évènements passés, et les traduire en savoir utilisable pour renforcer la résistance du système.

2. Rendre visible les conditions latentes accidentogènes aux managers et aux opérateurs du système.

Pour cela, il repose sur deux catégories de mesures, les mesures réactives et proactives. Utilisées correctement, celles-ci peuvent donner l'état des processus organisationnels sous-jacents. Ceux-ci sont directement liés à la dynamique accidentelle (voir tableau n°2).

- **Mesures réactives :** elles comprennent l'analyse des multiples évènements ou indices qui ont conduit à un incident, ou qui peuvent révéler un état de faiblesse des couches de défense. Elles sont possibles par la mise en place d'un système de reporting des incidents et presqu'accidents. C'est l'analyse des pénétrations partielles des barrières de sécurité, sans conséquences graves.

- **Mesures proactives :** les mesures proactives doivent s'appuyer sur le modèle d'accident donné précédemment. Le système d'information de la sécurité doit s'intéresser à mesurer trois types de données. Le premier type concerne les actes dangereux. En pratique, il n'est pas possible d'identifier l'ensemble des actes dangereux qui ont eu lieu. Ceux-ci sont parfois difficiles à définir, et difficile à identifier du fait de leur absence de conséquences. Il est alors nécessaire de définir des catégories d'actes (par exemple erreur et violation), et de définir les types de management adaptés. Le deuxième type de mesure concerne les facteurs locaux au poste de travail. Il s'agit d'identifier les précurseurs physiques et mentaux aux actes dangereux : niveau de supervision, pression de production, procédures infaisables... enfin, le troisième type concerne les hauts niveaux du système, générateurs de défaillances organisationnelles. Sans analyse de ces facteurs, les efforts réalisés aux niveaux inférieurs restent vains. La difficulté réside dans l'identification des processus organisationnels à surveiller. En effet, les systèmes sont constitués de nombreux éléments, inter-reliés, et interdépendants. Reason propose une typologie de macro-processus cibles de la mesure (Figure 21).

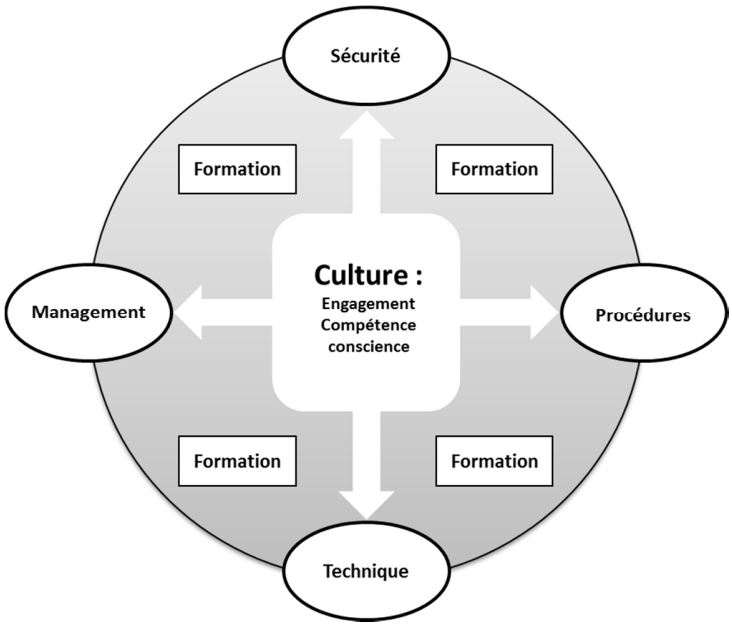


Figure 21 : Sous-systèmes organisationnels de sécurité sous-jacents au process primaire, traduit de Reason (1997)

La culture sécurité constitue le ciment de ces processus organisationnels. Elle est liée aux trois ingrédients nécessaires à la mise en œuvre du processus sécurité. Egalement, la formation est considérée comme un processus universel du système, et nécessaire à tous les autres. L'exercice de mesure associé à chaque processus organisationnel à deux objectifs. Premièrement, il s'agit d'identifier les processus donnant les plus grandes sources d'inquiétudes au moment donné. Deuxièmement, il s'agit de déterminer l'efficacité des dernières mesures correctives appliquées.

CRITIQUE DU MODELE

Après presque 20 ans de travaux sur le modèle d'accident organisationnel, Reason a proposé en 2006 une synthèse de l'évolution de ces travaux, et des critiques associées (Reason et al., 2006). D'après les auteurs, le modèle d'accident organisationnel a fait l'objet de deux critiques principales.

La première critique porte sur la description des couches de défenses, et des trous qui la composent. Le modèle n'est suffisamment précis sur la nature des trous existants dans les différentes couches, et notamment sur leurs interrelations. En conséquence, l'outil n'est pas utilisable comme outil d'enquête. Selon Luxhoj et al, (2003), sans la description précise des relations causales existantes entre les trous, les résultats sont trop vagues pour être utilisés en pratique. De plus, l'analogie des couches est intéressante pour imager la complexité de leur dégradation (processus de dégradation, influence des unes sur les autres...). Cependant, celle-ci ne peut définir la position des trous et leur nature, la raison de leur présence dès le début du système, la raison de leurs évolutions (taille, position), et la manière dont ces trous s'alignent pour permettre une trajectoire accidentelle (Dekker, 2002). Le manque de détails sur les trous est également constaté par Shappel et al. (2000). Si la métaphore du fromage suisse a révolutionné la vision de l'origine des accidents, la théorie ne donne que peu de détails sur ce que sont les trous en réalité, et notamment dans le contexte des opérations journalières.

La seconde critique principale porte sur l'insistance de Reason à se focaliser sur les conditions latentes dans la genèse des accidents. Cette focalisation sur les conditions latentes peut être remise en question au sein des cas où les erreurs des opérateurs ont été une contribution majeure de l'accident. Selon Reason et al. (2006), les faits soulevés sont les suivants :

- Les erreurs actives peuvent être le facteur dominant : les conditions latentes sont importantes, mais parfois les opérateurs ne font que seulement se tromper.
- Les liens relationnels, voire causaux, entre les conditions latentes, distantes, et les accidents sont généralement ténues, et seulement visibles avec le recul.
- Les conditions latentes sont toujours identifiables, avec ou sans accident.
- Des conditions latentes peuvent être difficiles à contrôler, même après plusieurs années.

- Une mauvaise application du modèle peut déplacer le blâme de l'opérateur au management.
- La mise en avant des problèmes de management peut éclipser ceux liés au facteur humain, tel que l'impact des émotions sur la performance par exemple, et freiner les recherches nécessaires à une meilleure compréhension de la fiabilité humaine.

Les organisations hautement fiables
K.M. Sutcliffe (2011)

SYNTHESE

Selon Sutcliffe, la haute fiabilité, entendue comme la capacité à maintenir une haute productivité et une haute sécurité à long terme, est le résultat de caractéristiques individuelles et organisationnelles spécifiques. La haute fiabilité n'est pas le produit d'invariance organisationnelle, mais plutôt le résultat d'un management continu des fluctuations.

CONTEXTE

Le paradigme des « organisations hautement fiables » fut d'abord développé par un groupe de chercheurs de l'Université de Californie, Berkeley, pour comprendre les points communs existant entre plusieurs organisations : le contrôle de la navigation aérienne, la gestion du réseau électrique, l'exploitation des centrales nucléaires, ainsi que celle d'un porte avion de l'armée américaine. Ces systèmes ne connaissent que très peu d'accidents, malgré un niveau de risque très élevé. L'objet de l'étude est alors de comprendre comment une telle fiabilité est obtenue, et maintenue dans le temps.

Roberts (1990) a alors défini comme hautement fiables l'ensemble des organisations à risques qui maintiennent un niveau élevé de sécurité à long terme malgré un potentiel catastrophique. Ces organisations prennent régulièrement de « bonnes décisions » qui permettent un fonctionnement fiable et de qualité.

Le concept d'organisation hautement fiable a également été remis en cause. Trois critiques principales ont été avancées :

1. **Le choix du terme « haute fiabilité » :** ce choix est problématique dans sa confusion avec le terme « sécurité ». La fiabilité fait référence à la capacité d'un système à assurer un service ou une production, alors que le terme sécurité renvoi à un état d'absence de défaillance. Par exemple, un système peut être considéré comme fiable parce qu'il assure un haut niveau de service, tout en ayant un état de

sécurité dégradé. Selon Hopkins (2007), fiabilité et sécurité ne sont pas équivalent, et ces deux objectifs peuvent être antagonistes.

2. **La formulation de la haute fiabilité, comme une propriété statique du système :** le terme HRO fait référence à une mesure statique de la fiabilité d'une organisation, alors que les HRO ont des propriétés, activités et réponses profondément dynamiques. La haute fiabilité demande une maitrise parfaite des activités, ce qui est impossible, compte tenu de la contingence du système. La gestion de la sécurité s'appuie sur une constante amélioration de la fiabilité et de la capacité de réponse, à la fois pour prévenir les défaillances et erreurs, et pour traiter et rattraper des défaillances devenues manifestes.

3. **La définition d'un label « HRO » :** il sous-entend une évaluation de la performance du système fondée sur un référentiel standard et absolu, plutôt que sur une évaluation relative. La haute fiabilité définit la capacité du système à maintenir une haute productivité et une haute sécurité à long terme, compte tenu de ses propres conditions d'évolution. Elle est donc spécifique à un système et à son contexte.

Pour résoudre ces limites, Rochlin (1993) propose une nouvelle définition des organisations hautement fiables : « Ce qui distingue les organisations hautement fiables, ce n'est pas leurs taux absolus d'erreurs ou d'accidents, mais une gestion efficace des activités à hauts risques, à travers un contrôle organisationnel du danger et des probabilités de risque. »

En 2007, Weick et Sutcliffe proposent également une nouvelle définition, argumentant que les HRO et non-HRO sont plus proches qu'elles ne semblent l'être. Une défaillance non traitée correctement peut être désastreuse pour tous les types d'organisation, même si les conséquences de la défaillance dépendent du contexte (une défaillance d'une HRO peut conduire à des pertes humaines, alors qu'un autre type d'organisation peut être soumis à une perte de réputation ou de crédibilité). Selon Weick et Sutcliffe, plus que les HRO, les non-HRO sont également amenées à prendre des décisions complexes dans un climat incertain, et souvent face à un savoir incomplet et sans vue globale de la situation.

Au regard de ces définitions, on peut identifier une évolution du concept. La haute fiabilité fut au départ considérée comme une caractéristique intrinsèque d'une organisation, et définie selon le taux d'accidents et de défaillances sur une longue période (Roberts, 1990). Ainsi, une organisation est, ou n'est pas hautement fiable, au regard de ses caractéristiques

(Roberts et Rousseau 1989). Les travaux récents abordent la haute-fiabilité comme un processus de maturation du système, vers un mode de gestion de plus en plus efficace, face au conflit production / sécurité. Il s'agit de mettre en place des caractéristiques qui permettraient aux organisations de devenir HRO : *reliability-enhancing* (Weick et Sutcliffe, 2007).

HYPOTHESES DU MODELE

Le choix des systèmes étudiés pour la conception du paradigme de la haute-fiabilité repose sur plusieurs critères de similarité :

- **Les conditions d'évolution :** les systèmes étudiés évoluent dans un environnement social et politique impitoyable. Leur technologie est risquée et présente un potentiel de dommages catastrophiques. Enfin, le champ des conséquences possibles d'une défaillance exclut l'apprentissage par l'expérimentation.
- **Une complexité interactive :** il existe des interactions entre les composants du système, et dont certaines peuvent être invisibles et imprévisibles. Ainsi, il n'est pas possible de définir l'ensemble des scénarios accidentels potentiels.
- **Des couplages étroits :** il existe des interdépendances fortes entre les éléments du système, incluant les composants, le personnel, et les procédures. Ces couplages induisent des effets de propagation aux conséquences non-linéaires et difficilement anticipable. Il est très difficile de définir avec précision les effets d'une défaillance localisée, sur l'ensemble des composants et des fonctions du système.

Plusieurs hypothèses sont à la base du modèle HRO :

1. **Les HRO sont des systèmes à hauts-risques :** la possibilité de conséquences catastrophique est nécessaire pour faire émerger la haute fiabilité.
2. **Les HRO sont des systèmes complexes :** il n'est pas possible, et pour aucun des acteurs, de comprendre le système dans sa globalité et sa précision. Il n'est pas possible d'anticiper de manière exhaustive son comportement.

DESCRIPTION DU MODELE

Selon Lekka (2011), la majorité des contributions relatives aux organisations hautement fiables proposent une riche description qualitative des processus et des caractéristiques identifiés dans les cas étudiés. Ceux-ci sont résumés dans la carte suivante (Figure 22) :

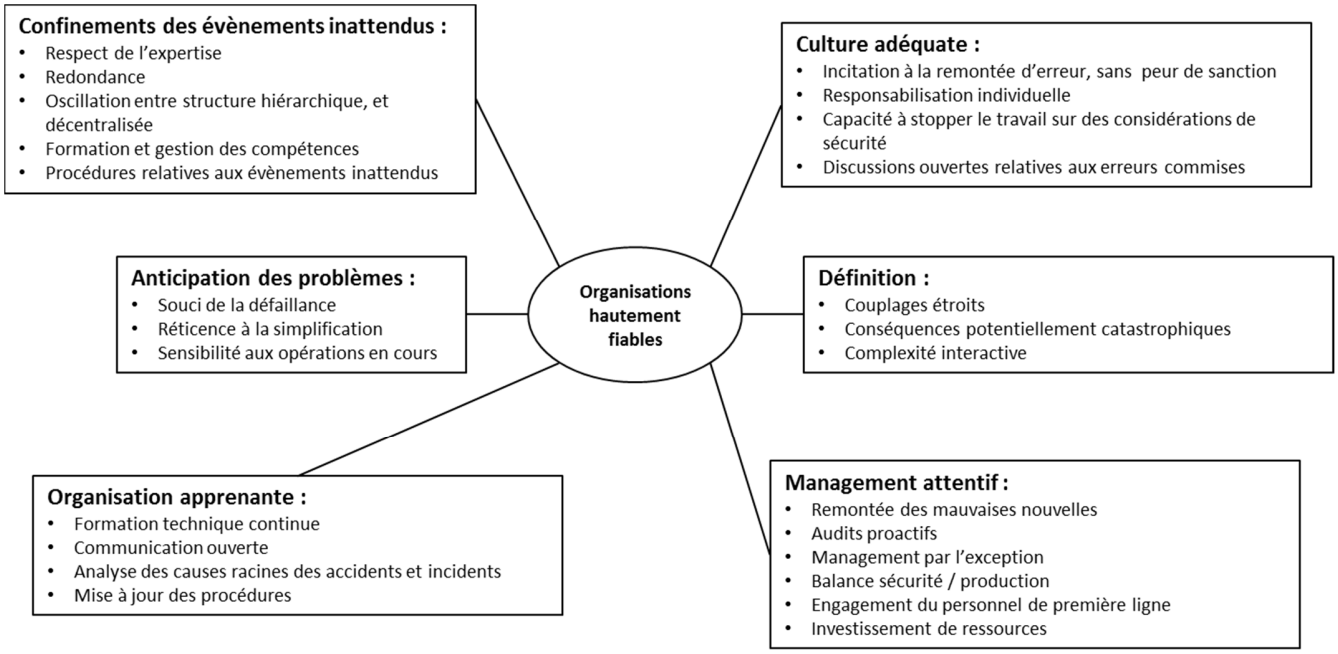


Figure 22 : Principaux processus et caractéristiques relatifs aux HRO, traduit de Lekka (2011)

Tel que précisé précédemment, la pensée des organisations hautement fiables s'articule autour de deux courants en concurrence. Selon Sutcliffe (2011), des performances « hautement fiables » s'obtiennent grâce à la prévention des accidents, et la résilience du système.

La logique de prévention :

Selon l'auteur, la prévention, ou l'anticipation requièrent que les membres de l'organisation identifient l'ensemble des scénarios accidentels, et définissent des procédures pour éviter leur occurrence. De cette perspective, la fiabilité dépend de l'absence de variance non-souhaitée de la performance. Cela est obtenu par le développement de routines et de procédures opératoires très standardisées, et régulièrement actualisées. Selon Sutcliffe, cet engagement dans la prévention a des avantages : réduction des incertitudes, de la quantité

d'information à gérer par opérateur, des trous de mémoire, des erreurs de jugement, des biais personnels, fournit un levier d'apprentissage, protège l'opérateur, réduit les modifications non largement disséminées, et permet la mise en œuvre de procédure de gestion du changement et d'actualisation des règles. Mais cette logique de prévention a des limites. Et le respect des procédures ne garantit pas la sécurité du système. En effet, il n'est pas possible d'anticiper tous les scénarios, dans toutes les conditions de travail. Et même si cette exhaustivité existait, elle générerait une complexité liée à l'excès de règle. En outre, cette complexité limiterait la flexibilité des opérateurs et leur capacité d'adaptation à des situations de surprise. La logique de prévention est nécessaire, mais limitée. La haute fiabilité requiert également la résilience du système.

La logique de résilience :

Selon Sutcliffe, la résilience est la capacité intrinsèque d'une organisation (équipe, unité, système...) à rester, ou revenir, à un état de stabilité dynamique, qui permette la poursuite des opérations dans un environnement de stress continue, ou après un incident. La résilience implique trois capacités : 1/ la capacité à absorber la pression, et à préserver les activités malgré l'adversité ; 2/ la capacité à rebondir à la suite d'un évènement fâcheux ; 3/ et la capacité à apprendre des expériences passées. Ainsi, les organisations se distinguent par leur capacité à prévenir et gérer les incidents avant qu'ils se propagent dans le système.

Les attributs des HRO :

Les HRO se distinguent par les efforts d'organisation mis en œuvre pour augmenter la conscience qu'ont les opérateurs du système, et ainsi être capable de détecter le plus précocement possible les évolutions contextuelles, et les effets induits sur le système. Roberts et Rousseau (1989) ont défini huit caractéristiques que possèdent les HRO. Si d'autres organisations peuvent en posséder certaines, les HRO les manifestent toutes :

- **Une hypercomplexité :** les systèmes possèdent une très grande variété de composants, de sous-systèmes et de niveaux.
- **Des couplages étroits :** les systèmes étroitement couplés possèdent des interdépendances réciproques entre les niveaux et unités, des dépendances temporelles entre les processus, des séquences invariantes, (l'opération B doit suivre l'opération A), une conception globale qui impose une seule manière d'atteindre les objectifs, et peu d'interstices dans des processus de production continus.

- **Une différentiation hiérarchique extrême, mécanismes de contrôle et de régulation élaborés :** de multiples niveaux hiérarchiques avec pour chacun des mécanismes de contrôle et de régulation propres.
- **Une redondance :** plusieurs décideurs et un système d'information complexe, caractérisé par une redondance dans l'émission et le contrôle des informations. En lien avec le principe de la variété requise, les systèmes hypercomplexes nécessitent des capteurs, mécanismes de contrôle et unités opérationnelles au moins aussi complexe que le système qu'ils régulent.
- **Un haut degré de responsabilité :** les écarts aux normes et procédures de fonctionnement peuvent avoir des conséquences catastrophiques. Dans ce contexte, le respect des procédures est vérifié en permanence.
- **Des feedback immédiats :** des prises de décision rapides et des feedback immédiats. Les temps de latence entre la décision et le feedback sont réduits au maximum afin de limiter les incertitudes entre deux situations.
- **Un facteur temps réduit :** les activités et temps de cycle sont mesurés en secondes.
- **Des conséquences critiques simultanées :** plus d'une conséquence critique peut se produire simultanément, à cause de la complexité des activités et l'incapacité à modifier ou retirer une décision opérationnelle déjà engagée.

En complément de ces huit propriétés, Roberts et Rousseau définissent également trois particularités relatives aux HRO :

- **L'invisibilité :** les HRO sont invisibles jusqu'à ce que l'accident se produise. A cet instant, le client, ou la société demandent des modifications dans l'organisation pour ne plus qu'un accident ne se reproduise plus. En comparaison, le même accident au sein d'une organisation qui n'est pas hautement fiable n'est pas remis en cause de la même manière par le public, notamment parce qu'elle ne cause pas de dommages aussi catastrophiques.
- **Des activités à la limite de la capacité humaine :** les HRO poussent les opérateurs aux limites de leurs capacités, en se fiant à un entrainement continu et des rotations fréquentes. Cette tendance est liée à la demande des systèmes de développer leurs capacités et leurs productivités en augmentant le nombre d'activités, sans augmenter le nombre de personnels.

- **Plusieurs sous-groupes aux intérêts différents :** les concepteurs, qui n'ont souvent pas conscience des limites humaines dans l'exploitation de tels systèmes ; les opérateurs et managers, qui gèrent des technologies auxquelles ils n'ont pas pris part au développement ; enfin les décideurs stratégiques (actionnaires…) sont un autre sous-groupe du système.

LA PRODUCTION DE SECURITE

Sutcliffe propose huit processus d'organisation, qui peuvent conduire à faire émerger une haute fiabilité du système : *High reliability Organizing.*

1. **Interactions respectueuses :** Les interactions respectueuses sont nécessaires pour une compréhension partagée de la situation. La combinaison de confiance, honnêteté et respect mutuel augmente la probabilité que les personnes parlent de leurs inquiétudes, partagent leurs représentations et échangent des interrogations.
2. **Relations interpersonnelles attentives :** Les interrelations attentives sont un process social ou les actions individuelles contribuent à un plus large modèle d'actions partagées, et dans lequel chaque action individuelle est à l'image du modèle d'action général. Lorsque des personnes interagissent attentivement, ils comprennent tout d'abord la configuration et les objectifs du système, ainsi que le rôle de leur contribution. Deuxièmement, ils voient comment leur travail s'articule avec le travail des autres, dans l'atteinte de l'objectif du système. Troisièmement, ils conservent une conscience des 2 paramètres précédents, tant qu'ils accomplissent leurs devoirs. Les interactions respectueuses et les interrelations attentives génèrent des représentations et actions partagées et forment les fondations relationnelles d'une organisation hautement fiable.
3. **Pratiques organisationnelles :** En complément des deux éléments précédents, un troisième paramètre est nécessaire. La fiabilité d'une organisation dépend également de la capacité des acteurs à prendre en compte les problèmes le plus tôt possible, et à les résoudre avant qu'ils ne prennent de l'importance. L'organisation met en œuvre des process et pratiques dont le but est : 1/ d'examiner une défaillance comme une atteinte à la santé du système. 2/ éviter les hypothèses simplificatrices sur le monde. 3/ Etre sensible aux opérations en cours et leurs effets. 4/ Développer la résilience dans le but de gérer des évènements non prévus. 5/ Comprendre et

localiser les expertises et mécanismes de créativité pour la décision, afin de migrer vers ces experts en cas de nécessité.

4. **Préoccupation pour la défaillance :** La préoccupation pour la défaillance est une prudence continue qui conduit l'analyse proactive et préventive des vulnérabilités et menaces possibles. Chaque défaillance ou presqu'accident est un indicateur de plus larges problèmes potentiels. Cela signifie que chaque acteur de l'HRO porte une grande attention à identifier ce qui doit se passer correctement, ce qui pourrait ne pas aller, comment cela pourrait mal se passer, et ce qui s'est réellement mal passé. Les acteurs sont sensibles aux signaux faibles et aux surprises. Les HRO mettent en œuvre une amélioration continue, une réévaluation permanence et une crainte des routines.
5. **Eviter les interprétations simplificatrices :** Les HRO évoluent dans un environnement complexe, et la représentation d'une situation par les acteurs est une tâche mentale également complexe. Un système technique complexe possède plus de variations qu'un Homme peut l'imaginer. Les acteurs ont alors souvent tendance à aborder une tâche difficile en simplifiant la manière par laquelle ils interprètent la situation. Cependant, ces simplifications peuvent être génératrices de troubles parce qu'elles donnent une représentation erronée de la réalité à laquelle ils font face. Cela limite leur capacité d'imagination des conséquences indésirables possibles, et les précautions prises. Pour compenser, les acteurs mettent en œuvre plusieurs stratégies. 1/ Stratégie d'humilité : les acteurs savent qu'ils ne savent pas, mais ne savent pas ce qu'ils ne savent pas. 2/ Stratégie de prudence : ils restent en alerte permanente, et ne prennent aucune situation pour définitivement acquise. 3/ Stratégie d'échange : la confrontation d'interprétation de la situation entre différents membres d'équipes et de réseaux divergents permet d'imaginer plus de situations possibles qu'une seule équipe homogène.
6. **Garder une sensibilité aux opérations en cours :** Garder une sensibilité aux opérations en cours signifie se représenter et maintenir une image globale de la situation actuelle, à travers une attention/veille sur les informations nouvelles en temps réel. Cette « conscience situationnelle » de chaque acteur permet de détecter des problèmes naissants et d'apporter des ajustements immédiats, ce qui évite potentiellement la génération de situations indésirables plus impactantes.
7. **Cultiver la résilience :** Un engagement vers la résilience implique un élargissement continu des capacités de récupération d'évènements non anticipés. De telles

capacités incluent : meilleure amélioration des compétences, apprentissage, diversification des tâches et adaptation. Les HRO dépensent beaucoup de temps à améliorer leur capacité d'anticipation, et rédigeant, améliorant et révisant les plans et procédures en intégrant les leçons des retours d'expériences. Cependant, les HRO savent qu'elles ne peuvent anticiper toutes les situations, et ne peuvent réduire toutes les incertitudes. Elles cherchent à développer des capacités de gestion des évènements surprenants et non-anticipés dès qu'ils surviennent. Les capacités de résilience sont le résultat de la mise en œuvre de doctrine d'actions, construites à travers entrainements et simulations, une variété d'expériences, d'apprentissage des feedback négatifs et des réseaux adhoc. Cela autorise la mise en œuvre rapide de pool de compétences pour maitriser les évènements surprenants.

8. **Flexibilité des processus de décision :** Une dernière caractéristique des HRO est leur tendance à modifier les processus de prise de décision vers l'expertise quand les problèmes se matérialisent. En cas de situations inhabituelles, le système de décision hiérarchique traditionnel s'efface au profit d'un système en tandem avec des experts. Le rang hiérarchique est alors subordonné à l'expertise, ce qui augmente la capacité à générer de nouvelles solutions pour de nouveaux problèmes. L'organisation gagne ainsi en expérience, en compétence, et en capacité de récupération.

CRITIQUES DU MODELE DANS LA LITTERATURE

Plusieurs limites du modèle de haute fiabilité sont soulevées par Lekka (2011). Les recherches sur les HRO ont incontestablement révélé un nombre important de processus organisationnels jouant un rôle majeur dans la production de sécurité. Pourtant, nombres de questions restent sans réponse.

Selon l'auteur, la première et principale critique porte sur l'échantillon d'organisations analysé, à l'origine du modèle de haute fiabilité. En effet, celui-ci ne comptent qu'un petit nombre d'organisation, seulement trois. De plus, ces organisations appartiennent à des milieux aux cultures spécifiques (militaire, contrôle aérien). Dans ce cadre, l'efficacité de la transposition des processus de haute fiabilité à d'autres types d'organisation, plus communes, tel que le médical, n'est pas démontré.

La deuxième critique porte sur le cadre conceptuel sous-jacent au modèle de haute fiabilité. Selon l'auteur, le champ de recherche des HRO manque d'un cadre théorique exhaustif qui expliquerait la capacité des HRO à maintenir un niveau élevé d'efficacité, là où d'autres organisations échouent. Il existe encore aujourd'hui un manque de connaissance sur le lien entre les processus organisationnels spécifiques à la haute fiabilité et les performances sécurité.

La troisième limite définit par Lekka porte sur le lien entre l'anticipation et la résilience. En effet, les HRO semblent combiner deux qualités importantes qui leur permettent des performances élevées. Ces deux qualités sont la capacité à anticiper d'une part, et à faire face d'autre part, aux évènements non-prévus qui peuvent arriver. Ces deux qualités s'appuient sur l'hypothèse sous-jacente qu'il est possible d'identifier et d'anticiper les possibles scénarios accidentels, et de définir et de mettre en œuvre dans le temps de réaction imparti une réponse opérationnelle adéquate à l'évitement de la catastrophe. Cette hypothèse se confronte aux récentes recherches démontrant l'existence d'un environnement organisationnel imprévisible, au sein duquel anticipation et prévention des défaillances en temps réel n'est pas possible. Cette contradiction pose la question de l'origine de la caractéristique de la haute fiabilité de l'organisation. Est-ce une propriété émergente de l'organisation, face à un environnement spécifique qui permette de conjuguer anticipation et résilience, ou est-ce une propriété intrinsèque particulière du fonctionnement de l'organisation qui lui permet de gérer l'imprévu, et ce dans tous les contextes ?

La quatrième limite concerne l'impact de la haute fiabilité organisationnelle, sur le niveau individuel de l'organisation. Selon l'auteur, les contextes très structurés et contraignants des organisations industrielles à risques ne sont pas ceux qui permettent le plus d'autonomie, de participation, de développement personnel et d'implication des employés. Pourtant, les retours d'expérience montrent des comportements différents des opérateurs de ceux « naturels », dans des situations stressantes et dangereuses. Très peu de recherches ont étudié l'impact d'une culture HRO au niveau individuel, et la manière dont les opérateurs se l'approprient. Des avancées dans ce domaine auraient des implications importantes pour la mise en œuvre de la culture HRO dans des organisations plus traditionnelles.

Enfin, une dernière limite des HRO concernent leur opérationnalisation. Comment implémenter les HRO en pratique ? Les études portant sur la haute fiabilité sont davantage descriptives, qu'explicatives. C'est-à-dire qu'elles ne permettent pas d'identifier les processus organisationnels sous-jacents avec précision, les prérequis et les conditions

contextuelles nécessaires, la manière de maintenir un niveau élevé de performance à long terme, et enfin la méthodologie nécessaire à la mesure de la haute fiabilité, et de son évolution.

La migration des activités du système
J. Rasmussen (1997)

SYNTHESE

Selon Rasmussen, l'accident est le résultat de la migration des activités du système, hors des frontières de la performance acceptable. Sous la contrainte de pressions économiques, les barrières de sécurité s'affaiblissent de manière systémique, préparant les conditions de l'accident. La sécurité est alors le résultat du contrôle du comportement du système, en augmentant les marges de sécurité, explicitant les limites acceptables, et en développant les compétences de rattrapages aux abords de ces limites.

CONTEXTE

La société actuelle est dynamique, et présente des conditions d'instabilité qui impactent la manière dont le risque industriel est classiquement géré. L'auteur avance les tendances suivantes :

- **Des évolutions rapides dans la plupart des domaines technologiques** (transport, industrie...). Ces changements surpassent les capacités d'adaptation réglementaires et normatives, générant des « lags » à tous les niveaux du système.
- **Une augmentation constante du potentiel industriel**, et donc des possibilités d'accidents majeurs associées.
- **Un développement rapide des technologies de l'information et de la communication**. Elles génèrent un niveau d'intégration et de couplage de plus en plus importants entre les systèmes industriels.
- **Le développement d'un environnement économique compétitif et agressif**. Il impose au décideur une gestion fondée sur des résultats à courts termes, plutôt que sur la prise en compte d'objectifs de long terme, comme celui de la sécurité industrielle.

Ces évolutions poussent à remettre en cause le traitement disciplinaire des problématiques de gestion des risques industriels. En effet, chaque composante du système, de l'opérateur au gouvernement, peut être étudiée séparément par un champ scientifique particulier. La modélisation est alors effectuée par une généralisation à partir d'un point de vue particulier.

Cependant, Rasmussen considère la gestion des risques comme un problème transdisciplinaire, considérant son management comme un problème de contrôle. L'approche transdisciplinaire doit être à l'origine de la modélisation de la structure de contrôle, et impliquer chaque niveau de la société.

Ainsi, les conséquences humaines, économiques et environnementales liées à un accident majeur sont le résultat d'une perte de contrôle d'un processus physique à risques. Le déroulement d'une séquence accidentelle est modelé par les acteurs du système, qui peuvent déclencher, ou empêcher la phase accidentelle. La sécurité dépend donc de la capacité du management à contrôler les activités de travail, et les process dangereux associés, et éviter ainsi les conséquences néfastes des pertes de contrôle.

HYPOTHESES DU MODELE

La modélisation de Rasmussen repose sur plusieurs hypothèses :

- **Le recours aux approches transdisciplinaires est nécessaire**. Les systèmes industriels sont des systèmes sociotechniques complexes, au sein duquel de nombreux niveaux décisionnels sont impliqués dans la production de sécurité (Figure 23). Dans ce cadre, l'approche prescriptive classique de contrôle fondée sur une déclinaison verticale des règles, efficace dans une société stable, est inefficace au sein de systèmes dynamiques. En effet, la décomposition structurelle classique (fondée sur la décomposition, et l'analyse des comportements comme un flux d'évènements) ne prend pas en compte la contingence contextuelle, et les degrés de liberté associés à chaque tâche.

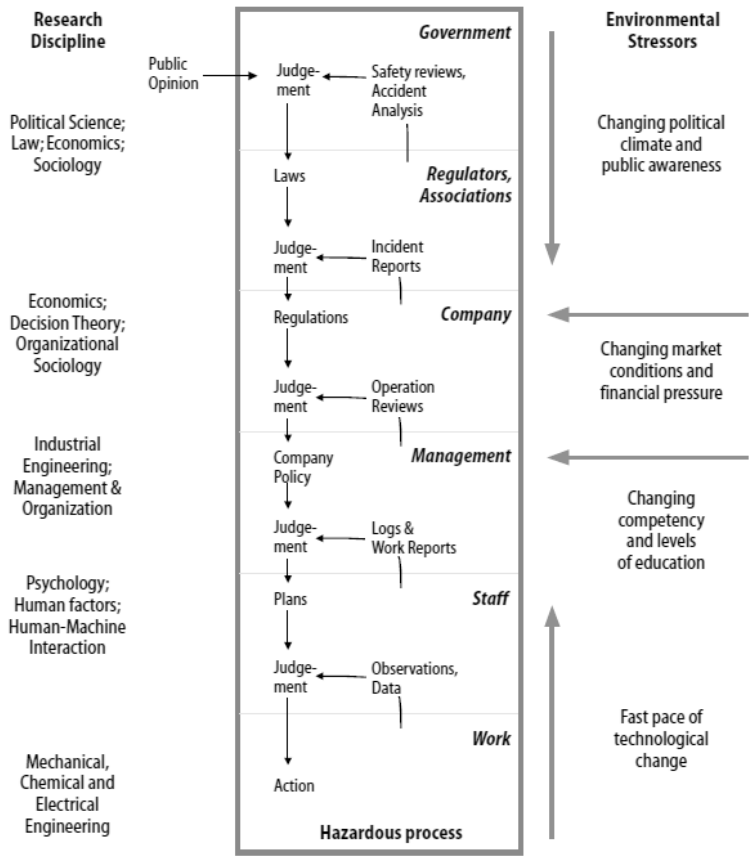


Figure 23 : Modélisation d'un système sociotechnique complexe, tiré de Rasmussen et al. (2000)

- **Il est possible d'identifier les limites de performance acceptable du système.** Selon l'auteur, l'accident arrive parce que le système se situait dans une zone de fonctionnement de non-sécurité. Il a migré au-delà des limites de fonctionnement acceptable. Il existe donc au moins deux zones de fonctionnement : une zone de performance acceptable, et une zone non-acceptable. Ces deux zones sont délimitées par des frontières. Définir la migration du système nécessite alors de connaitre les périmètres associés à chaque zone, et les limites à ne pas franchir pour un fonctionnement sûr.

DESCRIPTION DU MODELE

Selon Rasmussen, un accident est la conjonction de deux facteurs. Le premier concerne les pressions économiques et productives, qui poussent le système hors des limites de performance acceptable. La sécurité est une contrainte qui s'efface au cours du temps. La multiplication des écarts et ajustements locaux conduisent à une suppression des marges de sécurité, et une dégradation systémique de l'ensemble de la défense en profondeur. Le second facteur est celui de l'inefficacité du contrôle du système. Le management n'a pas été capable de détecter la migration en cours, au regard des performances du système. En conséquence, celui-ci n'a pas été en mesure de modifier la gestion du système pour revenir à un état de fonctionnement permettant un niveau de performance satisfaisant du point de vue de la sécurité. La figure suivante propose une schématisation de ce modèle, selon l'auteur (Figure 24).

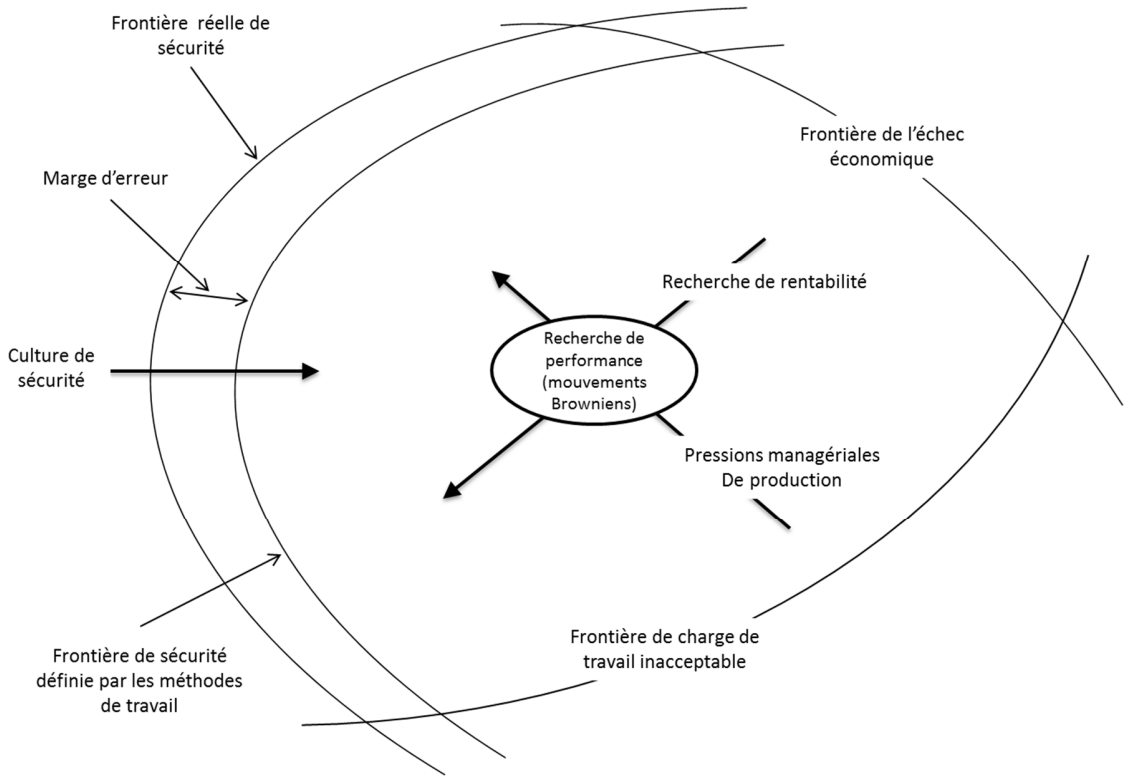


Figure 24 : Migration du système au-delà des limites de performance acceptable, adapté de Rasmussen (1997)

Dans ce modèle, à l'opposé des stratégies classiques fondées sur la suppression des causes d'erreur humaine, la sécurité du système repose sur trois piliers :

- L'identification des limites de performance acceptable, en matière de sécurité.
- L'explicitation de ces limites pour les décideurs.
- La lutte contre les pressions qui poussent le système au-delà des frontières de l'enveloppe acceptable.

LA PRODUCTION DE SECURITE

La gestion des risques doit être considérée comme une fonction de contrôle, focalisée sur le maintien d'un système de production dangereux dans les limites d'un fonctionnement acceptable. Le mode de gestion doit alors passer d'un contrôle pré-planifié, dans lequel tous les comportements du système sont définis, analysés et prévus (un canon), à un mode de gestion fondé sur la rétroaction et le pilotage (un missile). En effet, le second mode est plus à-même de prendre en compte les perturbations non-prévues, comme les pressions commerciales liées aux évolutions du marché. Rasmussen propose une démarche de définition de la fonction de contrôle associée à un risque particulier, au regard d'une taxinomie des risques définie par l'auteur. Elle est modélisée selon la figure suivante (Figure 25).

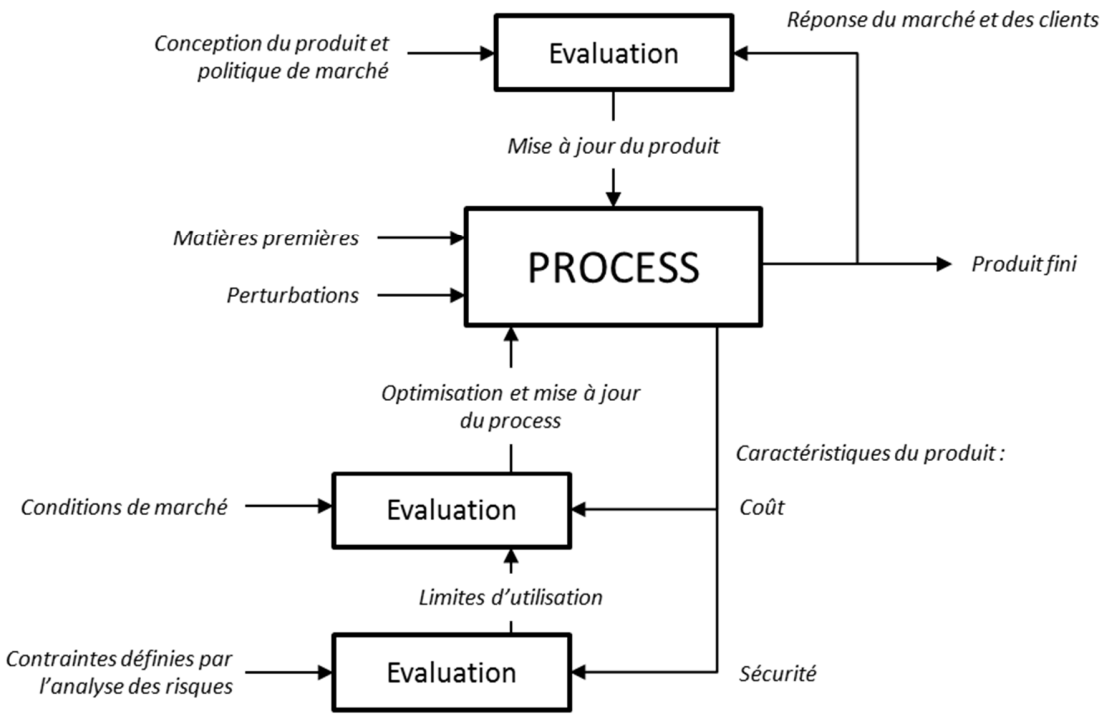


Figure 25 : Système de contrôle adaptatif connectant la production, la sécurité, et l'économie, traduit de Rasmussen et al. (2000)

L'auteur propose alors une démarche permettant la conception d'un système de management proactif des risques, comprenant les étapes suivantes :

- Identifier les acteurs et les décideurs impliqués dans le contrôle du processus de production, à tous les niveaux pertinents du système socio-technique.
- Identifier le périmètre d'activités sous leur contrôle, et les critères guidant l'allocation des responsabilités et ressources affectées à chaque contrôleur.
- Identifier la structure du système de contrôle distribuée, c'est-à-dire le réseau de communication existant entre les décideurs.
- Identifier le contenu des flux d'information entre les décideurs (cibles à atteindre, états du système...).
- Identifier la sensibilité aux risques (awareness) des décideurs (contenu et formes des informations).
- Identifier la compétence des décideurs au contrôle d'activités à risques.
- S'assurer de l'engagement des décideurs à la sécurité du système.

CRITIQUE DU MODELE

Le Coze (2013) propose une lecture critique des travaux de Rasmussen. Les modèles combinés du système sociotechnique complexe, et de la migration du système, ont plusieurs forces :

- Ils démontrent l'importance d'aborder les problèmes de sécurité industrielle avec une démarche interdisciplinaire et fonctionnelle.
- Ils caractérisent la notion de variabilité et d'adaptation d'une organisation dans son environnement, et formalisent l'idée d'exploration des limites de la zone de performances et de sécurité.
- Ils mettent l'accent sur l'aspect dynamique des systèmes socio-techniques, et leurs évolutions sous les contraintes externes.
- Ils mettent en perspective la notion d'erreur et de défaillance avec celle de variabilité et d'adaptation des opérateurs et des managers.
- Ils introduisent l'idée d'une auto-organisation des systèmes, qui permet une compréhension précise de la manière dont une situation peut dériver hors des limites de contrôle centralisé.
- Ils montrent la nature distribuée du problème de gestion de la sécurité, en localisant le rôle des différents acteurs, dans le temps et dans l'espace.
- Ils suggèrent une analogie intuitive et très illustrative entre cognition et organisation.

Selon le même auteur, ces deux modèles combinés ont également des faiblesses :

- Ils impliquent une vision hiérarchique du système socio-technique complexe, au sein duquel les autorités semblent avoir un contrôle top-down sur l'ensemble du système. C'est un aspect actuellement questionnable.
- Ils laissent implicite l'idée que les flux d'information sont en principe cybernétiques, et de nature séquentielle. Ils ne mentionnent pas la possibilité de flux directs entre les niveaux hauts et bas, et la présence possible de filtres entre les différents niveaux.
- Ils font l'hypothèse qu'il existe une réelle frontière des performances sécurisées, qui peut en principe être définie, et représentée par une ligne.

- Ils n'expliquent pas la manière de faire interagir les différentes disciplines scientifiques entre elles.
- Ils ne fournissent aucune information à propos des fonctions d'un système de management de la sécurité d'un système industriel.
- Ils suggèrent, plutôt que de distinguer analytiquement, les dimensions de l'organisation qui doivent être suivies.

La gestion de la sécurité dans les systèmes de production
A.R. Hale (2003)

SYNTHESE

Selon Hale, la sécurité est le résultat d'une conception robuste fondée sur une défense en profondeur, et un système de gestion de la sécurité efficace. Sur la base de limites identifiées dans la littérature, l'auteur propose un mode de gestion fondée sur le contrôle du risque, et adapté aux activités spécifiques du système, et à sa taille. Il propose une discussion des connaissances relatives au management de la sécurité autour de quatre catégories : connaissances certaines, erronées, ignorées, et sous-estimées.

CONTEXTE

Selon Hale, durant les dernières décades du XXème siècle, la sécurité industrielle a été un objet d'intérêt scientifique prégnant. L'accident a d'abord été compris comme le résultat de déviations techniques et humaines, que les organisations devraient prédire, et contrôler. La sécurité a alors été construite autour de deux principes : une conception robuste fondée sur une défense en profondeur, et l'instauration d'un système de management de la sécurité efficace.

En outre, l'analyse des accidents majeurs de ces dernières décennies à remis en cause l'encadrement réglementaire des activités industrielles à risques. Les règlementations prescriptives, détaillées, et spécifiques à une activité, ont fait place à une obligation de résultat. La pression est mise sur l'entreprise, qui doit développer son propre système de gestion de la sécurité, le mettre en œuvre, et évaluer son efficacité. Le rôle de l'autorité de régulation est alors de contrôler le système de gestion de la sécurité, qui apparait comme un proxy satisfaisant de la mesure du niveau de risque réel.

De nombreuses questions de recherche ont alors émergé sur la manière dont les systèmes de management de la sécurité devaient être développés, structurés, évalués, et améliorés (Delatour et al, 2014a). Des connaissances nouvelles ont permis de mieux comprendre ce que devait être un bon système de management de la sécurité. Pourtant, selon Hale, celles-ci sont encore lacunaires, et leur cohérence doit être questionnée.

HYPOTHESES DU MODELE

Hale met en avant trois limites sur la manière dont les connaissances relatives à la gestion de la sécurité industrielle sont construites et utilisées :

- **Des modèles de gestion de la sécurité inadaptés aux organisations industrielles productives :** les approches rationnelles issues d'une culture technique s'appuient sur l'idée que le SGS doit être conçu parfaitement. Son rôle est de détecter, et de corriger des déviations vis-à-vis d'un modèle de fonctionnement idéal. C'est une vision utopique de l'entreprise, constamment soumise à des pressions issues de son environnement. Le modèle de gestion doit être dynamique, et intégrer les signaux d'anticipation des risques. Il est de plus impossible de prévoir l'ensemble des risques, et de leurs effets dans le système. La notion d'apprentissage est donc nécessaire dans un SGS efficace.
- **Un excès de généralisation de la connaissance produite :** les connaissances produites en matière de gestion de la sécurité sont disparates, et parcellaires. Les études scientifiques portent sur des objets précis, par exemple, la manière dont les SGS sont appliqués en entreprise. Celles-ci sont alors généralisées, pour proposer des bonnes pratiques, pour tous les types d'organisation. Selon l'auteur, en procédant ainsi, on omet un certain nombre de spécificités dans la gestion de la sécurité, liées au type d'activité mis en œuvre, et au niveau de bureaucratisation de l'entreprise. Les connaissances produites doivent être périmétrées, et reprécisées.
- **Un détournement de la connaissance disponible :** en matière de gestion de la sécurité, les évolutions des pratiques en entreprises sont davantage liées à des effets de modes, et à des discours types de consultants, plutôt qu'à l'amélioration des modèles issus de réflexions scientifiques. Une pratique qui fonctionne dans une entreprise, sera transposée, à l'aide d'un benchmark, sans tenir compte des spécificités liées aux deux entreprises, sources et cibles. En conséquence, les SGS se construisent sur l'agrégation, et deviennent de plus en plus complexes. Il est alors plus difficile de comprendre leur périmètre de contrôle et d'action.

DESCRIPTION DU MODELE

Selon Hale, la sécurité est le résultat d'une conception robuste fondée sur une défense en profondeur, et un système de gestion de la sécurité efficace. Dans ce cadre, le système de gestion de la sécurité a pour rôle de maintenir l'ensemble des défaillances identifiées à leur plus bas niveau de probabilité, de supprimer ou réduire les scénarios potentiellement accidentels, et de fournir un contrôle robuste des activités industrielles.

Selon l'auteur, les modèles de gestion doivent être déclinés selon les spécificités du système, au regard de deux critères au moins : le type d'activité mis en œuvre, et le niveau de bureaucratisation de l'entreprise. Par exemple, médical et nucléaire ont des fonctionnements différents, et pme et groupes industriels ont des schémas décisionnels très éloignés.

A l'image du modèle de Rasmussen, Hale propose une échelle descriptive des niveaux de pilotage du système industriel. Celle-ci est composée de 3 niveaux : structure et politique, planification et procédures, réalisation du contrôle des risques (Figure 26).

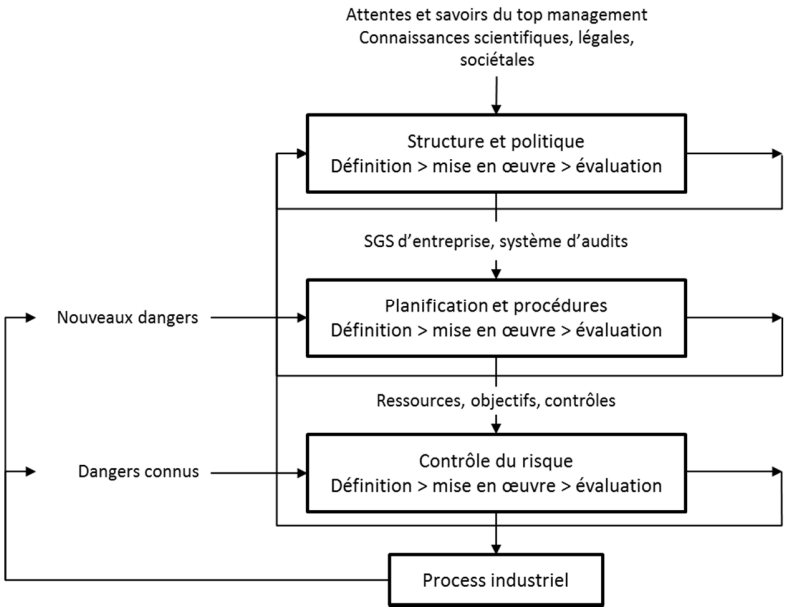


Figure 26 : La gestion de la sécurité, comme résolution d'un problème à trois niveaux, traduit de Hale (2003)

Le modèle de Hale s'appuie sur une catégorisation des connaissances disponibles en matière de gestion des risques industriels, et le rapport que nous avons à cette connaissance. Il définit quatre champs de savoir :

- **Les connaissances certaines :** ce que nous savons, de manière sure. Celles-ci concernent la structure du système de gestion de la sécurité, et les systèmes d'audit et de régulation.
- **Les connaissances erronées :** ce que nous pensons savoir, mais dont ce n'est pas le cas. Ce sont les connaissances issues d'excès de généralisation de la part des scientifiques. Elles concernent la typologie des évènements redoutés, de l'incident à l'accident majeur, l'inventaire des risques, le fonctionnement du SGS, et l'accidentologie.
- **Les connaissances ignorées :** ce que nous savons que nous ne savons pas. Ce sont les connaissances inconnues, et qui doivent faire l'objet de projets de recherche scientifique. Elles concernent la culture sécurité et l'apprentissage organisationnel, les processus de développement et de maturation des SGS, la prise en compte des systèmes multi-organisationnels, et la visualisation de la complexité.
- **Les connaissances sous-estimées :** les besoins en connaissance que nous refusons de voir. Ce sont les connaissances qui font l'objet d'un dénie d'intérêt compte-tenu de leur apparente faible pertinence. Elles concernent la notion de conflit sécurité/production dans le pilotage des activités à risques, le rôle des émotions dans la prise de décision, et les processus de changement organisationnel.

LA PRODUCTION DE SECURITE

Au regard des types de connaissances définis précédemment, Hale propose une production de sécurité fondée sur trois aspects :

Le premier aspect est celui de la mise en œuvre de bonnes pratiques relative à la structure du SGS, et à son mode de pilotage. Selon l'auteur, un SGS efficace doit être structuré avec les fonctions suivantes :

1. Une compréhension claire du processus de production primaire, et des scénarios accidentels associés. Le SGS doit s'appuyer sur l'évaluation des risques, et être adapté aux activités et à la taille de l'entreprise.

2. L'analyse et la gestion des risques doit s'appuyer sur un modèle de cycle de vie, considérant toutes les étapes du système : conception, installation, utilisation, maintenance... Le modèle de pilotage doit comprendre des boucles de rétroaction (Figure 27) :

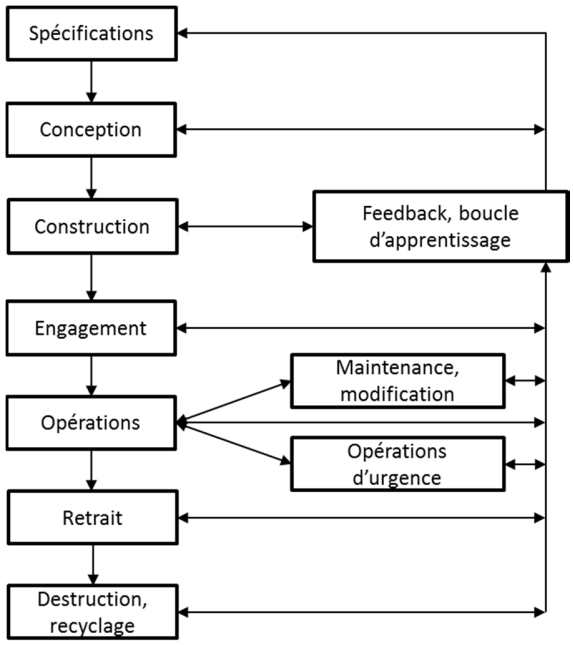


Figure 27 : Le cycle de vie de la gestion de la sécurité, traduit de Hale (2003)

3. La gestion doit être abordée par une approche de résolution de problème cyclique intégrant l'identification, le contrôle, et le suivi des scénarios, aux trois niveaux de pilotage du système. Le système se décline en trois niveaux de pilotage, de temporalité différente. Le niveau inférieur porte sur la gestion opérationnelle du risque, et le management des unités au contact du processus de production. Le niveau intermédiaire porte sur la planification, la définition des procédures, l'allocation des ressources, et l'optimisation du contrôle. Le niveau supérieur définit la structure et la politique relative à la gestion des risques.

4. Le mode de gestion doit comporter des boucles de suivi et de pilotage, à chacun des trois niveaux. Des indicateurs de performance doivent déclencher des ajustements à tous les niveaux du système.

5. Le niveau intermédiaire du système, en lien avec le niveau stratégique supérieur, doit délivrer les ressources et le contrôle nécessaires aux tâches opérationnelles critiques pour la sécurité du système (disponibilité, compétence, implication et motivation, communication, procédure, support technique, environnement de travail, gestion des conflits...).

Le lien entre ces points est représenté dans le schéma fonctionnel suivant (Figure 28):

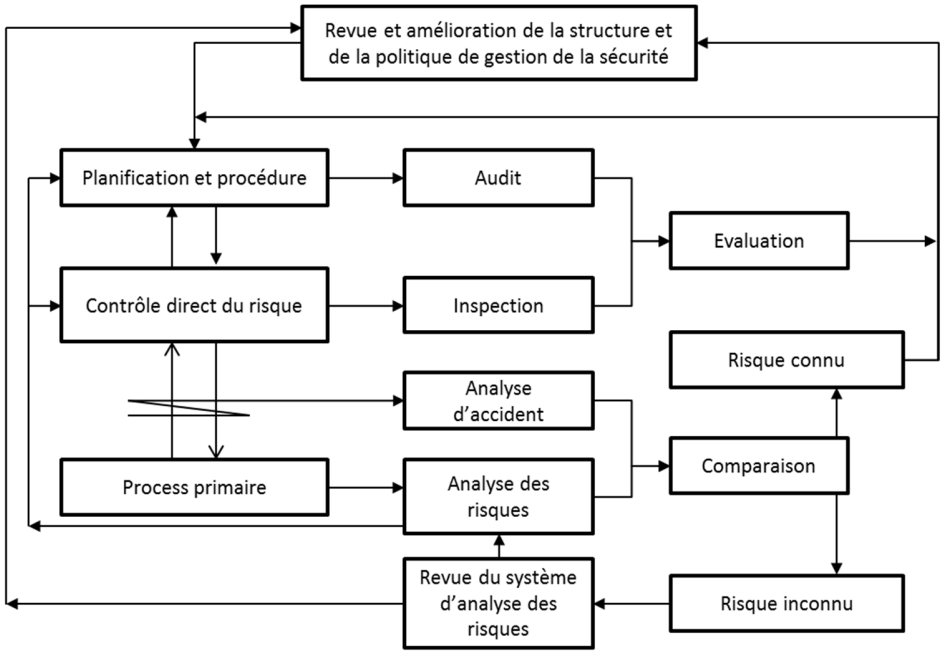


Figure 28 : Système de gestion de la sécurité, résolution de problème et feedback, traduit de Hale (2003)

Le deuxième aspect regroupe des alertes adressées aux concepteurs de SGS et aux managers, sur la manière dont ils mettent en œuvre la gestion de la sécurité. Ce sont des

actions considérées par la majorité comme efficace, mais remises en question par l'auteur. Ces alertes concernent :

- Les modèles d'analyse de risques : il existe une confusion entre l'inventaire des risques, et l'identification des scénarios d'accidents. Par exemple, l'utilisation de check-lists de risques dans les PME ne permet pas d'identifier les voies d'accident possibles, et n'est pas suffisamment précis pour définir une planification efficace de la gestion des risques.
- Les typologies d'accidents : de nombreux guide de gestion de la sécurité génèrent de la confusion sur l'interprétation du triangle d'Heinrich. La prévention des incidents et accidents mineurs ne réduit pas mécaniquement le risque d'accident majeur. Les scénarios relatifs à chacun des phénomènes sont de natures différentes.
- Le fonctionnement du SGS : si la structure d'un SGS efficace est assez bien connue, il existe très peu d'études sur son fonctionnement, et la manière dont il doit être mis en œuvre et modifié, pour être efficace. Définir une structure adéquate n'est pas suffisant pour garantir l'efficacité de la démarche de prévention.
- Les remontées et l'analyse des accidents : l'intérêt des démarches de retour d'expérience est reconnu par la plupart des praticiens. Pourtant, les meilleures volontés ne mènent généralement qu'à des démarches inachevées, du fait de la sous-estimation de la tâche à accomplir. De ce fait, la démarche permet à peine l'alimentation d'une base de données. Ce qui est bien loin de l'efficacité recherchée.

Le troisième aspect porte sur des questionnements proposés par l'auteur, et à prendre en compte lors de la conception d'un SGS, et plus largement dans la mise en œuvre d'une politique de gestion des risques industriels. Ces questions portent sur :

- La culture et l'apprentissage organisationnel : ces deux notions sont émergentes et encore débattues. Ils revêtent pourtant un positionnement central dans la gestion des risques. Mais leur opérationnalisation est encore ambiguë.
- Le développement du SGS : il semble probable qu'il existe une sorte de processus de maturation du SGS, qui ne peut être court-circuité sans impunité. Ce processus est encore méconnu, et n'existe qu'à travers le retour d'expérience des entreprises en pointe sur le sujet.

- Les systèmes multi-organisationnels : les démarches d'intégration organisationnelles se développent au sein de nombreux systèmes : intégration verticale et horizontale, coactivité au sein de plateaux commerciaux, ou de nœuds de communication... L'intégration des systèmes de sécurité semble montrer des résultats satisfaisant, et doit être étudiée plus profondément.
- La prise en compte de la complexité : la sécurité est un des aspects les plus difficiles à contrôler. Il faut anticiper chaque chance de chaque scénario accidentel. Une voie de progrès est la modélisation informatique d'un système de management. Les limites résident dans la visualisation de la complexité. Comment modéliser un SGS complet, et efficace ?
- Les conflits sécurité / production : la prise en compte de la notion de conflit est centrale pour le contrôle du risque. Au sein de la gestion de la sécurité, cette notion a plutôt été repoussée, afin d'éviter la posture d'opposition entre acteurs au sein de l'organisation. Pourtant, le dénie du conflit montre une faible culture de sécurité. Celui-ci doit être abordé explicitement.
- Le rôle des émotions dans la prise de décision : la conception des systèmes industriels est guidée par une analyse rationalisée et la recherche de solutions optimales. Pourtant, la question de gestion implique la perception des risques et la prise de décision. Les émotions y jouent un rôle majeur, et doivent être complètement intégrés aux réflexions relatives au management.
- Le changement organisationnel : le changement a longtemps été considéré comme un ennemi de la sécurité, parce qu'il modifie des systèmes de sécurisation éprouvés. La gestion des modifications techniques et organisationnelles a donc été pendant longtemps au cœur du SGS. Pourtant, l'anticipation rationalisée des conséquences d'une modification ne suffit pas à supprimer les risques. La question du changement organisationnel permanent doit être repensée, de manière plus subjective, et dynamique.

CRITIQUE DU MODELE

Les travaux de Hale s'inscrivent dans le courant naissant des « safety sciences », et constituent une contribution majeur de ce champ scientifique. Moorkamp et al. (2014) définissent le modèle de système de management de la sécurité de Hale comme une

approche de « minimisation de l'incertitude ». La sécurité est abordée comme le résultat de déviations qui doivent être supprimées, dans le but d'assurer un comportement organisationnel prévisible, stable, et sécurisé. Les auteurs opposent ainsi le modèle de Hale à celui de la résilience, défini comme une approche de « gestion de l'incertitude ». Selon Le Coze (2013), approcher les questions de sécurité à travers la modélisation d'un système de management de la sécurité, et de barrières de sécurité, est très efficace pour décrire, évaluer les risques présents dans une installation industrielle, et procéder à l'analyse d'accidents.

La principale critique des travaux de Hale concerne le type d'organisation au sein desquelles le modèle est pleinement efficace. Selon Moorkamp et al. (2014), Hale s'appuie sur une hypothèse implicite, qui limite fortement le champ des organisations cibles adaptées. Le modèle de SMS nécessite une organisation au fonctionnement stable et prévisible, afin de permettre la réalisation des longues boucles de contrôles, de manière complète, et à long terme. Ainsi, le modèle de Hale est approprié pour des organisations qui ne rencontrent que peu de variations de leur environnement. Celle-ci s'appuie sur la stabilité organisationnelle de leur structure pour agir. Dans ce type de système, la gestion de la sécurité est un instrument de contrôle de l'activité, qui doit rester positionné dans des limites prédéterminées. Hale reconnait lui-même cette limite, en indiquant qu'un modèle de sécurité efficace tend à devenir bureaucratique par nature (Hale, 2003).

L'ingénierie de la résilience en pratique
Hollnagel et al. (2010)

SYNTHESE

L'accident est vu comme le résultat de l'inadaptation d'un système à son environnement. Hollnagel décrit alors la résilience comme la capacité intrinsèque du système à ajuster son fonctionnement préalablement, pendant, ou consécutivement à un changement ou une perturbation rencontrée. L'ingénierie de la résilience s'appuie sur quatre capacités complémentaires à développer au sein du système : la capacité à faire face au réel, la capacité à anticiper les évolutions de l'environnement, la capacité à surveiller l'état du système, et la capacité à apprendre de l'expérience.

CONTEXTE

Selon Hollnagel (2011a), les approches traditionnelles de sécurité se sont principalement focalisées sur les évènements négatifs du système. L'attention est portée sur les choses qui vont mal, ou qui pourraient aller mal (défaillances, accidents...). Cette vision classique est illustrée par la définition habituellement donnée à la sécurité : l'absence de risques inacceptable. Ainsi, assurer un niveau de sécurité, c'est comprendre les causes de phénomènes redoutés pour s'en prémunir. En outre, cette approche est généralement formalisée à travers une matrice des risques. Elle caractérise le niveau de risque possible d'un évènement redouté selon deux critères : son niveau de probabilité d'apparition, et la gravité des conséquences possibles associées. Dans cette vision classique, la production de sécurité passe par la réduction de la probabilité et de la gravité d'un risque, jusqu'à un niveau acceptable.

Selon Hollnagel, cette approche de la sécurité a longtemps été efficace et suffisante pour des systèmes industriels gérables, au sein desquels le fonctionnement normal peut être maitrisé par la limitation des variations de performance. Cependant, elle est maintenant limitée, et nécessite d'être revue. Plusieurs tendances sont à l'origine de cette remise en cause :

1. Le dépassement des cadres d'analyse : depuis les années 1980, le management de la sécurité s'est focalisé sur les accidents, les incidents, et plus récemment les presqu'accidents. Mais aujourd'hui, ces derniers sont nombreux, très fréquents, et

ont des conséquences le plus souvent négligeables. Ils sont alors généralement laissés de côté lors de l'analyse.

2. Le rejet des évènements positifs : dû à une croyance erronée du fait que l'on a une meilleur connaissance des évènements négatifs qu'en étudiant seulement les évènements négatifs. Les évènements positifs sont rarement analysés.

3. Des systèmes industriels devenus complexes : ces vingt dernières années, le développement de systèmes sociotechniques génère un nombre grandissant de processus et d'activités difficilement gérables, et au sein desquels la variation de performance est devenue nécessaire pour s'adapter.

HYPOTHESES DU MODELE

Le modèle de résilience développé dans l'ouvrage d'Hollnagel et al. s'appuie sur deux hypothèses :

1. **Il est possible de définir et de catégoriser l'ensemble des résultats, positifs et négatifs, de l'activité d'un système :** l'approche classique du management de la sécurité prend en compte les résultats négatifs d'une activité : accident, incident, presqu'accident. Les auteurs proposent d'étendre le champ des conséquences possibles et d'intégrer les évènements positifs pour le système. Tel que décrit dans le tableau suivant (Tableau 8) il est possible de définir quatre types de résultats :

	Résultats recherchés (positifs)	***Résultats non recherchés (négatifs)***
Résultats avec une forte prévisibilité	Résultats normaux de l'activité du système, dans des conditions de sécurité.	Les résultats sérieux sont normalement éliminés du fait de la conception du système. Les résultats mineurs sont généralement tolérés (principe ALARP).
Résultats avec une faible prévisibilité	Résultats inespérés de l'activité du système.	Ils sont l'enjeu des analyses de risques. Ce sont les accidents et les incidents. Ce sont les résultats généralement associés à la sécurité.

Tableau 8 : Typologie des résultats possibles, traduit de Hollnagel (2011c)

2. **Les mêmes processus peuvent conduire à des résultats positifs et négatifs :** il n'existe pas de processus accidentel spécifique. Il est nécessaire d'analyser les résultats positifs et négatifs d'un système pour comprendre l'origine des défaillances. Selon les auteurs, il n'existe pas de processus « producteur d'erreur » spécifique qui s'active lorsqu'un accident est un train de se produire, ou encore qui reste dormant. Au contraire, il n'existe pas de différences fondamentales entre les processus qui mènent à la défaillance et ceux qui mènent au succès.

DESCRIPTION DU MODELE : INGENIERIE DE LA RESILIENCE

Face aux trois limites citées précédemment, la résilience aborde un positionnement différent. Elle est complémentaire à l'approche traditionnelle de la sécurité. A l'analyse des résultats des résultats négatifs du système (incident, accident...) est ajouté l'analyse des résultats positifs (tout se passe bien). Ces deux volets sont intégrés dans une approche globale de variation de la performance du système.

Hollnagel (2011a) décrit la résilience comme la capacité intrinsèque d'un système à ajuster son fonctionnement préalablement, pendant, ou consécutivement à un changement ou une perturbation. Cela lui permet de maintenir ses activités dans des conditions prévues et non

prévues. La sécurité est alors davantage que la seule gestion d'évènements redoutés. La résilience a pour finalité de rendre le système efficace et sécurité dans toutes ses conditions d'évolution. La sécurité vue regard de l'ingénierie de la résilience peut être illustrée avec le schéma suivant (Figure 29).

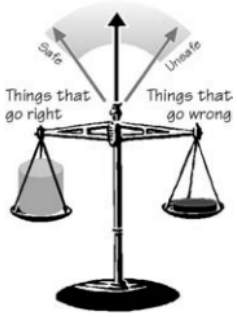


Figure 29 : La sécurité au prisme de l'ingénierie de la résilience, tiré de Rasmussen (2011)

Dans cette perspective conceptuelle, l'augmentation du niveau de sécurité d'un système est le résultat de deux stratégies complémentaires : la diminution des activités négatives, et l'augmentation des activités positives pour le système. Pour cela, la caractéristique clé d'un système résilient est sa capacité à ajuster son fonctionnement et ses performances. Chaque système doit être capable de s'adapter aux changements de son environnement, sous peine de disparaitre. Hollnagel (2011c) propose une typologie des ajustements possibles : les ajustements réactifs, concourants, et proactifs.

1. **Les ajustements réactifs :** ce sont les plus courants. Ils arrivent à la suite de conséquences d'un évènement négatif, tel qu'un accident, ou encore une rupture majeure. S'ils renforcent le système, ces ajustements ne garantissent pas sa sécurité et sa survie, et ce même si la réponse est rapide. Cela est dû au fait qu'un système ne peut répondre rapidement qu'à un nombre limité d'évènement prévues.

2. **Les ajustements concourants :** ce sont des ajustements réactifs rapides, et qui ont lieu alors que la situation est encore en cours de développement. C'est par exemple le cas de la montée en puissance d'un hôpital alors que l'accident est encore en cours.

3. **Les ajustements proactifs :** correspondent à des évolutions du système d'un état normal, vers un état de haute préparation, et la mise en œuvre des actions avant même que les perturbations aient lieu. Un état de haute préparation comprend une allocation particulière de ressources, l'activation de fonctions spécifiques, l'augmentation de défenses... Un exemple d'ajustement proactif est la mise en place des ceintures de sécurité dans un avion à l'approche de zones de turbulences. Cependant, et compte tenu de la complexité des systèmes, les indicateurs et les seuils de déclenchement des ajustements proactifs ne sont pas toujours aussi clairs que dans le cas de turbulences.

Selon Hollnagel, les ajustements proactifs sont les plus intéressants, parce qu'ils permettent une évolution du système dans des conditions maitrisées et pilotées. Le gain est cependant limité, du fait de l'incertitude associée à l'efficacité finale de la préparation, lors de l'apparition de l'évènement. En outre, la gestion des systèmes repose essentiellement sur le feedback. La non préparation d'un système peut rapidement conduire à une perte totale de contrôle.

LA PRODUCTION DE SECURITE : LES 4 PILIERS DE LA RESILIENCE

Selon Hollnagel, (2011a), l'ingénierie de la résilience a pour but d'insuffler la capacité de résilience dans un système. Celle-ci repose sur quatre pierres angulaires complémentaires et interdépendantes. Ces quatre propriétés sont couplées, dans le sens où elles s'alimentent entre elles, et une démarche d'ingénierie de résilience ne peut aborder chacune d'elles isolément. Elles sont illustrées dans le schéma suivant (Figure 30).

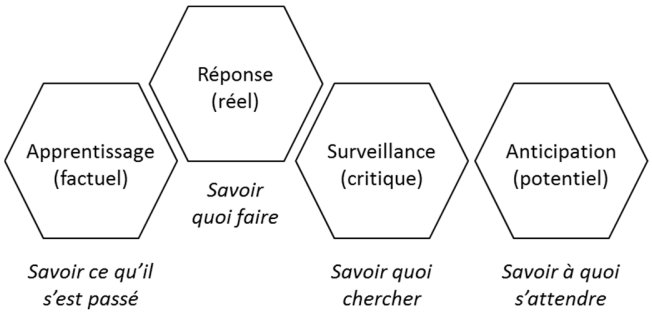


Figure 30 : Les quatre pierres angulaires de la résilience, adaptée de Hollnagel (2011)

1. **Savoir quoi faire :** il s'agit d'apporter une réponse aux perturbations régulières et irrégulières en mettant en œuvre une réaction prédéfinie, ou encore en ajustement le fonctionnement du système. C'est la gestion du réel.
2. **Savoir quoi chercher :** il s'agit de surveiller ce qui pourrait devenir une menace prochainement. La surveillance doit couvrir les évolutions récentes du système lui-même, et de son environnement. C'est la gestion du critique.
3. **Savoir à quoi s'attendre :** il s'agit de détecter et de prendre en compte les développements, les menaces, et les opportunités qui pourraient apparaitre dans le futur et qui auraient un impact sur le fonctionnement du système (tels qu'un changement majeur, une rupture, une pression nouvelle...). C'est la gestion du potentiel.
4. **Savoir ce qu'il s'est passé :** il s'agit d'apprendre de l'expérience, et notamment d'apprendre les bonnes leçons des bonnes expériences, qu'elles soient positives ou négative. C'est la gestion du factuel.

La résilience comme capacité à faire face aux évènements :

La première pierre angulaire de la résilience est la capacité à gérer le réel. Il s'agit de faire face en temps réel aux perturbations, ou aux évènements de rupture qui se présentent. Selon Pariès (2011), répondre à une situation particulière nécessite l'évaluation de la situation, l'identification de l'évènement de rupture, la définition des actions à mettre en œuvre, et leur implémentation au moment le plus adapté. Deux stratégies complémentaires permettent à un système de faire à une situation inattendue : l'anticipation, et la réactivité. Ces deux stratégies doivent être analysées avec deux perspectives. La première est directe. C'est celle de l'action. Il s'agit de s'assurer qu'une solution est bien mise en œuvre pour faire face. La seconde perspective, indirecte, est celle de la préparation de l'action. Il s'agit, pour les concepteurs, les managers, et les formateurs, de s'assurer de la présence d'une capacité de réponse efficace (présence des ressources, des compétences...), et de son maintien dans la durée. Pariès définit les deux stratégies de la manière suivante :

1. **L'anticipation de perturbations :** c'est l'identification a priori des situations de ruptures potentielles, et la prédéfinition des solutions associées (par exemple : défense en profondeur, procédures d'urgence, plan de continuité...). Les variations possibles du système sont analysées. Et des solutions de réponse sont stockées et prêtes à être activées. Cette stratégie est efficace pour les perturbations habituelles,

mais pose des difficultés pour l'anticipation des évènements très rares. Même prévus, ces évènements restent surprenants pour les opérateurs. Elle impose également une connaissance des situations pour lesquelles ces solutions sont prévues. Un système résilient doit donc avoir la capacité à identifier la nature de la situation rencontrée, la comparer au stock de réponses disponibles, et à mettre en œuvre la solution adéquate dans un temps contraint. Il nécessite également la capacité du système à reconnaitre qu'il est sorti de sa zone de maitrise. La résilience est donc davantage que seulement se préparer à ce qui peut se passer, mais également surveiller son degré de contrôle, et accepter l'échec des moyens et la perte de contrôle.

2. **La réactivité face à l'imprévu :** c'est la création en temps réelle de solutions particulières et nouvelles face à un évènement non connu. En effet, toutes les situations ne peuvent être anticipées dans le détail. La résilience signifie également la préparation à l'inconnu, c'est-à-dire aux évènements non anticipés. Cette préparation à la non-préparation s'effectue d'abord au niveau des opérateurs. Ceux-ci doivent être formés à être surpris émotionnellement et cognitivement, et garder une lucidité de réaction. La réactivité se prépare également au niveau du système. en situation inconnue, l'opérateur est confronté à l'incertitude. Le niveau de préparation à la réponse, c'est-à-dire son niveau d'abstraction fonctionnel, doit être adapté à cette incertitude. Plus celle-ci est grande, plus la réponse doit rester large et générique.

Enfin, Pariès pose la question de l'adaptation du système. Selon l'auteur, un choix doit être fait entre construire un système adaptable, et un système adapté. L'adaptation est un processus coûteux qui nécessite une dissonance entre un état idéal et un état réel. C'est en identifiant et en traitant ces écarts qu'un système s'adapte en permanence. Un choix doit donc être fait, entre un système totalement adapté à son environnement, moins sujet à la rupture, mais perdant son adaptabilité, et un système adaptable, constamment remis en question par de nouvelles situations et de nouvelles perturbations, mais entretenant une capacité à faire face aux aléas imprévus.

<u>La résilience comme capacité à surveiller l'évolution du système :</u>

Wreathall (2011) aborde la surveillance à travers la définition de la métrique adaptée à l'identification du niveau de performance sécurité du système. Au regard de la définition traditionnelle de la sécurité, la métrique principalement utilisée est le nombre d'incident, ou

d'accident sur une période donnée, ou encore la durée entre deux évènements significatifs. Selon l'auteur, cette approche est limitée. Si ce type de mesure fournit une certaine assurance que la sécurité a été gérée dans le passé, elle n'est que peu utile pour définir la manière dont la sécurité doit être gérée à l'avenir, pour plusieurs raisons. Tout d'abord, l'occurrence des évènements les plus importants (comme un accident majeur) comporte une grande part de chance. Deuxièmement, le compte des évènements n'apporte pas d'informations sur leurs origines, et leurs solutions. Troisièmement, une longue période de bon résultat peut faire émerger de l'autosatisfaction. Peut alors apparaitre des pressions internes pour ne pas signaler de faits nouveaux, afin de ne pas détériorer les performances passées. Enfin, dans la mesure où l'environnement d'un système, et son fonctionnement propre, ont des comportements dynamiques, les performances de l'année passée sont au mieux une faible indication de comment sera aujourd'hui et demain.

Selon Wreathall, le management de la sécurité est traditionnellement fondé sur le modèle des théories de contrôle classiques, représenté par la Figure 31. L'ingénierie de la résilience impose un management proactif du processus industriel, incluant la sécurité, mais pas seulement. Il s'agit d'anticiper les changements majeurs à venir, et impactant les performances du système. Dans ce cadre, mesurer les résultats du processus n'est pas suffisant. D'autres informations sont requises. A l'aide d'indicateurs, les informations sont directement issues du process, ainsi que de l'environnement direct du système. Anticiper les changements dans l'environnement, et réaliser des changements proactifs au sein du système, est une partie importante de la stabilité à long terme de l'organisation.

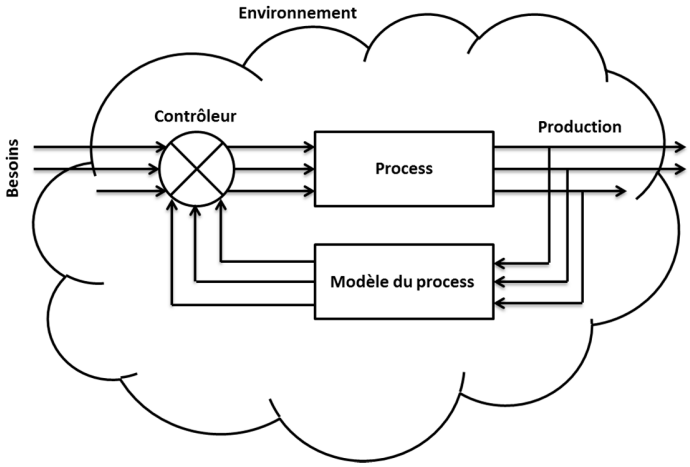


Figure 31 : Modèle classique de théorie du contrôle, adapté de Wreathall (2011)

Wreathall adresse alors la question des indicateurs de surveillance à travers plusieurs questionnements :

- **La sélection des indicateurs :** selon l'auteur, les indicateurs peuvent être définis comme une mesure proxy pour des éléments identifiés comme important dans le modèle sous-jacent de sécurité. Ils sont incertains et souvent déconnecté d'un idéal de mesure, eux-mêmes rarement disponible en pratique. En outre, il existe peu de modèle explicite permettant d'identifier les bons indicateurs. Les choix sont généralement portés sur des indicateurs qui ont montré leur efficacité dans le passé, ou encore des indicateurs portant sur les performances humaines.

- **La nature des indicateurs :** il existe une grande variété des types de mesure. Selon l'auteur, un indicateur doit posséder les caractéristiques suivantes : être objectif (mesurer un objet observable), quantitatif (mesurable par des valeurs, et en capacité d'identifier un changement de performance, disponible, facile à comprendre et à se représenter, et compatible avec d'autres systèmes d'information.

- **Le débat « Leading et lagging indicators » :** la différenciation entre ces deux types d'indicateurs n'est pas aisée. Un indicateur défini comme *lagging* selon une première perspective du système, peut être *leading* selon une deuxième. Sans

donner de réponse, l'auteur soulève ici la question de l'utilisation des indicateurs, et de leur intégration, dans un but de d'anticipation et de prévention.

La résilience comme capacité d'anticipation des ruptures potentielles :

Selon Woods (2011), pour être résilient, un système doit toujours garder une préoccupation l'efficacité de ses capacités d'adaptation, leur configuration, les ressources dédiées, et leur capacité à faire face aux ruptures. Laisser les capacités d'adaptation se dégrader rend le système vulnérable à la défaillance, ou même à l'effondrement. Woods propose alors une typologie de modèles sur la manière dont un système résilient peut anticiper la dégradation de ses capacités d'adaptation. Ces six modèles sont les suivants :

- **Les systèmes résilients sont capables de détecter la dégradation de leurs capacités d'adaptation :** cette facette est critique parce qu'elle pose la question de la relation du système à son environnement. Identifier ses capacités d'adaptation nécessite de redéfinir les scénarios de rupture pertinents, et d'interroger régulièrement le système sur sa capacité à faire face.

- **Les systèmes résilients sont capables d'identifier l'épuisement de leurs réserves, et de leurs marges de sécurité :** les réserves et les marges peuvent au quotidien s'éroder du fait de nombreuses petites décisions, qui prisent indépendamment n'ont pas de conséquences significatives, mais dont la somme peut conduire à l'inefficacité totale des parades. Ce phénomène est à rapprocher de celui de normalisation de la déviance de Vaughan.

- **Les systèmes résilients sont capables de reconnaitre les situations où il est nécessaire de modifier les priorités et les compromis :** l'étude des systèmes sociotechniques complexes montre que les compromis sont constamment présents et fondamentaux pour la conduite des activités (par exemple optimisation/fragilité, efficacité/précision...). Le système évolue dans un espace définit par ces compromis. Les systèmes complexes ont la capacité de modifier le positionnement de ces compromis en fonction de leur état, et des situations rencontrées.

- **Les systèmes résilients sont capables de réaliser des changements de perspective, et d'explorer de nouvelles perspectives, qui vont au-delà de leur position nominale :** C'est une capacité critique dans les systèmes avec des niveaux

d'interconnexion et d'interdépendance élevés. Elle permet d'identifier au mieux la manière dont ces systèmes peuvent défaillir, en intégrant par exemple des couplages non linéaires.

- **Les systèmes résilients sont capables de modifier leur fonctionnement en changeant les interdépendances entre les rôles, les activités, les buts et les niveaux :** c'est une capacité importante pour les systèmes qui ont besoin de synchroniser des unités multiples et garder une cohérence entre elle. Sans cette capacité, le système s'expose à des ruptures de contrôle entre des solutions localement adaptées, mais globalement inadéquate (ou inversement).

- **Les systèmes résilients sont capables de reconnaitre le besoin de développer de nouvelles voies d'apprentissage :** c'est l'enjeu de la résilience. L'anticipation ne peut être réalisée sans une remise en question des modèles d'apprentissage passés, face à des situations nouvelles, et potentiellement de rupture inconnue.

La résilience comme capacité d'apprentissage de l'expérience :

Selon Hollnagel (2011b), l'apprentissage est une capacité essentielle des systèmes résilients. En effet, la réponse des systèmes est majoritairement fondée sur la mise ne œuvre de solutions prédéfinies et stéréotypées. Celles-ci restent adaptées tant que les caractéristiques de l'environnement restent stables, et qu'aucun évènement imprévu n'ait lieu. Dans ce cadre, chaque perturbation significative et nouvelle nécessite la recherche de nouvelles voies de réponse adaptées. Selon l'auteur, trois conditions doivent être réunies pour que l'apprentissage soit possible :

1. **Une opportunité raisonnable d'apprendre :** la situation propice à l'apprentissage doit se répéter à une fréquence suffisante. L'éloignement des situations ne permet pas aux opérateurs de faire le lien les différentes leçons.

2. **Une similarité suffisamment importante entre les situations afin de pouvoir générer des généralisations :** Les situations doivent être comparables selon au moins quelques aspects, et pas seulement sur leurs conséquences.

3. **Une opportunité de vérifier que les bonnes leçons ont été tirées :** le même type de situation doit se répéter régulièrement, afin de vérifier que les leçons tirées précédemment sont bien mises en œuvre.

En outre, l'apprentissage est davantage qu'une collecte statistique, ou encore qu'une simple fonction mécanique. Pour être efficace, le processus d'apprentissage demande l'étude de faits objectifs. Ceux-ci doivent être analysés en profondeur, et explicités précisément, au-delà de mots-clés génériques (par exemple, défaut de coordination...). Enfin, une réflexion doit être menée sur la qualité des leçons qui doivent être tirées de l'analyse. L'implication de l'Homme dans le processus d'apprentissage peut conduire à l'identification de leçons différentes de la situation, compte tenu des points de vue, et des cultures de chacun.

Mesurer la résilience : *the resilience analysis grid*

Hollnagel propose un outil d'aide à la mise en œuvre d'une démarche d'ingénierie de la résilience. Il présente une approche pour mesurer la résilience d'un système, focalisé sur les quatre capacités citées précédemment (Hollnagel, 2011c). Celles-ci sont évaluées par une série de questions, et dont la réponse est représentée sous forme graphique (Figure 32). Le but est de comparer plusieurs mesures consécutives, afin d'aider au management d'un système résilient.

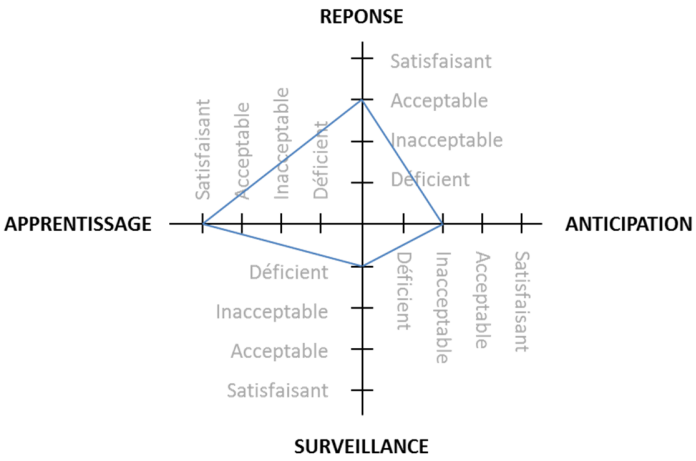


Figure 32 : Diagramme en étoile agrégé, adapté de Hollnagel (2011c)

CRITIQUE DU MODELE

Malgré une construction intellectuelle riche, et une contribution importante aux « Safety Sciences », plusieurs critiques du modèle de la résilience ont émergé dans la littérature scientifique. Le Coze (2013), en propose une synthèse.

Tout d'abord, Hale et Heijer ont critiqué l'intérêt d'introduire un nouveau vocabulaire au champ de la sécurité (Hale and Heijer, 2006). Selon les auteurs, le but de la sécurité n'est pas seulement de survivre aux accidents, mais également de les prévenir. L'application du concept de résilience dans son acception de « survivre face à l'adversité » ne présente alors que peu d'intérêt pour la sécurité, dans la mesure où il ne prend pas en compte l'aspect prévention. Mais si la définition de la résilience est étendue à la maitrise des performances et l'évitement des accidents, elle devient intéressante. Elle se substitue cependant à des notions déjà existantes qui prennent en charge le phénomène « accident industriel », tels que les organisations hautement fiables, ou encore les organisations munies d'une excellente culture sécurité. Le champ des « safety sciences » comprend de nombreuses acceptions relatives à la sécurité. Et de nombreux travaux ont montré la difficulté à les décrire avec précision. C'est également le questionnement de Roe et Schulman, qui s'interrogent sur l'utilité d'introduire de nouveau concept, comme celui de résilience, sans en expliquer les spécificités vis-à-vis des concepts déjà existants (Roe and Schulman, 2008).

Le second point questionné est celui du concept de résonnance et de l'analyse fonctionnelle, décrit par Hollnagel, comme explication du phénomène accidentel. L'intérêt d'un nouveau modèle est critiqué, dans la mesure où comme les précédents, il s'appuie sur les déterminants d'une perspective systémique.

Enfin, la troisième principale critique portée au modèle de résilience concerne la différentiation du concept vis-à-vis des travaux antérieurs. Selon Hopkins (2009b), organisation résiliente et organisation hautement fiables semblent être deux descriptions d'un même processus. Et les théoriciens de la résilience n'ont pas réussi encore à expliquer la différence entre ces deux idées. Selon Le Coze (2013), l'approche d'ingénierie de la résilience ne réussit pas à démontrer un apport scientifique clairement innovant. Même si l'origine du concept est issue d'une tradition scientifique, celle de la communauté de l'ingénierie cognitive, l'ingénierie de la résilience se rapproche de nombreux travaux déjà existants. A titre d'exemple, l'idée de résonance est similaire à celle de dégradation de la défense en profondeur, et des mouvements browniens, décrit dans le modèle de Rasmussen.

II.2 Analyse des modèles théoriques retenus

Après avoir présenté les principaux modèles de production de sécurité retenus, ceux-ci sont confrontés aux trois défis managériaux suivant :

- *Le défi de la complexité :* c'est le défi de la compréhension du système, de ses mécanismes, de son fonctionnement, et de son évolution.
- *Le défi de l'érosion du temps :* c'est le défi de l'instantanéité du monde actuel. Il s'agit de réinscrire la gestion dans la durée de long terme de la vie d'un système industriel.
- *Le défi de la décision :* rassembler les conditions d'émergence de la phase de décision, afin de passer du choix imposé par l'environnement, à la prise de risque d'initiative.

Gérer les risques d'accident organisationnel
J. Reason (1997)

<u>Le défi de la complexité :</u> faire l'inventaire des interactions qui caractérisent le système, identifier les propriétés émergentes.

La complexité est une notion omniprésente dans les travaux de Reason. Selon l'auteur, l'accident organisationnel arrive au sein des systèmes socio-techniques complexes. Ce sont des évènements difficiles à comprendre, contrôler, et prévoir. Ils résultent de la combinaison de multiples évènements, et impliquent des éléments de différentes natures du système.

Selon Reason, la complexité est une caractéristique du mode de fonctionnement du système. La sécurité d'un système de production est caractérisée par un grand nombre de barrières en interaction (défense en profondeur). Ces barrières sont également de différentes natures, et interconnectées entre elles : « I*t is a multiplicity of overlapping and mutually supporting defenses that makes complex technological systems »* (livre page 7). Ainsi, la complexité du système tient au nombre élevé d'interactions entre des barrières de différentes natures. Cela ne permet pas au concepteur et au manager de connaitre l'ensemble des évènements possibles, et les conséquences associées.

Le modèle de Reason prend également en charge la question de propriétés émergentes au sein du système. L'opacité du fonctionnement du système, issue de sa complexité, fait naitre des conditions latentes d'accident. Ces conditions émergent des décisions prises pour le pilotage du système industriel. Elles sont directement issues de la manière dont le système est géré. Elles ne sont pas directement visibles, mais contribuent à l'accident en se combinant avec d'autres facteurs.

Reason modélise la complexité du système dans le schéma des étapes du développement du phénomène accidentel (Figure 17). Les conséquences de la complexité sont modélisées en trois niveaux : l'opérateur, la situation de travail, et l'organisation. Ce modèle est intéressant parce qu'il permet de décrire l'effet de la complexité sur la sécurité des systèmes sociotechniques complexes. Il définit également des niveaux d'intérêt pour appréhender cette complexité.

En outre, le modèle proposé par Reason est plutôt descriptif. Et au regard du défi de la complexité, la limite de ces travaux est relative à leur opérationnalisation. En effet, l'auteur conçoit et décrit plusieurs éléments conceptuels qui permettent de décrire le système, et notamment les mécanismes inhérents à la phase accidentelle : conditions latentes, facteurs organisationnels.... Il les définit, et donne des exemples. Pour autant, l'auteur met en avant le caractère unique de chaque accident. Deux questions se posent alors. Premièrement, la première interrogation porte sur la manière de rapprocher des phénomènes constatés dans une entreprise, aux catégories définies par Reason. Par exemple, comment associer une condition organisationnelle, comme latente d'une dynamique accidentelle ? Deuxièmement, Reason ne traite pas la question de la criticité de chaque condition latente, et des mécanismes associés à leur conjonction à d'autres éléments du système. Peut-on associer un niveau de gravité des effets, ou encore un niveau d'interdépendance avec d'autres éléments du système ?

<u>Le défi de l'érosion du temps :</u> prise en compte des effets cumulés d'évènements, et l'anticipation de rupture dans la continuité de fonctionnement du système.

Le temps est une caractéristique importante du modèle de Reason. Selon l'auteur, l'accident a lieu à cause de la dégradation des barrières de défense, jusqu'à un niveau ou la dynamique accidentelle est rendu possible par l'alignement des trous : c'est la modélisation du fromage suisse. Ainsi, la condition nécessaire à l'accident est l'alignement de trous dans les défenses successives, permettant au potentiel de danger d'atteindre des cibles potentielles. Eviter l'accident revient à identifier et supprimer les trous dans les barrières de défense. Reason identifie plusieurs facteurs de dégradation des barrières de défense :

- Des défenses particulières peuvent être supprimées délibérément durant le réglage, la maintenance, ou par erreur ou violation de l'opérateur.
- Certaines barrières peuvent rester en panne, ou éteinte, du fait de l'excès de confiance du personnel dans la fiabilité et la sécurité du système.
- Des effets pervers dans la gestion du système peuvent conduire à des effets contre-productifs du point de vue de la sécurité : ironie de l'automatisation, sur-procéduralisation des opérations, ou encore excès de qualité.

L'idée d'érosion est également présente, dans l'aspect émergent et cumulatif des trous, qui s'alignent au fur et à mesure pour rendre la trajectoire accidentelle possible. Le modèle de Reason est donc intéressant pour aborder le défi de l'érosion du temps. Il permet de mettre

en lumière un phénomène de dégradation de la sécurité du système, et en particulier sur chaque barrière de défense. Il apporte également des explications et des illustrations de cette dégradation.

Cependant, ce modèle a également des limites. Au regard du défi de l'érosion du temps, le modèle est plutôt descriptif. Les travaux de Reason n'apportent pas de précision relative à la manière dont les trous apparaissent et évoluent. De même, les mécanismes de dégradation des barrières de défense ne sont pas explicités. Par exemple, aucune précision n'est mentionnée sur les liens existants entre l'apparition de conditions latentes, et la dégradation des barrières. Egalement, l'aspect des ruptures dans la continuité du fonctionnement du système manque. Elle est indirectement présente, par la définition des trous. Les conditions latentes contribuent à la création des trous, sans en expliquer les mécanismes.

Le modèle identifie l'aspect cumulatif, sans pour autant le caractériser, et lui associer un niveau de criticité. Peut-on identifier une situation limite pour laquelle les barrières de sécurité sont trop dégradées pour assurer le fonctionnement du système dans des conditions acceptables de sécurité ?

Le défi de la décision : construire et représentation actualisée de la situation, et une argumentation convaincante.

La décision n'est pas clairement identifiée dans le modèle de Reason, mais elle est fortement sous-jacente. Selon l'auteur, les conditions latentes d'accident sont rendues possibles par de mauvaises décisions au niveau des couches managériales du système, du haut vers le bas.

Selon l'auteur, deux types de décision sont concernées :

1. Les décisions issues des hautes sphères managériales (top management, ou encore management stratégique) : elles impactent tout le système par effet de cascade. Elles créent des conditions qui peuvent contribuer à l'occurrence d'une dynamique accidentelle.
2. Les décisions issues de « managers de lignes » : il leur appartient régulièrement de choisir de supprimer ou non certaines barrières de sécurité, dans le but de satisfaire à des exigences opérationnelles.

S'il apporte une typologie intéressante des décisions liées à la production de sécurité, le modèle de Reason ne décrit pas l'origine de ces décisions, et les processus associés.

Selon l'auteur, éviter l'accident nécessite une manière adéquate de gérer la sécurité, et comprend trois stratégies :

1. Une mesure adéquate de l'état de santé du système de gestion de la sécurité.
2. Des qualités spécifiques associées aux managers.
3. Une culture de sécurité au sein du système.

Reason propose alors une identification des processus organisationnels sous-jacent à la sécurité. Connaitre l'état de ces processus permet d'identifier le niveau de sécurité du système. Pour Reason, le système de gestion est donc un bon proxy pour mesurer l'état réel de risque présenté par le système.

Pour réaliser une mesure du niveau de sécurité, Reason propose la construction d'un système d'information de la sécurité. Le modèle est plutôt prescriptif dans la mesure où il oriente le manager dans la manière de définir les objectifs de sécurité, et de construire le système d'information sécurité (types d'indicateurs, signaux faibles). Son système d'information permet d'alimenter le manager en information pré-réfléchies et actualisées. Celles-ci lui permettent théoriquement de l'aide face à ses dilemmes.

L'intérêt des travaux de Reason est dans le lien fait par l'auteur entre le processus accidentel et l'outil de surveillance nécessaire au pilotage du système et de son maintien dans une zone de sécurité. Il met en exergue l'existence du compromis de sécurité, et le dilemme existant entre sécurité et production, et l'équilibre à atteindre entre ces deux dimensions. Si les travaux de Reason permettent d'aborder le défi de la décision à travers l'aide à la décision, et la construction d'un système d'information sécurité adéquat, ceux-ci ont des limites. Premièrement, Reason n'explique pas comment cet outil d'aide à la décision doit être utilisé, à l'exception de la description sommaire des compétences génériques que doit posséder le manager. Deuxièmement, il ne décrit pas les processus logiques d'acquisition et d'interprétation des données, qui conduisent à des informations pertinentes et éclairantes (C'est par exemple le cas pour la sélection et l'utilisation des indicateurs de gestion). Il n'aborde pas la question des processus de prise de décision, et ne décrit pas la place de cet outil dans les processus décisionnels.

Enfin, le modèle de Reason ne définit pas l'entité de manager opérationnel au sein du système. Il ne fait référence au manager qu'à travers une généralisation de niveau : le

management, les tenants des processus organisationnels. Une seule mention est faite au manager technique, à des managers de ligne, ou encore des superviseurs, sans considération particulière vis-à-vis d'autres couches managériales.

Les organisations hautement fiables
K. Sutcliffe (2011)

<u>Le défi de la complexité :</u> faire l'inventaire des interactions qui caractérisent le système, identifier les propriétés émergentes.

La notion complexité est à la base du modèle des organisations hautement fiables. Roberts et Rousseau ont défini huit caractéristiques primaires que possèdent les HRO. Si certaines autres organisations peuvent en posséder certaines, les HRO les manifestent toutes. Parmi ces huit caractéristiques, deux d'entre elles font référence la complexité :

- L'hypercomplexité : le système est constitué d'une très grande variété de sous-systèmes, composants, de niveaux, et de composants.
- L'existence de couplages étroits : les systèmes étroitement couplés possèdent des interdépendances réciproques entre les niveaux et unités, des dépendances temporelles entre les processus, des séquences invariantes, une conception globale qui impose une seul manière d'atteindre les objectifs, et peu d'interstices dans des processus de production continus.

Du fait de ces deux caractéristiques, il n'est pas possible de comprendre complètement l'état du système, de prédire son fonctionnement, et d'intervenir pour contenir des défaillances potentiellement catastrophiques.

On peut conclure au regard de ces deux caractéristiques que le modèle des organisations hautement fiables prend en charge la complexité, et notamment la question de l'inventaire de l'ensemble des interactions qui caractérisent le système. La très grande variété des nombreux composants, et l'existence de couplage, ne permet pas d'identifier l'ensemble des mécanismes qui animent le système. Prédire tous les scénarios accidentels possibles est alors impossible.

Ce modèle a cependant, au regard du défi de la complexité, des limites. Tout d'abord, la question de la complexité à travers l'existence de propriétés émergentes n'est pas abordée, même indirectement. Egalement, il n'existe pas de mise en perspective de la notion d'hypercomplexité, à celle de complexité. Au regard des définitions proposées, ces deux idées semblent identiques. Enfin, le modèle des organisations hautement fiables est plutôt descriptif. La complexité est définie comme une caractéristique du système, qui rend l'occurrence d'évènements non prévues inévitable. La complexité est évoqué, mais peu

décrite, et sur la base de travaux précédents (Perrow, notamment sur la question des couplages). Elle peut être même considérée comme une hypothèse du modèle, dans la mesure où la théorie des organisations hautement fiables s'applique aux organisations complexes.

<u>Le défi de l'érosion du temps :</u> prise en compte des effets cumulés d'évènements, et l'anticipation de rupture dans la continuité de fonctionnement du système.

L'idée d'érosion du temps n'est pas directement et clairement prise en charge par le modèle des organisations hautement fiables. Cependant, on peut la rapprocher de plusieurs éléments. Tout d'abord, on peut citer la notion d'anticipation. Les HRO montrent une capacité de détection et de gestion des évènements non prévus, ou non souhaités. Cette caractéristique s'exprime par un souci de la défaillance, et une sensibilité aux opérations en cours.

Le défi de l'érosion du temps peut également se retrouver dans la caractéristique d'organisation apprenante. Celle-ci s'exprime dans les organisations hautement fiables par une formation continue, et une mise à jour continue des règles, et des procédures associées au fonctionnement en sécurité du process industriel.

Au regard de ces deux caractéristiques, ce sont les effets de l'érosion du temps qui sont pris en compte. Cependant, le modèle n'explicite pas d'effets systémiques, et ne fait pas référence à l'anticipation de ruptures potentielles.

<u>Le défi de la décision :</u> construire une représentation actualisée de la situation, et une argumentation convaincante.

La décision prend une place importante dans le modèle des organisations hautement fiables. Elle joue un rôle central, aussi bien dans la logique de prévention, que celle de résilience, qui anime les HRO. Les deux questionnements associés au défi de la décision sont abordés.

Concernant la construction d'une représentation actualisée de la situation, plusieurs schémas organisationnels ont été identifiés par les auteurs : la capacité de l'organisation à faire remonter les mauvaises nouvelles, la réalisation régulière d'audits proactifs, l'existence de discussions ouvertes, sans sujets tabous, et une forte sensibilité aux

opérations en cours. Tous ces schémas participent à un partage de l'information connu entre les acteurs du système. Ainsi, on peut considérer qu'ils jouent un rôle dans la prise de décision d'anticipation.

Concernant le second questionnement, le fait que la décision soit convaincante repose sur deux éléments. Il est tout d'abord fondé sur la déférence à l'expertise, et à la sensibilité à l'équilibre nécessaire entre production et sécurité. Ces deux aspects contribuent à la construction d'une argumentation convaincante, pour faciliter la prise de décision de prudence. Les décisions invoquées au titre de la sécurité sont davantage entendues.

Au regard de ce troisième défi, le modèle des organisations hautement fiables reste descriptif. Le modèle propose des schémas organisationnels qui ont été observés dans plus organisations. Le modèle des HROs apparait comme un idéal à atteindre. Il ne fournit pas de définition des couches décisionnelles, et très peu de référence au management opérationnel. Les processus de prise de décision, par lesquels le manager se construit une représentation actualisée, ne sont pas définis. Egalement, la notion d'expertise n'est pas définie. L'aspect argumentation de la décision est donc davantage lié à une question de posture, que de méthodologie.

La migration des activités du système
Jean Rasmussen (1997)

<u>Le défi de la complexité :</u> faire l'inventaire des interactions qui caractérisent le système, identifier les propriétés émergentes.

Rasmussen aborde la problématique de la sécurité à travers le concept de contrôle des activités. Dans une société devenue dynamique, les théories classiques sont devenues inefficaces pour maintenir un haut niveau de sécurité. L'auteur définit alors un modèle de système socio-technique complexe.

Dans ce modèle, la complexité tient à trois caractéristiques :

- L'existence de nombreux niveaux décisionnels : politiciens, managers, inspecteur, opérateurs... De nombreux échelons sont impliqués dans le contrôle des activités industrielles. Chaque niveau joue un rôle dans la définition des lois, des règles et des instructions qui guident la manière dont le process primaire de production, à la base du système, est mis en œuvre.
- L'influence de l'environnement sur le process de production : conscience politique, pression financière, conditions de marché, niveau de compétence et d'éducation, changements technologiques... le contexte sociétal a une influence sur les décisions générées par les différents niveaux du système.
- La présence de multiples disciplines académiques : la structuration de chaque niveau du système sociotechnique est fondée sur un champ académique différent. Chaque discipline possède ses définitions, et décline la problématique de la sécurité à travers ses propres modèles.

Au regard du modèle de Rasmussen, le système comprend l'ensemble des éléments de la société qui jouent un rôle dans la gestion des risques industriels. Ce périmètre dépasse largement le cadre de l'entreprise industrielle à risque.

La notion de complexité est très peu explicitée dans le modèle de Rasmussen. La seule référence est relative à la formulation « système sociotechnique complexe ». Pourtant, on peut considérer qu'elle est indirectement décrite à travers les trois caractéristiques précédemment citées.

Avec ce modèle, Rasmussen propose un inventaire des interactions qui caractérisent le système. Les flux montant et décidant semblent également définir des boucles de rétroaction. Cependant, cette modélisation est descriptive. Elle formalise des relations et des niveaux décisionnels qui permettent de mieux appréhender le fonctionnement du système global. Pour autant, elle ne pose pas la question de l'inventaire exhaustif des interactions existantes au sein du process, et de la définition de l'ensemble des comportements possibles qui le caractérisent.

En outre, le modèle de Rasmussen propose une relation hiérarchique et processuelle entre le niveau du système. Il n'identifie pas de phénomènes systémiques, et n'aborde pas la question des propriétés émergentes du système.

Le défi de l'érosion du temps : prise en compte des effets cumulés d'évènements, et l'anticipation de rupture dans la continuité de fonctionnement du système.

Selon Rasmussen, les activités du système sont conditionnées par des contraintes administratives, fonctionnelles, et sécuritaires. Ces évolutions imposent des changements de stratégies dans le pilotage. Au fur et à mesure des activités, la perte d'équilibre entre sécurité, rentabilité, et charge de travail, fait migrer le système au-delà des limites de performance acceptable. A titre d'exemple, un excès de pression de production conduit à une dégradation progressive de la défense en profondeur. Le système est alors placé dans une zone de fonctionnement de performance non acceptable, au-delà de la frontière de sécurité.

L'érosion du temps n'est pas une idée directement explicité par Rasmussen. Cependant, elle est à rapprocher de celle de migration des activités du système. Deux points communs peuvent être identifiés :

- L'idée d'évènements indépendants : les mouvements du système sont pilotés par des « gradients », des motivations individuelles ou collectives vers un état de bien être ou de performance.
- L'idée d'accumulation : la somme des gradients individuels conduit petit à petit le système à sortir de sa zone de performance acceptable. La migration résulte de la somme de tous.

On peut conclure de ces aspects que le défi de l'érosion du temps, comme prise en compte des effets cumulés d'évènements a priori indépendant, est bien prise en compte dans le modèle de Rasmussen.

Mais ce modèle a également des limites. Il peut tout d'abord est considéré comme descriptif. En effet, les gradients sont peu décrits, et l'auteur n'apporte pas d'éléments méthodologiques permettant d'y associer des éléments rencontrés dans les situations réelles.

Egalement, le modèle de Rasmussen ne prend pas en compte l'idée d'anticipation des ruptures. Dans la modélisation proposée, une rupture dans la continuité des activités du système pourrait correspondre à un saut brownien de grande ampleur, un grand écart immédiat entre une zone de performance acceptable et une zone dangereuse.

<u>Le défi de la décision :</u> construire une représentation actualisée de la situation, et une argumentation convaincante.

Les travaux de Rasmussen n'aborde pas directement la question de la décision du manager, mais aborde plutôt la problématique sous l'angle du pilotage global du système. En effet, le contexte est dynamique, et le système socio-technique et complexe. Le mode de gestion doit alors passer d'un contrôle pré-planifié, dans lequel tous les comportements du système sont définis, analysés et prévus, à un mode de gestion fondé sur la rétroaction et le pilotage. Le second mode est plus à-même de prendre en compte les perturbations non-prévues. Le pilotage est donc fondé sur un système de contrôle adaptatif connectant la sécurité, la production, et l'économie.

Rasmussen identifie le niveau du management au sein du système sociotechnique, comme niveau de contrôle et de décision en termes de gestion de la sécurité. L'auteur questionne trois aspects important du manager, sans apporter de réponse :

- Le niveau d'information : l'identification et la mesure de l'état actualisé du système est importante pour la définition des réponses adéquates aux situations rencontrée. Chaque entreprise doit posséder un système d'information (documentation).
- Les compétences : les compétences du manager sont critiques pour son activité de contrôle, et de transposition d'une règle générale, en décision locale. Il doit être

capable d'intégrer les informations importantes, et de définir la meilleure décision en fonction du contexte.

- L'engagement : cet aspect concerne la volonté du manager à agir correctement, et à se sentir concerné par les questions de sécurité.

Enfin, Rasmussen propose un état de l'art des principales tendances au sein des travaux abordant la prise de décision dans le paradigme des sciences humaines.

Concernant le défi de décision, le modèle proposé par Rasmussen est quelques peu prescriptif, car il définit des questionnements à aborder, et propose un modèle de système de contrôle adaptatif.

Cependant, il a également des limites. Concernant la construction d'une représentation actualisée de la situation, le modèle ne décrit pas les processus de prise de décision en jeu. Il aborde la nécessité pour le manager d'être informé, sans pour autant discuter ou prescrire un système d'information adéquat, aussi bien en termes de contenu, que d'architecture de l'outil. La qualité de la décision semble reposer sur le fait que le manager soit informé, compétent, et engagé. Pour autant, le modèle n'apporte pas d'idée concernant les conditions de prise de décision, et les outils d'aide à la décision nécessaire. Enfin, le modèle ne prend pas en charge la question de la production d'une décision qui soit convaincante. La construction d'un système sociotechnique à différents niveaux décisionnels hiérarchiques ne suppose pas l'existence de jeux d'acteurs, ou encore de filtres.

La gestion de la sécurité dans les systèmes de production
A.R. Hale (2003)

<u>Le défi de la complexité :</u> faire l'inventaire des interactions qui caractérisent le système, identifier les propriétés émergentes.

Le mot de complexité est très peu cité dans les travaux de Hale. La notion est également peu explicitée. Hale s'appuie tout d'abord sur les travaux de Rasmussen pour énoncer l'idée que l'on ne peut supprimer toutes les déviations présentes au sein d'un système industriel. Il est également impossible de prédire à l'avance tous les risques, et les effets de toutes les nouvelles technologies dans les structures organisationnelles.

Hale s'appuie également sur la notion de maitrise pour appréhender la complexité. L'auteur avance que les systèmes industriels de production sont parmi les systèmes les plus complexes à gérer. En effet, nous cherchons à contrôler la moindre petite chance qu'un scénario accidentel puisse arriver (parfois inférieure à 1 sur 1000000).

Nous pouvons constater que le défi de la complexité n'est pas pris en charge par le modèle proposé par Hale. Aucune référence n'est faite, ni à la problématique d'inventaire des interactions qui caractérisent le système, ni à l'existence de propriétés émergentes (si ce n'est la simple mention sur un graphique que le niveau intermédiaire de pilotage doit prendre en compte de nouveaux risques, sans préciser s'il s'agit de risques émergents). La notion de complexité apparait alors davantage comme une hypothèse, plutôt qu'une caractéristique du modèle.

<u>Le défi de l'érosion du temps :</u> prise en compte des effets cumulés d'évènements, et l'anticipation de rupture dans la continuité de fonctionnement du système.

Le modèle de Hale ne prend pas directement en charge le défi de l'érosion du temps. Le modèle est en outre très prescriptif sur des aspects que l'on pourrait rapprocher de ce défi :

- Un système de gestion de la sécurité doit posséder une compréhension claire du fonctionnement du processus primaire de production, ainsi que tous ses auxiliaires. L'analyse des risques doit être exhaustive et actualisée.
- Le SGS doit posséder une capacité d'apprentissage pour la prise en compte et l'analyse des situations non-prévues.

Selon Hale, la sécurité est le résultat d'une conception robuste fondée sur une défense en profondeur, et un système de gestion de la sécurité efficace. Au sein du modèle, l'analyse des risques est complète, les écarts sont corrigés au fur et à mesure par le système de pilotage, et les évènements non prévus sont pris en compte grâce à la capacité d'apprentissage de l'organisation. En conséquence, l'érosion du temps semble ne pas être un comportement possible du système.

Le défi de la décision : construire et représentation actualisée de la situation, et une argumentation convaincante.

Plusieurs aspects des travaux de Hale permettent d'aborder le défi de la décision.

Tout d'abord, Hale propose d'aborder la question de la gestion de la sécurité à travers une approche de résolution de problème, composée de trois niveaux : structure et politique, planification et procédures, réalisation du contrôle des risques. Le niveau intermédiaire de pilotage a pour tâche l'allocation des ressources et le contrôle des activités des niveaux de production inférieur. Hale définit également plusieurs caractéristiques associées à ce niveau, et notamment :

- Des compétences pour la gestion des situations prévues, et permettant l'improvisation face à des situations nouvelles.
- Un engagement et une motivation de la part des acteurs dans la conduite en sécurité des activités de production.
- Des règles pour la gestion des conflits entre sécurité et autres aspects du système (production, maintenance...).

Dans cette description, Hale cible donc le rôle du manager opérationnel, mais sans en faire explicitement référence.

Hale aborde aussi la question de la décision de manière sous-jacente, à travers la prescription d'un processus de pilotage base sur le contrôle et le feedback. Chaque élément du processus est une fonction à remplir pour la résolution des problèmes liés à la gestion de la sécurité. Pour autant, chaque élément n'est pas décrit avec précision. Le modèle ne va pas dans la description au-delà de l'identification des principales fonctions, et des principaux liens relationnels existant entre ces fonctions.

Hale aborde également la question de la décision à travers la question du conflit entre sécurité et production. L'auteur prône une reconnaissance de l'existence de ce conflit dans la réalisation des activités quotidiennes, et une gestion explicite de ce conflit. Cependant, il n'apporte aucune précision sur la manière de gérer ce conflit.

Enfin, Hale aborde la décision à travers l'influence des émotions dans la prise de décision. Après avoir identifié quelques contributions scientifiques sur la question, l'auteur met en avant l'idée que le processus de prise de décision ne peut être que subjectif. Ainsi, le rôle des émotions doit être analysé et intégré aux processus décisionnels. Pour autant, Hale ne donne pas de piste sur la manière de procéder à cette intégration.

Au regard de ces éléments, les travaux de Hale ne permettent de répondre que partiellement au défi de la décision. Le modèle est prescriptif à un niveau macroscopique. Il définit des grandes fonctions que doit remplir un système de gestion de la sécurité. Pour autant, il ne définit pas avec précision quels sont les processus de prise de décision mis en œuvre par le manager opérationnel. D'autre part, la question de la construction d'une argumentation convaincante n'est pas abordée, même si elle est effleurée par la formalisation du conflit entre sécurité et d'autres dimensions, et les compétences nécessaires que doivent posséder chaque niveau de contrôle.

L'ingénierie de la résilience en pratique
Hollnagel et al. (2010)

<u>Le défi de la complexité :</u> faire l'inventaire des interactions qui caractérisent le système, identifier les propriétés émergentes.

La notion de complexité est très peu explicitée au sein du modèle de la résilience coordonné par Hollnagel. Une référence au système socio-technique complexe est présente en prologue de l'ouvrage :

« The developments in socio-technical systems during the last 20 years or so have, however, created in increasing number of systems and processes that are intractable, and where performance variability consequently is a necessity and an asset than a liability » (Hollnagel et al. ,2010, page xxxv).

La complexité est dans ce prologue traité comme un constat du monde actuel. Elle apparait comme une hypothèse du modèle.

La complexité est également abordée indirectement dans la notion de variabilité de la performance. Selon l'auteur, le système est soumis à différentes perturbations tout au long de la réalisation de ses activités. Elles peuvent être d'origine interne, du fait du comportement des acteurs, ou de la fiabilité des composants. Elles sont également d'origine externe, du fait des liens forts unissant le système et son environnement. Cette variabilité potentielle dans la performance ne peut être complètement prise en compte dans les modèles d'analyse des risques. Des situations non-prévues, et aux conséquences potentiellement catastrophiques, sont toujours possibles.

La notion de complexité peut aussi être rapprochée de la notion d'incertitude associée à l'efficacité des barrières de sécurité. Le modèle de résilience décrit la sécurisation du processus de production à travers la nécessité d'une défense en profondeur. Chaque couche de défense constitue un niveau d'incertitude pour le manager ou l'opérateur. Va-t-elle remplir son rôle, et être efficace ? Et le niveau d'incertitude globale associé la sécurité du système augmente à chaque fois qu'une barrière tombe. Ainsi, l'incertitude représente une difficulté pour l'opérateur et le manager à comprendre une situation inhabituelle, et à réagir correctement.

Au regard de ces trois aspects, on peut conclure que le défi de la complexité est pris en charge par le modèle de la résilience. Aucune mention n'est faite de l'inventaire des interactions qui caractérisent le système. Pour autant, le modèle est descriptif, et met en avant deux dimensions importantes de la complexité : l'impossibilité de prévoir tous les scénarios, et mécanismes associés du système (variabilité de la performance), et l'aspect évolutif des comportements du système (l'incertitude, et la surprise face aux situations non prévues).

L'érosion du temps : prise en compte des effets cumulés d'évènements, et l'anticipation de rupture dans la continuité de fonctionnement du système.

La résilience est définie par l'auteur comme la capacité intrinsèque d'un système à ajuster son fonctionnement pour faire face aux conditions opérationnelles à la fois prévues et non prévues. Ce cadrage sémantique ne permet pas structurellement la prise en compte du phénomène d'érosion du temps dans le modèle de la résilience.

En effet, l'objet de la résilience est l'adaptation continue. De plus, le modèle proposé par Hollnagel est prescriptif. Il définit la manière d'obtenir cette adaptation. Ce sont les quatre piliers de la résilience, que tout système doit mettre en œuvre pour garder la maitrise de ses activités en toutes situations.

De fait, la prise en compte des effets cumulés d'évènements à priori indépendants doit être réalisée au fur et à mesure que ces évènements arrivent. De plus, l'anticipation des ruptures est prise en compte à l'aide de stratégie de préparation du système, et notamment par la formation des opérateurs. Ceux-ci doivent être prêts à être surpris, pour garder la capacité affective et cognitive de faire à une situation urgente et exceptionnelle.

En conséquence, le phénomène d'érosion du temps à long terme n'est théoriquement pas possible dans un système résilient.

En outre, le modèle propose le phénomène de décompensation. C'est la propagation d'une perturbation à travers le système, par le jeu des interdépendances. Cela est rendu possible par le fait que les réponses prévues ne permettent pas de maitriser la perturbation. Il est le fait d'une inadaptation du système, et ne correspond pas à l'idée d'érosion du temps.

<u>Le défi de la décision :</u> construire une représentation actualisée de la situation, et une argumentation convaincante.

Le modèle de la résilience n'aborde pas directement la question de la décision du manager opérationnel. Dans son ouvrage, l'auteur propose un modèle prescriptif global au système. Cependant, plusieurs aspects du modèle peuvent alimenter le défi de la décision.

La question de la décision est d'abord abordée par la question du pilotage. Afin de maintenir une performance opérationnelle satisfaisante, et pour gérer l'ensemble des perturbations qui s'imposent, le système doit posséder un élément de pilotage. Hollnagel propose alors de s'appuyer sur les théories du contrôle classique. Les activités du process sont corrigées en permanence par un contrôleur, en fonction des données reçus par le système d'information. De manière sous-jacente, on peut rapprocher le rôle de contrôleur de la fonction de manager opérationnel. Pour autant, le modèle n'identifie pas de niveaux décisionnels précis.

Egalement, le modèle de la résilience aborde la question de la décision à travers la question de la définition d'un système d'information. Les outils de mesure, et plus particulièrement les indicateurs, doivent permettre de mesurer l'état de résilience du système, et engendrer des ajustements, si les résultats identifiés ne sont pas satisfaisant. L'ouvrage est également prescriptif dans la définition des caractéristiques pour la construction des indicateurs. Il propose même un exemple avec la description d'un système de gestion de la fatigue pour le personnel de vol.

Enfin, le modèle de la résilience traite indirectement la prise de décision avec la capacité à décider. Afin de gérer toute les variabilités de performance du système, l'opérateur, ou le manager, doit avoir la capacité de reconnaitre une situation non prévue, ou une situation prévue nécessitant la mise en œuvre d'un protocole non planifié au départ. Cela nécessite une disponibilité intellectuelle et affective, une lecture précise de la situation, une identification de l'évolution des évènements, et des ressources disponibles. Le modèle définit donc un cadre de compétence que doit posséder chaque manager, ou opérateur, afin d'être capable de comprendre la situation, et de décider.

Ces deux derniers aspects, relatifs au système d'information, et aux compétences des acteurs, contribuent au défi de la décision. En effet, ce sont deux éléments essentiels pour permettre la construction d'une représentation actualisée de la situation. Cependant, le modèle, s'il propose un système de pilotage, n'explicite aucunement avec précision les

processus de prise de décision présent au niveau du management opérationnel. Il n'aborde donc pas non plus le second questionnement du défi de la décision, à savoir la construction d'une argumentation convaincante. Cette limite peut tenir à deux aspects. Tout d'abord, la sécurité englobe tous les aspects de la variabilité de la performance. Dans cette définition, le conflit entre sécurité et production n'émerge pas directement, dans le sens où l'ajustement demandé est issue d'une lecture partagée de la situation. Egalement, les cas d'étude qui imagent le concept de résilience concernent des pilotes de ligne, et des médecins. Ce sont deux catégories de population par ailleurs déjà doté d'un fort pouvoir décisionnel. La question du conflit s'efface donc devant celle du dilemme intérieur. Ce sont également des métiers qui nécessitent une réponse rapide. Le dilemme intellectuel est alors rapidement bridé par l'obligation d'agir.

III – Nécessité d'un nouveau regard sur l'accident industriel

Après avoir porté un regard critique sur les principaux modèles étudiés, il convient de noter les apports de notre analyse. L'objectif de cette troisième sous-partie est de répondre au questionnement initial : quel est la capacité de ces cinq modèles à répondre aux trois défis identifiés ? Pour répondre à cet objectif, le plan est le suivant. Tout d'abord, une première partie propose une synthèse des limites identifiées dans l'analyse précédente. Enfin, une deuxième partie propose de répondre à ces limites par un nouveau regard porté sur l'accident industriel majeur, davantage centrée sur le manager opérationnel.

Les apports de notre étude sont formalisés de deux manières différentes. Un premier tableau propose une vue de synthèse des différents arguments positifs et négatifs de chaque modèle, vis-à-vis du défi identifié (Tableau 9). A la suite de ce tableau, un paragraphe descriptif reprend en synthèse, et par défi, les limites des modèles sélectionnés.

Défis	Modèles	Gérer le risque d'accident organisationnel	Les organisations hautement fiables	La migration des activités	La gestion de la sécurité dans les systèmes de production	L'ingénierie de la résilience en pratique
Le défi de la complexité	+	Description de la complexité (interaction entre les barrières, et identification de ses effets sur 3 niveaux du système. Définition de conditions latentes (propriétés émergentes).	Définition de l'hypercomplexité (interactions multiples), et des couplages étroits entre les éléments (interdépendance).	Formalisation du système socio-technique complexe. Définition de liens relationnels entre les couches décisionnels.	Référence aux travaux de Rasmussen pour traiter la question de la complexité.	Complexité indirectement traité par le constat de la difficulté à gérer les systèmes, la notion de variabilité de la performance (impossibilité à prévoir tous les scénarios), et l'incertitude associée à l'efficacité des barrières de sécurité (aspect évolutif du comportement du système).
	-	Modèle descriptif. Opérationnalisation difficile. Pas de définition du niveau de criticité des conditions latentes, et des mécanismes de conjonction dans la dynamique accidentelle.	Modèle descriptif. Non prise en compte des propriétés émergentes. Différentiation complexité/hypercomplexité.	Modèle descriptif. Définition sommaire des liens entre les niveaux décisionnels. Caractérisation sommaire et macroscopique de la complexité du système. Pas de prise en compte de propriétés émergentes.	Aucune référence n'est faite, ni à la problématique d'inventaire des interactions qui caractérisent le système, ni à l'existence de propriétés émergentes.	Modèle descriptif. Pas de reflexion relative à l'inventaire des interactions qui caractérisent le système.
L'érosion du temps	+	Phénomène de dégradation des barrières de défense (modèle du fromage suisse). Typologie de facteur de dégradation. Aspect cumulatif de chaque dégradation indépendante (modèle du fromage suisse).	Identification de la caractéristique d'anticipation, et d'organisation apprenante.	Définition du phénomène de migration des activités du système.	Modèle prescriptif. Sécurité basé sur une compréhension précise de son fonctionnement, et sur sa capacité d'apprentissage.	Modèle prescriptif. Résilience basée sur l'adaptation continue. Définition de l'anticipation comme capacité d'adaptation.
	-	Modèle descriptif. Caractérisation de la criticité du niveau de dégradation global. Lien avec les conditions latentes.	Modèle descriptif. Pas de référence à l'existence de symptômes systémiques, et de phénomènes de rupture.	Modèle descriptif. Faible description des facteurs de migration. Opérationnalisation difficile. Pas de référence à l'idée d'anticipation des ruptures.	Pas de définition de comportements systémiques, ou de ruptures potentielles.	Pas d'identification d'un phénomène d'érosion du temps.
Le défi de la décision	+	Typopologie de décisions conduisant à la dégradation des barrières. Définition des processus organisationnels sous-jacents à la sécurité (proxy). Prescription d'un système d'information de la sécurité. Identification de la nécessité compromis entre production et sécurité. Description sommaire des compétences du manager.	Identification de schémas organisationnels permettant la construction d'une représentation actualisée de la situation, et d'argumentation de la décision.	Identification du niveau du management dans l'échelle des niveaux décisionnels. Questionnement de trois aspects du manager pour la prise de décision (niveau d'information, compétence, engagement).	Définition d'un niveau de pilotage, et des compétences nécessaires. Prescription d'un processus de pilotage basé sur le contrôle. Identification du conflit existant entre sécurité et production. Identification du rôle des émotions dans la prise de décision.	Modèle prescriptif. Définition d'un modèle de pilotage basé sur une boucle de contrôle. Définition d'un système d'information, basé sur des indicateurs de résilience. Définition d'un cadre de compétence pour le contrôleur.
	-	Aspect non directement pris en charge, mais sous-jacent. Pas de définition de l'entité manager opérationnel, ou des niveaux décisionnels du système. Pas de définition des processus de prise de décision, et d'agumentation.	Modèle descriptif, décrit comme un idéal à atteindre. Pas de définition de l'entité manager opérationnel, ou des niveaux décisionnels du système.	Pas de définition des processus décisionnels. Pas de réponse apportée aux questionnements soulevés. Pas de réflexion sur l'argumentation.	Modèle prescriptif à un niveau mascroscopique. Pas de définition des processus de prise de décision. Pas de réflexion sur l'argumentation.	Pas de définition de l'entité manager opérationnel, ou des niveaux décisionnels du système, et des processus décisionnels associés.

Tableau 9 : Synthèse des limites des modèles sélectionnés

Le défi de la complexité

L'analyse des cinq modèles de production de sécurité met en lumière l'intérêt porté sur la notion de complexité. En effet, l'ensemble des modèles cherchent à décrire la dimension complexe des systèmes industriels. Certains modèles la décrivent directement :

- Accident organisationnel : la complexité est décrite à travers les interactions entre les barrières de défense, et l'émergence de conditions latentes, propices à l'accident.
- Organisations hautement fiables : les nombreuses interactions multiples des éléments qui composent le système génèrent une hypercomplexité, et des couplages étroits.
- Migration des activités : les liens fonctionnels entre plusieurs niveaux décisionnels créent un système sociotechnique complexe.

D'autres décrivent indirectement la complexité :

- La gestion de la sécurité dans les systèmes de production : la notion de complexité est directement issue de travaux antérieurs.
- La résilience : la complexité est décrite à travers la difficulté constatée à gérer le système, la notion de variabilité de la performance, et la notion d'incertitude associée aux barrières de sécurité.

En outre, chaque modèle décrit, avec différents degré de précision, l'impossibilité de décrire l'ensemble des mécanismes qui caractérisent le système (interdépendances, couplages, liens décisionnels). Egalement, les propriétés émergentes sont assez peu traitées par les différents modèles. Seuls les modèles de l'accident organisationnel, et de la résilience, décrivent l'existence de phénomènes systémiques non prévus lors de la conception (conditions latentes, incertitude). Ainsi, le comportement du système, ses différents scénarios de fonctionnement, ne peuvent être parfaitement connus et prédits, dans leur déclenchement, leur déroulement, et leurs conséquences.

L'analyse comparative montre également des limites inhérentes à l'ensemble des modèles. Une première limite concerne leur apport. Les cinq modèles analysés abordent la notion de complexité sous un angle descriptif. Ils apportent des éléments descriptifs (conditions latentes, couplages, variabilité de la performance) de la complexité et de ses effets. Pour

autant, peu d'éléments sont proposés quant à la manière de traiter cette complexité. L'opérationnalisation de chaque modèle semble difficile à mettre en œuvre. Comment détecter concrètement une condition latente ? Comment définir son niveau de criticité ? Ou placer la limite de fonctionnement sûr d'un système ?

La seconde limite à dépasser concerne la focalisation sur le manager opérationnel. En effet, dans chacun des modèles, la complexité est décrite de manière globale et sans dimensions multiples. Cependant, la complexité, telle qu'elle peut être perçue par le manager opérationnel, n'est pas décrite. Les différentes définitions proposées ne permettent pas de décliner cette complexité globale du système, en complexité davantage située, au niveau de sous-systèmes (décisionnel, fonctionnel...). Par exemple, il serait intéressant d'avoir une perspective précise de la complexité du système, au niveau du manager. Comment cette complexité globale se décline-t-elle à son niveau fonctionnel ? Est-ce les mêmes effets de la complexité sur l'ensemble des niveaux ?

Au regard de ces deux limites, on peut avancer que les différents modèles de production de sécurité proposés ne permettent pas de répondre au défi de la complexité, pour le manager opérationnel. Deux questions restent en suspens. La première question concerne la définition d'une complexité située du point de vue du manager opérationnel. La seconde question est celle de la gestion de cette complexité.

Le défi de l'érosion du temps

Au sein d'un système sociotechnique complexe, le défi de l'érosion du temps est défini comme la problématique de prise en compte des effets cumulés d'évènements a priori indépendants, mais pouvant, par effet cumulatif, générer des conséquences importantes. Au regard de notre analyse comparative, l'idée d'érosion du temps n'est pas directement prise en charge. Pour autant, on peut considérer qu'elle est présente de manière sous-jacente. Et deux principales tendances se dégagent de notre analyse.

Premièrement, plusieurs modèles, plutôt descriptifs, traite la question de l'érosion du temps à travers le phénomène de dégradation lente (ou progressive) du niveau de sécurité du système. Il s'agit du modèle de l'accident organisationnel. L'accident est le résultat d'une dégradation des barrières de défense, jusqu'à un point ou la dynamique accidentelle est devenu possible. Le second modèle est celui de la migration des activités du système.

L'accident est rendu possible par la dérive du système vers une zone qui se situe au-delà des frontières de sécurité et de rentabilité.

Au cours de l'érosion du temps, la deuxième tendance traite la question de l'anticipation, et de l'organisation apprenante. Ces modèles sont plutôt prescriptifs. A l'idée d'érosion, ou de dégradation, se substitue l'idée de performance variable, ou de perturbations internes ou externes au système. Cette tendance comprend le modèle des organisations hautement fiables, qui intègre les schémas organisationnels d'anticipation et d'organisation apprenante. Elle comprend également le modèle de gestion de la sécurité dans les systèmes de production, au sein duquel la sécurité est le résultat d'une connaissance profonde du système, et d'une capacité d'apprentissage face à des phénomènes nouveaux. Elle comprend enfin le modèle de résilience, pour lequel l'anticipation est définie comme la capacité d'adaptation du modèle aux perturbations internes ou externes qui influent sur le système. Loin d'être antinomiques, ces deux tendances apparaissent plutôt comme complémentaires. En outre, plusieurs de ces modèles ciblent le rôle du management opérationnel, comme fonction d'anticipation.

Notre analyse comparative montre également des limites communes à tous les modèles. Premièrement, qu'ils soient de la première ou de la seconde tendance, tous les modèles renvoient finalement à l'idée d'une dégradation progressive d'un système de sécurisation construit sur le principe de défense en profondeur. Ce phénomène de dégradation est illustré par une dérive, ou migration du système. Cependant, cette représentation conceptuelle, graphique, n'est proposée qu'à un niveau global du système. Peu de précisions sont proposées quant à la définition de cette dérive au niveau local. Seul le modèle de Reason propose le couple conditions latentes / erreurs ou violations de l'opérateur.

Egalement, les modèles ne donnent que peu de précisions quant à deux aspects importants de l'érosion du temps, qui sont la prise en compte de symptômes systémiques (signaux faibles...), et l'anticipation de phénomènes de dégradation rapide, de rupture. Concernant ces deux questions, certains modèles décrivent les phénomènes. C'est le cas par exemple des signaux faibles au sein du modèle des organisations hautement fiables. Cependant, ils n'apportent pas de solution pour l'opérationnalisation de l'anticipation.

En conclusion, l'analyse des modèles existants montre l'intérêt de l'idée d'érosion du temps, et apporte une réponse conceptuelle, qui est celle de l'anticipation. Pour autant, la

question de la constitution de cette capacité d'anticipation, et notamment au niveau du management opérationnel, reste sans réponse.

Le défi de la décision d'initiative

Le défi de la décision s'articule autour de deux problématiques. La première concerne la construction d'une représentation actualisée de la situation pour le décideur. La seconde problématique concerne la construction d'une argumentation solide et convaincante face à une hiérarchie. Il s'agit de faire reposer la décision sur une réflexion structurée et objective.

Au regard de notre analyse comparative, le défi de la décision est globalement pris en charge par les modèles analysés. Pour autant, aucune tendance ne se dégage, et chaque modèle aborde la question de la prise de décision à travers différents éléments constitutifs, et de manière descriptive et prescriptive. L'inventaire issu de l'analyse est le suivant :

- Définition de l'entité « management opérationnel » : le management opérationnel constitue un niveau décisionnel important dans la gestion des activités, au sein du système sociotechnique complexe de Rasmussen.
- Typologie des décisions : Reason propose une typologie des décisions pouvant conduire à une dégradation des barrières de défense.
- Le rôle du système de gestion de la sécurité : Selon Hale, le système de gestion de la sécurité constitue un proxy intéressant pour le suivi du niveau de sécurité du système.
- Le compromis sécurité / production : plusieurs modèles mettent en exergue l'existence d'un dilemme entre nécessité de production, et règles de sécurité.
- La qualification du manager : plusieurs modèles mettent en avant l'importance de la qualification du manager, en termes de compétences, de niveau d'information, et d'engagement envers la sécurité du système.
- Le modèle de pilotage : la sécurité apparait comme le résultat d'un pilotage des activités fondé sur une boucle de contrôle et de rétroaction.
- Le système d'information : le pilotage du système s'appuie sur un système d'information de la sécurité. Il fournit au décideur des données actualisées sur l'état du système.

Chacun de ces aspects constitue un critère d'efficacité de la prise de décision. Ils permettent la construction d'une représentation actualisée pour le décideur, nécessaire à la prise de décision d'anticipation.

En outre, notre analyse comparative met aussi en lumière des faiblesses relatives à la prise de décision. En effet, chaque modèle n'aborde que partiellement la définition du processus de prise de décision. Deux questions se posent alors. Premièrement, parmi l'inventaire précisé ci-dessus, quels sont les éléments les plus importants pour la prise de décision ? Lesquels sont facultatifs ? La seconde question posée est celle de l'intégration des différents aspects de l'inventaire. Sous quelle forme méthodologique peut-on procéder à l'intégration de tous ces aspects, afin de garantir une décision la plus pertinente, et la plus efficace possible ?

Enfin, notre analyse met également en avant une faiblesse commune à l'ensemble des modèles. En effet, la question de l'argumentation relative aux décisions de sécurité n'est pas directement abordée. A la lecture précise des modèles, il est possible d'identifier ce questionnement de manière sous-jacente à deux aspects de la prise de décision. Tout d'abord, l'argumentation peut être décrite indirectement à travers la définition de la posture du manager, telle qu'elle est définie dans le modèle de la résilience. La décision s'impose alors davantage du fait de la position dominante du décideur, plutôt que de sa pertinence. Egalement, le débat de l'argumentation peut être indirectement abordé par la reconnaissance du conflit existant entre nécessité de production, et besoin de sécurité. Ce débat est présent dans la plupart des modèles de production de sécurité, mais reste à l'état de questionnement.

Au regard de ces éléments, on peut conclure que le défi de la décision est globalement bien pris en charge par les modèles de production de sécurité étudiés. Cependant, la question de l'intégration des différents aspects identifiés dans les modèles, et le débat relatif à la construction d'une argumentation convaincante associée à la décision, restent sans réponse satisfaisante. Comment rassembler les conditions d'émergences d'un processus décisionnel efficace, et convaincant ?

Conclusion de la Deuxième Partie

Construit sur des développements successifs (sureté de fonctionnement, et prise en compte des facteurs humains et organisationnels, analyse systémique), le modèle de sécurité, ou encore de sécurisation, apparait aujourd'hui comme réactif. Les processus de sécurité se sont construits par à-coup et ruptures, en retour d'expérience aux accidents industriels. La crise reste la conclusion d'une rupture brutale. Elle fait prendre conscience du danger, et a imposé aux décideurs soumis à la continuité, une notion de prévoyance qui a peu à peu pris le pas. Pris par la prévoyance, nous sommes allés jusqu'au processus de clairvoyance fondé sur la précaution. Sans reprendre toutes les analyses et concepts difficiles à démontrer dans ce mémoire, ce glissement a imposé la gestion du risque comme un objectif incontournable dans le processus de sécurisation en amont. Et les résultats obtenus sont assez exceptionnels, nous engageant ainsi sur une dynamique du risque Zéro.

La gestion du risque a effacé la possible occurrence de l'accident. L'accent est porté sur la prévention, et la mise en place de barrières de sécurité. S'il a permis de baisser significativement le nombre d'accidents, cela soulève de nouvelles problématiques managériales. Augmentation à long terme du niveau de risque, et découplage entre règles de gestion et leurs effets, poussent à explorer de nouvelles voies de réflexion.

Cinq des principaux modèles de production de sécurité ont été retenu au filtre de l'expertise que nous voulions mener. Et leur analyse a permis de mettre en avant leurs limites, quant à la capacité à répondre aux trois défis de la complexité, de l'érosion du temps, et de la décision. Ainsi, soumis à la gestion du quotidien et aux maintiens des activités, l'altération de la capacité du manager à faire face à ces défis peut le placer dans une situation de rupture managériale. Dans ce processus, le manager est soumis à des grilles de compréhension du système qui masquent son sens critique (lié au doute), perd la maitrise des activités.

Si cette analyse est concluante, elle a cependant des limites. Premièrement, le choix porté sur les cinq modèles de production de sécurité peut être remis en question. En effet, chaque modèle est issu d'une tradition de réflexion plus large. L'analyse théorique aurait pu porter sur un seul modèle uniquement, et ainsi le décrypter dans la profondeur du champ scientifique associé. Cependant, le choix de la diversité et de l'analyse comparative relève d'une justification méthodologique. En effet, l'objectif initial de l'étude n'est pas de

préparer une contribution précise et relative à un modèle, et inscrite dans un champ disciplinaire unique. Il s'agit de comprendre les différents modèles et méthodologies disponibles pour produire la sécurité au sein d'un système industriel à risque.

Egalement, d'autres modèles ont été écartés. Et plus particulièrement, le modèle de normalisation de la déviance aurait été pertinent dans cette analyse. Le choix de ne pas traiter ce modèle se justifie au regard de deux critères. Tout d'abord, les ressources limitées de l'étude ont imposé un nombre maximum de modèle à prendre en compte. De plus, les travaux de Vaughan ont porté sur un type de système particulier, qui est certes à risque, mais dont le mode de fonctionnement diffère quelques peu des systèmes étudiés par les autres modèles, et notamment en terme de type de technologie mise en œuvre, culture professionnelle, et de structuration administrative.

Face à la gravité des conséquences associées à l'occurrence d'un accident majeur, la possibilité d'une rupture managériale impose finalement la question de l'aide à la décision. Comment structurer l'environnement du manager pour éviter cette rupture ?

Résumé de la Deuxième Partie

L'objectif de cette deuxième partie est d'analyser les principaux modèles de production de sécurité au regard des trois défis identifiés pour le manager opérationnel.

En effet, le XXème siècle a été le berceau de nombreuses avancées scientifiques en matière de gestion de la sécurité industrielle. Le modèle de sécurité s'est construit grâce à des développements successifs. D'abord la sureté de fonctionnement, puis le développement des facteurs humains, et enfin les facteurs organisationnels et systémiques. Une mise en perspective de ces développements scientifiques, des dates d'accidents industriels majeurs, et des avancées réglementaires, nous permet de constater la logique de ce modèle. La sécurité industrielle est construite sur la réactivité. Elle s'est constituée par à-coup, en réponse aux accidents industriels. C'est également une sécurité de substitution. Le risque s'est substitué à la crise. La gestion du risque a effacé la possible occurrence de l'accident. L'accent est porté sur la prévention. Les avancées en termes de sécurité ont été significatives, et ont permis de repousser plus loin le doute. S'il a permis de baisser significativement le nombre d'accidents, ce modèle atteint des limites. Augmentation à long terme du niveau de risque, fortes contraintes normatives, et découplage entre règles de gestion et leurs effets, poussent à explorer de nouvelles voies de tranquillisation, vis-à-vis d'un risque majeur.

Au sein de ces grands courants, des disciplines issues des sciences de l'ingénieur, et des sciences humaines et sociales, ont cherché à apporter de nouvelles manières de compréhension des mécanismes de l'accident, et de production de sécurité. Cinq des principaux modèles de production de sécurité ont été sélectionnés. Et leur analyse a permis de mettre en avant leurs limites, quant à la capacité à répondre aux trois défis de la complexité, de l'érosion du temps, et de la décision.

Ainsi, dans la gestion quotidienne des activités, l'altération de la capacité du manager à faire face à ces défis peut le placer dans une situation de rupture managériale. Le manager n'a pas plus le sens critique du système. Il n'en détecte plus les faiblesses. Il perd la maitrise des activités.

Face à la gravité des conséquences associées à l'occurrence d'un accident majeur, cette partie pose finalement la question de l'aide à la décision. Comment structurer l'environnement du manager pour éviter la rupture managériale ?

Troisième Partie

Développer l'écosystème décisionnel pour faciliter la décision managériale

Sous-table des matières #3

Sous-table des matières #3 203
Introduction de la Troisième Partie 205
I. De l'aide à la décision à l'aide à la gestion 207
I.1 La rupture managériale 207
I.2 Les limites de l'aide à la décision 210
I.3 Le recours à l'outil de Gestion 217
II. Développer l'écosystème décisionnel du manager 238
II.1 Le concept d'écosystème 238
II.2 Le manager opérationnel au cœur d'un écosystème décisionnel 243
II.3 Dé complexifier la prise de décision 251
Conclusion de la Troisième Partie 261
Résumé de la Troisième Partie 263

Introduction de la Troisième Partie

Depuis les accidents emblématiques des années 1980, dont certains ont été analysés en première partie, la manière d'appréhender le risque a largement évolué, du centre de gravité technique et technologique, à la gestion et au management. La sécurité s'ouvre alors à des démarches plus globales. Les dimensions organisationnelles, culturelles, politiques, et éthiques de la sécurité ne sont plus négligeables. La sécurité doit être assurée malgré l'existence de défaillances techniques et humaines dans le système industriel.

Au centre du système, le manager opérationnel est un maillon incontournable de la sécurité. Il est être un maillon critique (faible) de la chaine sécuritaire. Dans la dynamique du quotidien, celui-ci cherche à identifier les signaux précurseurs de l'accident. La décision d'initiative se substitue alors au mode de fonctionnement normé et procédural.

Or, dans l'étape difficile de la décision, le manager est confronté à trois défis. Défis de la complexité, de l'érosion du temps, et de la décision s'imposent, et si le manager n'y prend pas garde, l'exposent à la rupture.

Les communautés scientifiques ont depuis plusieurs décennies cherché de nouvelles manières de produire de la sécurité, au sein de système complexes. L'analyse de cinq modèles parmi les principaux a permis d'en identifier la portée et les limites. Face aux trois défis, le fonctionnement du manager doit être réfléchi, et une aide à la décision est nécessaire.

Dans ce cadre, quelle aide à la décision apporter au manager opérationnel, au sein de systèmes socio-techniques complexes ?

Le manager fait également face à l'ambiguïté. Au sein de système où la rentabilité est celle de la productivité, le manager est soumis au principe de continuité des activités de production. Formalisée par « des pressions de production », où encore un « conflit production / sécurité », ce dilemme bloque la prise de décision. Le manager attend alors des éléments de légitimation dans le flux continu des évènements, et décide parfois trop tard.

Pour répondre à cette problématique, cette troisième partie se décompose selon le plan suivant. Après avoir explicité la notion de rupture managériale, une première sous-partie analysera les limites de deux principales approches d'aide à la décision.

Enfin, une deuxième sous-partie proposera un regard décalé sur le manager, à travers son écosystème décisionnel. Des pistes de réflexions seront également proposées pour son développement.

I. De l'aide à la décision à l'aide à la gestion

Complexité, érosion du temps, et décision sont trois défis qui s'imposent au manager. Quel support apporter au manager, plongé dans de nombreuses situations décisionnelles quotidiennes ? Pour répondre à cette question, cette première sous-partie propose d'abord d'identifier les effets des trois défis cités à travers la notion de rupture managériale. Ensuite, deux réponses possibles, parmi les principales voies de support à la prise de décision seront analysées : l'aide à la décision, et le recours aux outils de gestion.

I.1 La rupture managériale

Afin de remplir parfaitement sa fonction, on peut supposer que le manager opérationnel a une compréhension parfaite du système qu'il gère. Il a connaissance des aléas, des erreurs, des écarts de procédure, des ajustements, des modifications de ressources, des absents, des malades... Il peut ainsi prendre en compte tous ces aspects du quotidien, et les traduire en décision opérationnelle. Repousser une intervention de maintenance, rappeler du personnel, limiter les activités de production, réorganisation les tâches, sont autant des décisions de prudence qui permettent de maintenir un système de production en activité, et dans des conditions de sécurité acceptables. Le manager pilote parfaitement les activités dont il a la charge.

Cependant, l'analyse d'accidents industriels passés, réalisée dans la première partie, a montré toute la difficulté associée à ces schémas. Après chaque accident, la question de la prévention et de la prudence est posée, face à des systèmes de production dont on ne peut revendiquer la complète maitrise. Au cœur des évènements, l'analyse fait état d'une situation dégradée pour le manager, qui n'a pu prendre la décision de stopper les activités avant la catastrophe.

Au-delà du cadre contraignant de la procédure, et de l'injonction de sécurité envisagée (Agulhon et al., 2014), c'est tout l'environnement décisionnel qui doit être questionné. Loin du monde idéal décrit ci-dessous, la première partie de ce travail a montré que complexité, temps, et décision sont trois défis qui s'imposent au manager opérationnel.

Dans la gestion quotidienne des activités, l'altération de la capacité du manager à faire face à ces défis peut le placer dans une situation de rupture managériale. Cette situation peut être définie comme la perte de maitrise du pilotage des activités. Le manager n'a plus la critique du système. La variabilité des situations qui se présentent ne lui permettent plus de réagir. Il perd sa capacité d'anticipation. La rupture managériale n'est pas forcément visible, ni complète et peut se manifester différemment suivant la situation. Mais elle peut se matérialiser de différentes manières :

- Le manager possède une vision partielle de la situation.
- Il ne prend pas en compte certains phénomènes systémiques (signaux faibles...).
- Il ne comprend pas l'état du système.
- Il n'anticipe pas les situations à venir.
- Il accepte des écarts aux procédures, sans s'interroger sur leurs conséquences.
- Il ne décide pas. Il se réfère uniquement aux règles en place...

Cette situation est problématique dans la mesure où les règles de fonctionnement ne correspondent plus à la réalité des activités. La réalité du terrain se substitue aux analyses de risques théoriques, et les conséquences pour le système peuvent être importantes. En effet, elle peut, à long terme, le placer dans un état propice à l'accident.

Une modélisation de ce phénomène est proposée dans le schéma ci-dessous (Figure 33). La bulle de gauche correspond à un état normal du système. Les meilleures techniques disponibles en termes de sureté de fonctionnement ont été choisies. Les normes sont appliquées, et les réglementations respectées. Le système de gestion de la sécurité, et le pilotage opérationnel permettent une adaptation du fonctionnement du système aux différentes perturbations rencontrées. Toutes ces stratégies permettent de revendiquer un risque calculé, et une sécurité industrielle maitrisée.

Or, ce risque calculé devient inefficace face à l'incertitude, et à la présence de signaux de risques. Le manager se retrouve alors dans une situation décisionnelle ambiguë, qu'il doit lui-même assumer. Enjeux de production et de sécurité se confronte au regard du principe de continuité d'activité.

Dans cette situation, la dégradation de l'environnement décisionnel du manager le place lentement dans une situation de rupture managériale. Le manager ne joue plus son rôle de décideur, et le système change d'état. Il peut être qualifié d'hasardeux. Son fonctionnement

n'est plus remis en cause. Il devient de plus en plus sensible et vulnérable aux perturbations. Son niveau global de sécurité se dégrade, jusqu'à un point ou la sécurité repose sur les marges de sécurité. Le système de gestion n'a plus la bonne compréhension du fonctionnement du processus de production. A titre d'exemples, on peut citer une méconnaissance de l'état réel des installations, ou encore l'avalisation récurrente d'écarts aux procédures de sécurité. Le niveau de confiance, et d'efficacité, associé aux barrières de défense est faible. C'est la situation des presqu'accidents, et des incidents. Le risque de perte de contrôle du processus de production, et le risque d'accident industriel majeur, augmentent.

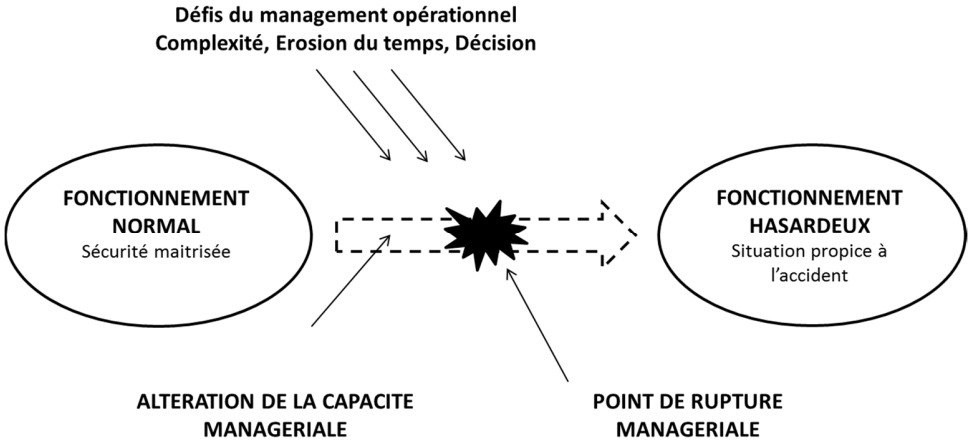


Figure 33 : Dynamique d'émergence de la rupture managériale

En outre, la situation de rupture managériale peut être compensée. D'autres niveaux décisionnels peuvent suppléer au déficit d'un manager opérationnel. Cela peut être par exemple le cas entre manager de production, et manager responsable de la gestion de la sécurité, ou encore des niveaux hiérarchiques différents dans le même département. La situation de rupture managériale peut également être masquée par une prise d'autonomie au niveau opérationnel. Les agents outrepassent leurs prérogatives, et prennent alors la liberté d'agir dans l'intérêt du système.

Dans un contexte où les processus sont dynamiques et l'information continue, l'environnement décisionnel du manager doit être repensé, pour éviter la rupture.

I.2 Les limites de l'aide à la décision

Dans le cadre contraint et structuré d'une entreprise, le manager opérationnel doit remplir son rôle. Depuis les développements de Mintzberg (1984), la fonction de manager est mieux définie. Parmi les dix rôles du cadre définit par Mintzberg, il est ceux de concevoir les règles de gestion, et d'assurer un rôle décisionnel au sein de l'entité structurel qu'il anime. Pourtant, l'existence de la décision, comme objet sociologique, fait encore débat (Urfalino, 2005). Embrassée assez récemment de manière générique, telle que la critique de la décision de Sfez (1976), jusqu'aux derniers travaux appliqués au risque industriel (Kongvisk et al., 2015), la littérature semble formaliser non pas une, mais plusieurs types de décisions, plus dans des champs scientifiques différents. Pour imager ces propos, Scherpereel (2006) propose une taxinomie de plusieurs dizaines d'approche de la décision, en fonction des contextes scientifiques. Différentes recherches en gestion ont alors attribué un rôle important à l'utilisation de l'intuition par les managers dans leurs pratiques décisionnelles. Dans un environnement turbulent, le manager à recours à l'intuition.

Qu'est-ce que l'intuition ?

Cette notion revêt plusieurs acceptions, parfois même contradictoires. Pour certains, l'intuition serait irrationnelle, équivalente à un sixième sens. Pour d'autre, celle-ci est liée à l'expérience, et s'appuie sur des connaissances emmagasinées et réveillées par un problème donné. Selon Mintzberg, (1984), l'intuition ne peut être expliquée, écrite et ne peut être, non plus, décomposée, ordonnée, et contrôlée. Il s'agit d'un processus mystérieux, caché au plus profond du subconscient, et sujet à la plupart des émotions humaines. Plusieurs essais de définition de l'intuition sont regroupés en revue de littérature par Akinci, (2012), ou encore Dammak (2013). Pour autant, selon Canet et al. (2012), dans le champ du management, la définition de Dane et al. (2007) est souvent retenue : l'intuition est un processus non conscient impliquant des associations qui sont produites rapidement et dont résultent des jugements chargés d'affectations. Il faut donc inclure dans ce concept à la fois le processus (l'intuition) et les manifestations de celui-ci (les intuitions). L'intuition renvoie à des situations courantes dans la vie des organisations : des situations où en quelques secondes, une sorte de « préconscient » met en évidence des interactions entre des données acquises via l'expérience, des réflexions, des rencontres, des lectures, des hypothèses sans lien apparent, qui ont été accumulées au cours des semaines, des mois voire des années passés. Selon Dammak (2013), l'intuition se définit par ce qui la nourrit. L'expérience, la

connaissance de l'environnement, les caractéristiques personnelles du décideur, et la confrontation des fruits de l'intuition à la réflexion a posteriori sont des facteurs qui contribuent à la construction d'une intuition. Elle se définit également par son rôle. L'intuition est un catalyseur de la prise de décision. Par son principe « divinatoire », elle permet de sentir l'évolution des choses. Elle est aussi anticipatrice. Elle permet d'estimer les conséquences des décisions et permet d'être l'étincelle génératrice d'idées.

Canet et al. (2012), s'appuient des définitions de Sadler-Smith et al. (2004), et de Dane et Pratt (2007) afin de définir des caractéristiques générales de l'intuition. Selon Sadler-Smith et Shefy (2004), « l'intuition est un processus implicite […] (1) dont la vitesse d'opération est plus lente que l'instinct, mais plus rapide qu'une idée ; (2) probablement en lien avec des modèles dérivés de la mémoire des individus, avec des apprentissages implicites, des événements significatifs en termes d'émotions ou des archétypes universels ; (3) qui peut se combiner avec de la rationalité analytique ; (4) qui est holistique, réactif et automatique ». Selon Dane et Pratt (2007), « l'intuition est un processus non conscient impliquant des associations qui sont produites rapidement et dont résultent des jugements chargés d'affectations. Il faut donc inclure dans ce concept à la fois le processus (l'intuition) et les manifestations de celui-ci (les intuitions), bien que ces deux aspects du phénomène ne doivent pas être confondus ». Canet et al. (2012) proposent les caractéristiques suivantes :

- Si nos jugements intuitifs sont clairement accessibles à notre pensée consciente, le processus intuitif n'est pas conscient (nous n'avons pas conscience des règles qui ont permis l'élaboration de notre jugement).
- L'intuition est rapide car elle est perception immédiate de la connexion possible entre différentes idées.
- Les émotions et l'affectif sont un composant essentiel de nos intuitions. Elles orientent les associations effectuées dans le processus intuitif.
- Il convient de distinguer l'intuition de l'instinct (qui est un schéma comportemental inné) et de l'habitude (représentant une conduite acquise et non remise en question, par inertie cognitive, comportementale ou morale).
- L'intuition implique des associations entre des stimuli issus de l'environnement et des catégories, formes ou patterns inconscient stockés dans notre mémoire.

Si l'intuition est parfois encouragée (Vaughan, 1996), elle est aussi perçue comme un facteur de risque dans la prise de décision. L'intuition peut favoriser une prise de décision

rapide (il n'y a pas de comparaison lente et laborieuse entre plusieurs options), réflexive (car nourrie d'analogies avec des expériences antérieures) et économe en attention demandée au décideur (le mécanisme étant non conscient). Mais l'intuition expose le décideur a ses propres biais cognitifs (Tversky et al., 1974), (Arnott, 1998), affectifs (Slovic et al, 2007) et émotifs (Hollings, 2013). L'habitude, l'instinct, ou encore les émotions se substituent parfois au processus de décision intuitif. Sans connaissance de ces principes, la décision intuitive n'est plus active, éclairée et digne d'un certain niveau de confiance, mais elle est réactive, émotive et peut être infondée vis-à-vis du cadre décisionnel. Parfois, celle-ci peut être bloquée. L'indécision prime alors, indiquant la faillite du rôle du manager, et menant parfois jusqu'à la panique de l'Homme (Laclémence, 2010).

L'aide à la décision comme support du manager

L'aide à la décision trouve ses fondements dans la recherche opérationnelle. Celle-ci se définit comme l'ensemble des méthodes scientifiques visant à fournir à des décideurs une assise rationnelle à la prise de leur décision (Heger, 2006). L'objet ici n'est pas de proposer une revue précise de la littérature sur le sujet. Une analyse généalogique de l'aide à la décision est par ailleurs proposée par Tsoukiàs (2006). Il est cependant utile de rappeler que l'aide à la décision s'est fortement développée dans les années 70, en réponse aux critiques faite à la recherche opérationnelle. En effet, La démarche de recherche opérationnelle était fortement liée au cadre conceptuel proposé par la théorie classique de la décision qui repose sur les hypothèses implicites suivantes (Simon, 1947) :

- Le décideur possède toujours une bonne connaissance du problème et des contraintes qui lui sont liées ;
- Tout problème peut être formulé comme un problème de recherche d'efficience ou d'efficacité ;
- Le décideur dispose de l'ensemble des ressources et des informations nécessaires pour l'identification de la solution à apporter.

Or, les observations menées par Simon (1947) sur la prise de décision dans les organisations ont révélé un tout autre contexte décisionnel. Les situations rencontrées sont de multiples natures : gestion des ressources, ajustement du rythme de travail, modifications des règles de production, ou encore des décisions relatives à la sécurité du process industriel. Face à ce type de situation, le manager doit se positionner face à une

organisation évolutive, dans un environnement qu'il ne perçoit pas parfaitement. Les observations menées par Simon (1983) révèlent un contexte décisionnel incompatible avec un processus de décision objectivement rationnel. Selon Simon, la décision n'est pas le résultat d'un choix comparatif entre plusieurs solutions possibles, mais plutôt un processus de construction cognitif aboutissant à une décision « acceptable ». Cet écart à la rationalité objective peut s'expliquer au regard de trois raisons. Premièrement, la rationalité exige la connaissance parfaite et l'anticipation des conséquences de chacun des choix. En réalité, les connaissances disponibles sont toujours partielles. Deuxièmement, comme il s'agit de conséquences futures, l'imagination doit compenser le manque d'expérience. Ce processus reste cependant imparfait. Troisièmement, la rationalité oblige à choisir entre diverses alternatives possibles. En pratique, le décideur n'envisage qu'un nombre très limité de cas. Son imagination se révèle incapable de concevoir l'ensemble des solutions possibles. Selon Simon, l'être humain recherche la rationalité, mais est gêné par les limites de son savoir. Il a donc mis au point des procédures de travail qui lui permettent de surmonter partiellement cette difficulté. Ces procédures consistent à prendre l'hypothèse que le monde peut être décrit avec un nombre limité de variables et leurs conséquences. Il n'est pas possible de mobiliser des ressources suffisantes pour distinguer ce qui relève des causes et des effets. Le décideur est ainsi amené par exemple à exclure l'ensemble des effets indirects de sa décision. La théorie de l'auteur appelée théorie de la rationalité limitée, stipule alors que les décideurs adoptent la première solution trouvée qu'ils jugent subjectivement satisfaisante, sans rechercher une hypothétique solution « optimale » (Simon, 1983).

Face aux limites explicitées ci-dessus, Roy (1985), Roy et al., (1993), Tsoukiàs (2006) ainsi que Bouyssou et al. (2006) proposent de considérer une vision dite constructiviste de l'aide à la décision. Contrairement à la présupposition de l'existence d'une vérité objective, donc indépendante des perceptions que peuvent avoir les acteurs qui l'observent ; l'approche constructiviste ne cherche pas à identifier une quelconque vérité préexistante. Elle s'intéresse plutôt à construire un modèle de rationalité qui satisfait d'une part les préférences du décideur et d'autre part les conditions de rigueur scientifique qu'introduit l'analyste du fait des méthodes et outils qu'il mobilise (Mazri, 2007).

Pour cela, elle réfute l'idée d'une formulation unique d'un problème de décision, présente dans la théorie de la décision classique. L'aide à la décision n'est plus un processus d'optimisation, au sein duquel le décideur doit adapter son information et sa perception du problème au modèle théorique, mais un processus interactif organisé en vue de produire

des recommandations. Elle considère qu'une fois que le décideur à compris son problème, la recherche de solution devient simple (Tsoukiàs, 2006).

Tsoukiàs (2006) propose alors un processus d'aide à la décision, basé sur les considérations suivantes :

- Au moins deux participants : le décideur et l'analyste (l'aidant).
- Au moins deux objets du processus, les préoccupations du décideur, et les motivations de l'analyste.
- Un ensemble de ressources qui inclut la connaissance que le décideur a sur le domaine de ses préoccupations, la connaissance méthodologique de l'analyste, et le temps disponible.
- Un objet de convergence qui consiste en une représentation partagée entre les participants des préoccupations du décideur.

Ce processus est constitué des étapes suivantes (Figure 34) :

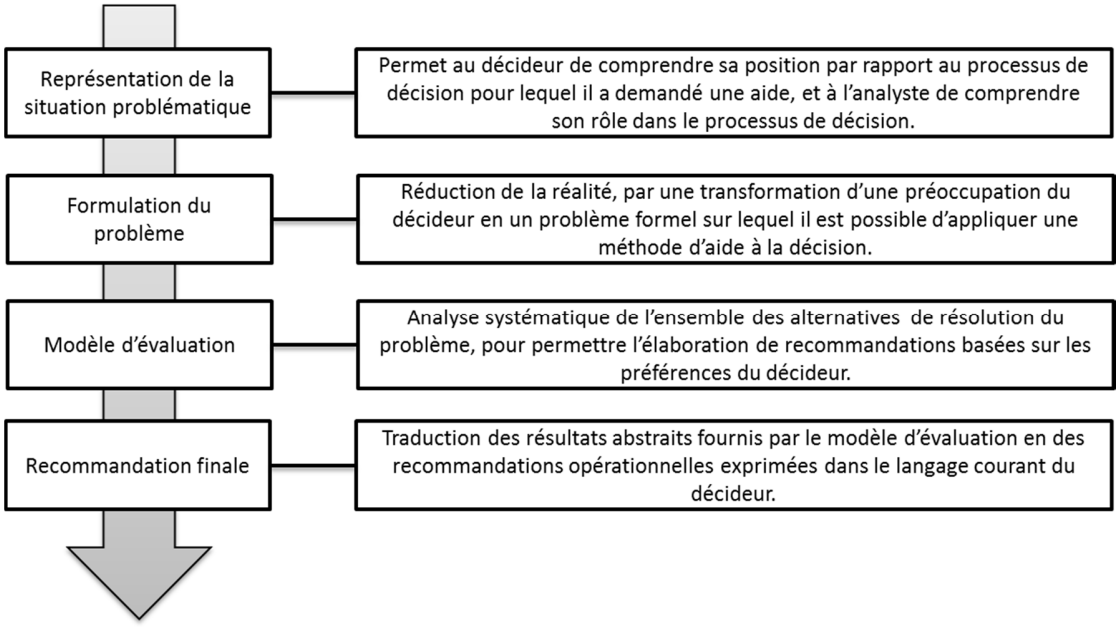


Figure 34 : Processus d'aide à la décision, adapté de Tsoukiàs (2006)

L'approche d'aide à la décision est intéressante parce qu'elle prend en charge les questionnements portés par notre analyse. L'aide à la décision a pour objectif d'aboutir à la

prise de décision. C'est une démarche structurée et méthodique qui vise à aider le décideur à réduire l'ambiguïté de la situation décisionnelle à laquelle il fait face, et construire une représentation précise et utile qui permette la prise de décision (il s'agit plus précisément d'une co-construction entre le décideur et l'analyste). Tsoukiàs (2006) propose également une autocritique de l'utilisation d'une approche formelle et abstraite, qui constitue le sous-bassement du processus d'aide à la décision. Cette approche plusieurs avantages :

- Elle permet à tous ceux qui participent au processus de prise de décision de parler le même langage, ce qui, a priori, augmente la transparence du processus de prise de participation.
- Elle permet d'identifier les structures sous-jacentes aux problèmes traités et permet donc éventuellement de réutiliser ses structures.
- Elle évite les biais du raisonnement humain dus à la tradition et à la formation.
- Elle évite les erreurs associées à l'utilisation informelle de méthodes formelles.

Une approche formelle et abstraite présente également quelques inconvénients :

- Elle est beaucoup moins efficace si on la compare à la puissance et à l'efficacité de la communication naturelle.
- Elle a toujours un coût (pas toujours monétaire).
- La réduction de l'ambigüité peut être indésirable.
- Elle représente l'imposition d'un carquant à l'intuition et à la créativité de l'esprit humain.

L'aide à la décision constitue une ressource intéressante dans le sens où elle contribue à structurer et faciliter la prise de décision, en apportant du contenu méthodologique externe, et en favorisant une posture de remise en question du décideur. Elle repose sur les hypothèses implicites suivantes :

- Le décideur a la capacité à identifier a priori les situations nécessitant le recours à un processus d'aide à la décision.
- Le décideur possède les ressources, et a la possibilité de recourir à un analyste externe, et de mettre en œuvre un processus d'aide à la décision.
- La situation décisionnelle est suffisamment stable pour que le processus d'aide à la décision puisse aboutir à des recommandations utiles.

Face à ces hypothèses, l'analyse des accidents menée dans la première partie de ce travail a révélé un contexte décisionnel différent, pour le manager, et dans le cadre d'activités quotidiennes de gestion :

- Le manager ne peut anticiper l'ensemble des situations décisionnelles qu'il va rencontrer, et notamment celles porteuses d'ambigüité.
- La majorité des situations décisionnelles rencontrées par le manager nécessite une réponse rapide.
- Les situations décisionnelles rencontrées sont dynamiques et évoluent rapidement.

On peut donc en conclure que l'aide à la décision, telle qu'elle est décrite ci-dessus, ne permet pas de répondre à la problématique de structuration de l'environnement décisionnel du manager opérationnel.

I.3 Le recours à l'outil de Gestion

Dans le but d'améliorer sa compréhension du système, le manager peut également s'appuyer sur des outils de gestion (tableau de bord, indicateur....). La littérature s'accorde à donner une définition assez consensuelle d'un outil de gestion. C'est un outil de formalisation de l'activité organisée (Moisdon, 1997). La question de l'implantation des outils de gestion, et des dynamiques de changement qu'elle implique, occupe une place particulièrement importante dans la réflexion sur les organisations contemporaines (David, 1998 ; Moisdon, 1997 ; Alcouffe et al., 2009). L'engouement pour les outils a fait écho à l'histoire des organisations. De nombreux auteurs constatent aujourd'hui la prolifération d'outils de gestion (De Vaujany, 2006).

Il peut être défini à l'aide de plusieurs caractéristiques :

- Il est ancré dans le concret, et fonctionne de manière continue : l'outil de gestion fonctionne comme un script qui scénarise l'action d'un ensemble d'individus de l'organisation en vue d'une plus grande performance (Detchessahar et al., 2007).
- Il est le support d'une finalité d'action, et recherche son efficacité : pour cela, il a besoin d'être approprié. Il est formé et déformé par ses utilisateurs. Chacun joue avec les règles, et les détourne (De Vaujany, 2006). Il est donc support à la création ou à la modification de règles.
- Il est un outil d'application de la stratégie : mais dont l'action finale dépend également de la vision du manager qui utilisera l'outil de gestion. l'enjeu porte souvent sur la bonne appropriation de ces outils par les acteurs de l'entreprise et sur leur capacité à appuyer la stratégie (Bourguignon et al., 2004). C'est notamment le cas du management opérationnel, qui construit et déconstruit les discours stratégiques de l'organisation. C'est donc un acteur essentiel de la fabrique de la stratégie mise en œuvre (Rouleau, 2005).
- Il est de nature double : il est d'abord technique, tangible, matériel, c'est-à-dire que son contenu matérialise et objective un aspect ou un comportement d'un élément de l'organisation. Il est également social, dans la mesure il est construit par et pour l'acteur organisationnel. Il est étroitement lié aux représentations des acteurs. L'outil de gestion est donc centrée sur l'action organisationnelle, laquelle nécessite des objets artificiels créés par et pour l'acteur (Mazars-Chapelon et al., 2000). Il est

donc un contenu, mais également un processus d'appropriation. Il peut donc faire l'objet d'usage prévus, mais également imprévus (Oiry, 2011).

- Il s'intègre à un réseau d'autres outils et pratiques de gestion de l'organisation : il est intégré de façon systématique et codifiée, et dans une logique fonctionnelle (De Vaujany, 2006).

Un outil de gestion agit comme une lunette, qui filtre, et structure les éléments de l'organisation. Il réduit la complexité, et donne du sens à un environnement rapide et perturbé. Il apparait alors, de manière générique, comme une réponse intéressante à notre problématique de prise de décision.

Cependant, plusieurs accidents industriels majeurs ont montré la limite. Et de nombreux rapports d'enquête (Bhopal, Texas City, Deepwater Horizon...) ont remis en cause la conception, et l'utilisation, des outils de gestion. Dans la section suivante, trois types d'outils sont analysés : les audits, les indicateurs de pilotage, et la prise en compte des signaux faibles. Il s'agit d'identifier la capacité de tels outils à aider le manager dans sa prise de décision.

Les audits de sécurité

Le recours à l'audit s'est largement développé au sein des entreprises depuis ces vingt dernières années. Il répond à deux objectifs principaux, le contrôle interne, et la certification des systèmes de gestion de la sécurité. Le système de gestion de la sécurité certifié est devenu un instrument des entreprises pour s'assurer un bon niveau de sécurité (Hohnen et al., 2011). Plusieurs tendances peuvent expliquer ce phénomène. Tout d'abord, dans un contexte industriel de compétitivité croissante, la certification des systèmes de management est devenue un levier important de compétitivité des entreprises. En effet, le succès à long terme d'une organisation dépend de sa capacité à améliorer ses opérations, par sa réorganisation interne, ainsi que par la réponse aux exigences de l'environnement de l'entreprise (Vinodkumar et al., 2011). Egalement, le fonctionnement de la certification des SGS répond aux autres certifications déjà existantes dans d'autres domaines, et largement initié par le système de management qualité ISO 9000, au début des années 2000 (Power, 2008). Ainsi, une très grande majorité des grandes entreprises mettent en œuvre des audits. Considérant l'augmentation des accidents industriels, et de leurs conséquences en termes de pertes physiques, d'infrastructures, et d'impacts sur l'environnement, de plus en plus d'entreprises sont volontaires pour les certifications sécurité (Vinodkumar et al., 2011). En

outre, le système de certification représente également un coût. Il est moins prévalent dans les petites entreprises (Grant et al., 2005).

Un système de certification consiste en l'établissement d'un système de contrôle et de régulation dans l'entreprise. Il est évalué et audité par des agents d'audit externes (Hohnen et al., 2011). L'audit est donc un outil de gestion d'entreprise :

1. C'est un outil de contrôle, au sens où il permet de comparer des pratiques de gestion existantes, à un ensemble de pratiques théoriques. Il contrôle ainsi la bonne adéquation de la réalité par rapport à un référentiel d'audit.
2. C'est un outil de régulation : il permet d'identifier et de qualifier les écarts existant entre les pratiques réelles et le référentiel. Il apporte une description des faiblesses constatées, et oriente donc l'entreprise sur les solutions à mettre en œuvre pour les corriger.
3. C'est un outil de suivi de l'évolution : il fait l'objet d'une méthodologie d'analyse définie, ce qui permet une comparaison entre plusieurs audits. Il permet donc de formuler des tendances sur l'évolution du niveau de maitrise.
4. C'est un outil de compréhension : il produit un rapport d'audit situé dans le temps. Il comprend différents niveaux de synthèse. Il donne ainsi différentes représentations de l'entreprise, qui alimentent l'écosystème décisionnel du management.

Selon Robson et al. (2012), le processus d'audit mis généralement en œuvre comprend les étapes suivantes :

1) *Recueil des preuves :* il s'agit de procéder à un recueil systématique de données nécessaires à l'audit, à travers plusieurs techniques complémentaires : utilisation de la documentation, interview d'acteurs, et phases d'observation du terrain.
2) *Evaluation des preuves :* c'est la comparaison entre les données recueillies et le référentiel d'audit, et leur qualification en termes d'acceptabilité.
3) *Transmission des résultats :* c'est la formation des résultats de l'audit. Cette partie comprend la qualification des écarts constatés.

Au-delà de cette définition, on constate que l'audit est généralement utilisé pour évaluer les structures et les processus de l'organisation de la sécurité. Il détermine si oui ou non l'organisation est en conformité avec un ou plusieurs standards (politique de l'entreprise,

réglementation, standards externes), qu'ils soient internes à l'entreprise, ou externe (Robson et al., 2012). Il est également utilisé pour examiner l'efficacité du management des risques. C'est un élément essentiel du système de gestion de la sécurité (Robson et al., 2012). C'est un moyen de mesure direct et complet de la mise en œuvre et l'efficacité du SGS de l'entreprise (Robson et al., 2010).

Caractérisation du processus d'audit

Vinodkumar et al. (2011) ont défini plusieurs critères d'analyse d'un système d'audit :

- *La validité du contenu :* elle fait référence au champ couvert par le référentiel d'audit. Par exemple, un référentiel d'audit exhaustif couvre l'intégralité des éléments du SGS.
- *La fiabilité inter-auditeur :* elle mesure l'écart qu'il peut exister entre plusieurs évaluations réalisées par des auditeurs différents, sur le même objet.
- *La validité du modèle :* correspond à la capacité du système d'audit à bien mesurer ce qu'il doit mesurer en théorie. La validation est généralement réalisée en établissant des hypothèses sur les relations attendues sur les scores d'audit du SGS, testant ces relations avec des méthodes appropriées, pour enfin confirmer les hypothèses.
- *Autres propriétés :* en fonction des contextes et des modèles d'audit, plusieurs autres critères d'analyse, par exemple la cohérence des résultats après une réalisation répétée des audits, ou encore la capacité à détecter précisément les écarts et leurs évolutions dans le temps.

Les résultats quantitatifs de l'audit sont souvent également utilisés par l'entreprise comme des éléments de mesure de la performance. L'audit joue alors un rôle dans les prises de décision. La validité et la fiabilité des audits sont donc des caractéristiques essentielles (Robson et al, 2012) Pourtant, peu de recherches sont disponibles sur ce sujet (Robson et al., 2010). Egalement, le fait de réaliser l'audit par des agents externes, fait supposer l'ajout de qualité au SGS interne, en particulier parce que ce type d'audit présume à la fois d'une concordance entre le système réel et le référentiel, et une focalisation sur l'amélioration continue du système (Hohnen et al., 2011).

En outre, l'attention portée aux caractéristiques de l'audit (fiabilité, validité...) dépend du contexte dans lequel est réalisé l'audit. Dans certains cas, les propriétés de l'audit sont

moins importantes. Par exemple, les audits simples sont parfois utilisés pour évaluer la gestion et la planification des organisations qui commencent la mise en œuvre de leur SGS. De manière similaire, certaines entreprises ont des SGS développés, mais dans lesquels les audits sont utilisés périodiquement seulement pour s'assurer qu'il n'y ait pas de gap majeur dans le SGS. Dans ces deux cas, un système d'audit direct est nécessaire. L'un veut s'assurer de la validité du contenu de l'audit, alors que l'autre entreprise veut s'assurer de la fiabilité de son système d'audit, c'est-à-dire que le référentiel comprend bien tous les éléments du SGS, et qu'il est apte à détecter les gaps. D'autres propriétés du système d'audit peuvent être importante (fiabilité des auditeurs, validité des prédictions, sa réactivité) lorsque l'audit est utilisé dans le cadre d'évaluation de performance : par exemple : benchmarking, déterminer si un niveau de référentiel est atteint, ou processus de monitoring à long terme. La qualité de la mesure peut également être importante lorsque le résultat de l'audit détermine des conséquences organisationnelles (récompenses financières, reconnaissance, opportunité de contrat, ou encore des pénalités). Des conclusions d'audit non-viables, erronées, ou invalides, peuvent conduire à un rapport d'audit erroné. (Vinodkumar et al., 2011).

Enfin, le système d'audit est un processus actif qui a un impact sur les pratiques de gestion. Selon Power (1996) et Strathern (2000), l'audit constitue un processus actif qui « rend les choses auditables ». Dans ce cadre, l'audit et ses mécanismes influencent le SGS, parce qu'il impose une certaine vision et compréhension du système (Hohnen et al., 2011).

Les travaux portant sur le processus d'audit

La pratique des audits tend à se développer. Pourtant, la littérature montre une pauvreté des études portant sur les différentes variables du management de la sécurité, à travers les différents systèmes de certification. Les principaux travaux portent sur des éléments spécifiques de l'audit. Plusieurs recherches sur la certification se sont focalisées sur ses effets positifs, notamment en termes de reconnaissance. Alors que d'autres recherches ont montré son faible impact, et le faible qu'elle soit dominée par la bureaucratie, avec peu de place pour la participation des employés (Hohnen et al., 2011). Plusieurs auteurs ont montré que les audits ne garantissent pas nécessairement le niveau de sécurité espéré (Hohnen et al., 2011). Par exemple, l'explosion d'une raffinerie directement après un audit (Hopkins, 2000). La recherche s'est peu intéressée à la dimension qualitative des SGS. Par exemple, les changements, ou la continuité, des éléments composant le SGS (Hohnen et al., 2011).

Des travaux ont montrés que le processus de certification, qui est spécifique, impacte indirectement le sujet audité (Power, 2003). Robson et al. (2012), ont défini un modèle conceptuel décrivant les facteurs qui affectent la fiabilité et la validité d'un système d'audit de SGS (Figure 35).

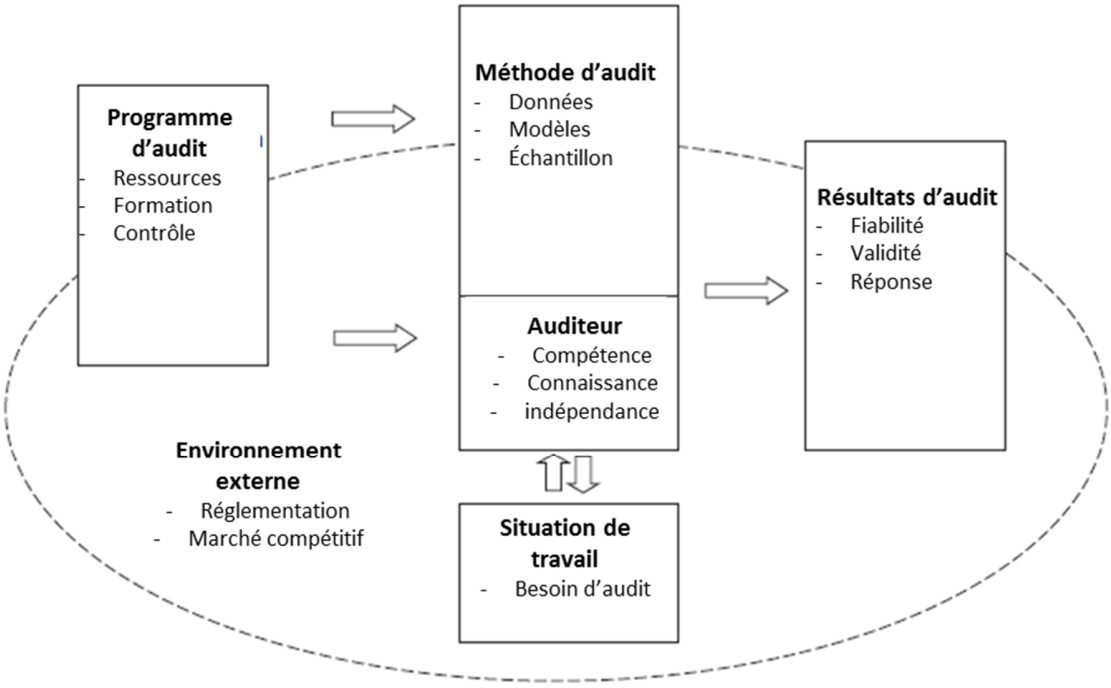


Figure 35 : Modèle conceptuel des facteurs affectant la fiabilité et la validité des audits des systèmes de gestion de la sécurité, adapté de Robson et al. (2012).

Dans ce cadre, le système d'audit est affecté par les caractéristiques de plusieurs éléments :

- *La programmation de l'audit :* correspond aux conditions de préparation et de réalisation de l'audit. Elle comprend des caractéristiques telles que les ressources allouées, le processus de recrutement des auditeurs, la formation des auditeurs...

- *La méthodologie d'audit :* définit la manière dont les auditeurs réalisent l'audit : thème de l'audit, secteur concerné, les sources de données, les modèles de questionnement, les méthodes de mesure et de classement...
- *La qualité des auditeurs :* fait référence au profil des auditeurs : savoirs, compétences, indépendance vis-à-vis de l'entreprise...
- *Les résultats de l'audit :* concerne la qualité des résultats de l'audit : validité, fiabilité...
- *Le contexte de l'entreprise :* définit les attentes de l'entreprise vis-à-vis du processus d'audit : obligation d'audit, besoin d'une nouvelle certification...
- *Les conditions environnementales :* font références aux contraintes et obligations qui s'imposent à l'entreprise, et donc au processus d'audit. Par exemple : obligations réglementaires, contraintes de marché...

Si le système d'audit permet l'évolution à long terme du système de management de la sécurité, plusieurs facteurs peuvent limiter son action et remettre en cause son efficacité. Il est possible d'identifier trois familles : La première est liée à la capacité du système de gestion de l'entreprise à être audité. La seconde famille porte sur l'aptitude de l'outil à réaliser sa fonction d'audit et fournir des résultats utiles pour la remise en question des systèmes de gestion. Enfin, la troisième famille est relative aux conditions de réalisation de l'audit.

Capacité du système de gestion à être audité

La première caractéristique porte sur la capacité du système à être audité. La réalisation d'un audit sur une entreprise ou une organisation nécessite que celle-ci soit « auditable ». Cela signifie que les acteurs et les données nécessaires soient disponibles pour les auditeurs. La majorité des référentiels d'audit, en matière de sécurité, se définissent comme utilisable pour la majorité des entreprises, quelles que soient leurs activités, leur taille, ou encore leur organisation. Pourtant, dans les faits, plusieurs caractéristiques altèrent l'auditabilité d'une organisation.

La première concerne la capacité concrète du système à fournir les données et les disponibilités d'acteurs aux auditeurs. Le développement des systèmes d'information à générés des masses de données considérables. L'audit d'un système en fonctionnement rend difficile la disponibilité des opérateurs et des managers, ainsi que la visite des activités

à risques. En somme, l'ensemble des informations existantes ne peuvent être appréhendées de manière exhaustive.

La deuxième caractéristique porte sur l'acceptabilité du processus d'audit par les acteurs audités. L'audit possède son propre référentiel. Il définit donc la « bonne » vision du système et de son fonctionnement. Il catégorise l'environnement de travail en procédures et technologies. Il apporte sa propre généralisation. C'est l'objet du processus d'audit que d'identifier les écarts entre le fonctionnement théorique du système, et la réalité des pratiques. Mais ce fonctionnement n'est efficace que si la vision du fonctionnement théorique du système est partagée par les acteurs du terrain. Le cas contraire peut conduire à un refus du processus d'audit, et donc son inefficacité.

La troisième caractéristique est relative à la capacité du système à intégrer les résultats de l'audit dans son organisation, et la capacité à faire évoluer ses pratiques de gestion. La dimension de l'audit impose une analyse et une transcription des recommandations dans les pratiques concrètes du système. La mauvaise réalisation de cette étape rend inefficace la totalité de l'audit.

Aptitude de l'outil à réaliser sa fonction d'audit

Plus qu'un système « auditable », une démarche d'audit réussie nécessite que l'outil d'analyse ait la capacité de réaliser sa fonction d'audit, et délivre les résultats escomptés. Cependant, plusieurs limites peuvent altérer la démarche. La réalisation d'un processus d'audit demande une méthodologie lourde. Elle nécessite beaucoup de préparation pour maximiser la phase de récupération des informations. Pour autant, les délais et temps d'audit rendent difficile la compréhension fine du fonctionnement du système pas les auditeurs, et notamment la corroboration par différents types de données. Egalement, les modèles de référentiels ne peuvent capturer qu'une certaine partie du SGS. La généralisation ne peut capturer la diversité et la richesse des situations de terrain. L'audit rend visible une certaine partie du système, sans parfois s'intéresser à son efficacité réelle. Enfin, les motivations de l'entreprise influent sur le processus d'audit. Celui-ci doit alors se positionner entre obligation de résultat positif, et obtention de l'assurance raisonnable qu'aucune anomalie significative ne figure dans le système.

Conditions de réalisation de l'audit

L'audit est un processus qui se superpose à ceux déjà présent dans le système. Tel que défini dans le modèle de Robson et al. (2012), de nombreux facteurs contextuels influencent la bonne réalisation de l'audit. L'efficacité de la démarche nécessite donc un équilibre entre chacune des contraintes. L'émergence de contraintes asymétriques, telles que la redéfinition des finalités de l'audit, peut alors remettre en cause l'ensemble de la démarche. Egalement, la réalisation des audits nécessite généralement le recours à un prestataire d'audit. Le système est alors exposé à un mélange des genres, dans lequel prestation d'audit et conseil de gestion se chevauchent. Le diagnostic indépendant n'est plus découplé des recommandations personnalisées à l'entreprise. Le manque de définition des actions en audit et conseil peut alors divertir l'auditeur de son objectif, et ainsi altérer la qualité du processus global.

Les indicateurs de gestion de la sécurité

La question de la conception et l'utilisation d'indicateurs de performances appliquée à la gestion des risques industriels n'est pas nouvelle (Mazri et al., 2014). Néanmoins, elle a été remise en lumière à la suite de l'explosion de la raffinerie de Texas City, en 2005. En effet, les enquêteurs pointent des faiblesses dans la gestion du site industriel, et notamment dans l'utilisation des indicateurs de performance sécurité. Le Bakel panel (2007) initie alors une réflexion portant sur deux aspects. Le premier concerne la confusion existante entre les indicateurs relatifs à la sécurité du personnel, et ceux relatifs à la sécurité du process industriel. La seconde est relative aux limites des indicateurs de résultats, qui décrivent le comportement du système tel qu'il a été dans le passé (il y a quelques secondes, quelques heures, ou quelques jours...), et préconise l'utilisation d'indicateurs d'activités (leading). Les orientations prises par le Bakel Panel ont ensuite été critiquées par Hopkins. Selon l'auteur, à l'instar du guide émis par le HSE (HSE et al., 2006), le Baker Panel ne fournit pas d'éléments satisfaisant pour distinguer leading et lagging indicators. Cette réponse fut le point de départ d'une discussion au sein de la communauté de la sécurité industrielle sur la définition des indicateurs leading et lagging (Hale, 2009). Le journal *Safety Science* invita des chercheurs et praticiens à répondre à Hopkins (Hale, 2009). Une vingtaine de contributions ont alors alimenté le débat, révélant encore la diversité des compréhensions et la confusion des termes présente dans ce domaine (Hopkins, 2009 ; Allford, 2009). Le but des indicateurs sécurité semble pourtant faire consensus. Le sujet principal des indicateurs

de performance est triple : 1/ surveiller le niveau de sécurité d'un système (que ce soit un service, un site, ou un domaine industriel), 2/ décider, où et quand mettre en œuvre des actions correctives, et 3/ motiver les personnes en position d'agir, à prendre les mesures nécessaires (Hale, 2009). Le débat porte alors sur plusieurs autres aspects des indicateurs : les modèles d'accident sous-jacent à leur conception, les objets et mesure, et les types de mesures à réaliser. Concernant les théories sous-jacentes, plusieurs modèles se confrontent. Les principaux courants sont issus du Triangle d'Heinrich (1931), du modèle en plaques de Reason (1997), ou encore du modèle systémique (Herrera et al., 2008 ; Leveson, 2004). Sur la base de ces modèles, plusieurs types de mesures sont développés. Selon HSE et al. (2006), la mesure de la performance peut être divisée en mesure active, et réactive. «Réactive» signifie identifier et reporter les accidents, et apprendre du retour d'expérience, tandis que « active » signifier fournir un feed-back sur la performance avant que l'accident n'ait lieu. Plusieurs objets de mesures sont développés dans la littérature. Les indicateurs de risque sont issues d'une approche fondée sur le risque (Øien, 2001), alors que le indicateurs de sécurité peuvent être issues de plusieurs approches : performance sécurité (HSE et al., 2006), analyse du nombre d'incidents (Øien, 2008), et résilience (Øien et al., 2010).

Presque dix ans après l'accident de Texas city, la question des indicateurs alimente encore les réflexions. Le terme « indicateurs sécurité » correspond à un parapluie pour une multitude de concept, parfois utilisé de manière interchangeable. Selon Øien al. (2011), ces discussions montrent un manque de connaissances des recherches précédentes développées dans les années 1980 et 1990. Par exemple, le débat portant sur les indicateurs leading et lagging semblent en effet similaire aux travaux sur les indicateurs directs et indirects. Ainsi le besoin actuel n'est pas plus de créer de nouvelles connaissances sur les indicateurs, que de formaliser et structurer cette génération d'indicateurs post-Baker panel.

<u>De multiples guides, avec un objectif partagé</u>

De nombreux guides, référentiels, ou bonnes pratiques ont été édités depuis une dizaine d'années, relatifs à la conception et à l'utilisation des indicateurs de performances sécurité. Les principaux sont mentionnés dans le tableau suivant (Tableau 10).

Nom	Organisation	Date	References
Developing process safety indicators: A step-by-step guide for chemical and major hazard industries.	HSE	2006	(HSE, 2006)
Safety performance leading indicators.	CBA	2009	(CBA, 2009)
Guidance on Developing Safety Performance Indicators.	OECD	2009	(OECD, 2009)
Process Safety Performance Indicators for the Refining and Petrochemical Industries.	API / ANSI	2010	(API, 2010)
Process safety leading and lagging metrics.	CCPS	2011	(CCPS, 2011)
Metrics for Safety Key Performance Indicators for the Performance Scheme.	EC, EASA, EUROCONTROL	2011	(EC, 2011)
Process safety - recommended practice on key performance indicators.	OGP	2011	(OGP, 2011)

Tableau 10 : Principaux référentiels relatifs aux indicateurs de gestion

Une comparaison entre ces principaux modèles révèle une grande diversité des approches utilisées : multiples termes, types d'indicateurs, définitions, objet de mesure, méthode de conception de l'indicateur, et destinataires des mesures (Delatour et al., 2014).

- *Diversité de termes :* process safety indicators, key performance indicators, risk-based indicators, resilience-based indicators, positives performance indicators.
- *Diversité des types d'indicateurs* : indicateur de résultat vs d'activité, d'entrée et sortie de processus, indicateur réactif vs proactif, sécurité du personnel vs sécurité du process, indicateurs direct vs indirects.
- *Diversité des définitions :* par exemple, les mêmes termes leading / lagging peuvent faire l'objet de définitions différentes suivant les référentiels (Hinze et al., 2013).
- *Diversité des objets de mesure :* mesure du risque, de la sécurité, de la performance du système de gestion de la sécurité, de la culture sécurité, de la résilience.

- *Diversité des méthodes de conception :* indicateurs préétablis, méthode de conception fondée sur un modèle d'accident (triangle d'Heinrich, Modèle en plaque de Reason), méthode fondée sur le cycle de vie de l'indicateur, intégration de l'indicateur dans le système de gestion de la sécurité (Reiman et al., 2012).
- *Diversité des destinataires de la mesure :* opérationnel, management, corporate, autorités de contrôle.

La comparaison des principaux guides sélectionnés montre une diversité des approches de conception et d'utilisation des indicateurs de mesure des performances sécurité. Pourtant, un même élément se retrouve dans l'ensemble des guides. Le but des indicateurs, et leur légitimation apparait dans chacun des documents étudiés. Il est intéressant de constater un foisonnement des types d'outils disponibles, répondant à une même légitimation et à un même but. Au moins deux causes expliquent ce constat. Premièrement, les domaines industriels qui alimentent la réflexion sur les indicateurs ne possèdent pas le même niveau de connaissance. Chimie, nucléaire, transport... ont des niveaux de compréhension différents du fonctionnement de leur organisation. Les avancées dans la conception des indicateurs sont disparates. Deuxièmement, cette diversité des concepts peut s'expliquer par un débat qui perdure encore dans la littérature scientifique sur les outils de mesure de la performance appliqués aux risques industriels.

Le besoin de formalisation d'une nouvelle génération d'indicateurs de gestion

La plupart des indicateurs proposés répondent au même objectif d'anticipation des accidents industriels. Cependant, ils se basent sur des modèles hétérogènes, ils cherchent à mesurer des aspects différents des organisations, et sont conçus et mis en œuvre selon des méthodes diverses.

Egalement, nous constatons que la littérature scientifique semble faire consensus sur la nécessité de mesurer les performances sécurité. Pourtant, la question de la conception et de l'utilisation des indicateurs alimente encore le débat. L'utilité de la mesure des performances sécurité dans le cadre de la maitrise des risques industriels n'est plus à démontrer. Pourtant, la conception et l'utilisation des indicateurs constitue encore un challenge, tant pour la sphère scientifique que la sphère industrielle.

Challenge relatif à la conception des indicateurs :

- *La diversité des champs à mesurer :* peut conduire à une grande quantité d'informations à gérer. Il n'est pas possible de suivre de manière précise une telle quantité d'indicateurs, qui nécessite beaucoup de ressources. Le choix est fait de privilégier certains indicateurs considérés comme représentatifs. Comment sélectionner ces champs privilégiés, alors que les causes d'accidents sont issues de l'ensemble de l'organisation ?
- *Les indicateurs génériques :* sont conçus de manière peu contextualisée au domaine industriel cible. Comment transposer un indicateur d'un domaine à l'autre, alors qu'ils font preuve de modes de gestion clivés (nucléaire, chimie, et transport n'ont pas le même niveau de connaissance) ?
- *Le mythe de la mesure :* certains aspects intéressant dans la construction des accidents ne sont pas mesurable. Comment prendre en compte ces dimensions, et garder un recul nécessaire face à l'outil de gestion ?
- *Performance du système de mesure :* un problème circulaire. Comment mesurer la performance du système de mesure ?

Challenge relatif à l'utilisation des indicateurs :

- *Le pilotage par l'indicateur :* la focalisation sur le résultat entraine un changement des comportements. Comment s'assurer du management de la sécurité plutôt que du management de la mesure ?
- *Prise de décision :* la majorité des référentiels abordent la question du reporting, et des indicateurs comme support pour la communication. Pourtant, aucun n'aborde la place de l'indicateur dans le processus de prise de décision. Comment formaliser la place de l'indicateur dans le processus de prise de décision ?
- *Variabilité de la mesure :* l'évolution des normes, et le principe d'amélioration continue, pousse à modifier les référentiels et seuils de criticité des indicateurs. Comment faire évoluer les indicateurs, en permettant une comparaison à long terme des résultats ?

La prise en compte des signaux faibles

La littérature relative aux signaux faibles dans la gestion des risques industriels à connu des développement récents (Delatour et al., 2014b). Elle s'est articulée autour de deux objectifs principaux. Le premier objectif concerne la reconstruction des évènements passés, dans une analyse a postériori. Le signal faible souffre dans ce cas d'un biais rétrospectif important. Un élément peut être considéré comme important après l'occurrence de l'accident, c'est-à-dire une fois les circonstances particulières de la séquence accidentelle connues, bien que non significatif dans la gestion quotidienne du risque, avant l'accident. La recherche de plus en plus importante des signaux faibles correspond dans ce cas à un symptôme de la non-acceptation de l'accident par la société. On cherche alors à quel instant la maîtrise du système a été perdue, et qui est le responsable. L'accessibilité à la connaissance du résultat influence profondément la manière dont nous considérons les évènements passés. Le déterminisme (ou le « je le savais »), par lequel les observateurs d'évènements passés surestiment la capacité des autres à prévoir et anticiper. S'ils étaient impliqués dans ces évènements, ils ont tendance à surestimer ce qu'ils auraient pu eux-mêmes prévoir. La logique des évènements qui se sont déroulés apparait comme linéaire et régulière, selon une configuration reconnaissable à prétendue causalité interne, et donne l'impression qu'ils n'auraient pu se dérouler autrement. Ce biais peut jouer un rôle délétère dans l'attribution des responsabilités individuelles post-accidentelles. Avant de s'intéresser à la paille dans l'œil de son prochain, l'observateur rétrospectif devrait être conscient de la poutre (le biais de rétrospection) qui est dans le sien. Le caractère très particulier de chaque accident industriel ne permet pas aux concepteurs de se baser uniquement sur les leçons tirées des accidents passés. De plus, les dimensions des nouvelles installations ne permettent plus de réaliser des tests extensifs sur des sites pilotes pour démontrer la faisabilité d'un projet. La fiabilité et la sécurité de systèmes doit être évaluée par des méthodes analytiques, qui s'appuient sur des données empiriques issues d'incidents ou de presqu'accidents.

Le second objectif est tourné vers le futur, et cherche à identifier les évènements à venir, dans une approche d'anticipation. Dans le domaine de la gestion des risques industriels, la notion de « signaux précurseurs » à émergée de l'analyse de grands accidents technologiques Challenger, Columbia, Texas City… En 1978, Turner propose l'hypothèse des précurseurs. La plupart des accidents sont liés à des enchainements d'erreurs et de défauts, parfois complexes, mais presque toujours détectables au cours d'une période dite d'incubation (Turner et al., 1997). Vaughan (1996) reprend l'idée que des signaux précurseurs sont disponibles dans l'organisation mais que ceux-ci ne sont pas traités. Elle

appelle cette dynamique de l'organisation jusqu'à l'accident «normalisation de la déviance». Le mouvement des organisations hautement fiables a également mis en avant l'importance de la prise en compte des signaux faibles dans la sécurité des systèmes. Le maintien des opérateurs à un niveau élevé de vigilance, appelé «conscience situationnelle», permet de détecter les problèmes naissant et d'apporter des ajustements immédiats, ce qui évite potentiellement la génération de situations indésirables plus impactantes (Weick et al., 2008). La notion de signal faible s'est également développée dans d'autres domaines scientifiques, tels que le traitement du signal, la théorie de l'information, la stratégie d'entreprise (Lesca et al., 2002), et les « futures studies » (Hiltunen, 2008a). A travers ces courants de recherche, la littérature reconnait l'existence des signaux faibles, et leur disponibilité dans l'organisation Vaughan (1996). Au-delà de leur simple présence, ils sont les symptômes d'une période d'incubation de l'accident industriel (Turner et al., 1997). Si les théories de Vaughan et Turner permettent de décrire les biais d'organisations qui ont subi un accident industriel, elles n'apportent pas d'outils de gestion et d'anticipation. C'est également le cas pour le courant des organisations hautement fiables. Les auteurs décrivent la théorie de « sensemaking », et les conditions qui la favorisent, pour expliquer la prise en compte des signaux faibles. Cependant, ils n'apportent pas d'outils de mise en œuvre de cette théorie dans l'organisation.

Définition du signal faible

Selon Saltmarsch et al. (2012), les signaux faibles doivent être considérés au regard de deux dimensions : la causalité et la temporalité. La causalité indique si oui ou non un évènement qui précède un accident fait partie de la chaine causale accidentelle (la défaillance d'un composant par exemple), ou si l'évènement est simplement corrélé à l'accident (lorsqu'un animal fuit juste avant un tremblement de terre). La temporalité indique si un évènement est identifié comme signal faible a priori, ou comme signal précurseur dans une analyse à postériori (Saltmarsch et al., 2012). Le processus d'identification et de prise en compte des signaux faibles est mis en œuvre sur trois niveaux du système : l'individu, l'organisation, et l'industrie. Une gestion efficace des signaux précurseurs nécessite un investissement à chacun de ces niveaux. Hiltunen (2008b), ajoute propose trois dimensions du signal. La première dimension fait référence à l'*objet*. C'est l'élément référent, à un évènement futur. La seconde dimension décrit le *representamen*. C'est la forme concrète du signal (rumeur, image, évènement particulier). Enfin, la troisième dimension concerne l'*interpretant*. C'est le sens du signal et sa potentialité, c'est-à-dire sa capacité à faire imaginer à une personne

la situation future. A ces dimensions, Hiltunen définit plusieurs conditions nécessaires au signal faible : un vecteur support, une masse critique, ainsi que des acteurs dédiés (Hiltunen, 2008a). La notion de masse critique du signal faible a également été développée par Lesca et al. (2002). La faiblesse du signal vient de son potentiel informatif. Celui-ci doit dépasser un certain seuil d'intérêt pour être entendu (Mevel, 2004). Cette notion de seuil d'intérêt était déjà appréhendée par Bliss et al. (1998) dans le domaine de la sécurité. Cependant, le problème d'interprétation du signal, et de ses conséquences, est plus délicat dans le domaine de la sécurité. Lesca et al. (2002) identifie plusieurs caractéristiques qui définissent la faiblesse du signal : sa fragmentation (complète ou incomplète), sa visibilité (au milieu d'autres informations), sa signification (ambiguïté, évidence), sa familiarité (information déjà rencontrée), son utilité apparente, sa persistance (du sens dans le temps), sa pertinence (dans un contexte donné), et sa fiabilité.

Les signaux faibles remis en cause

La notion de signal est reconnue par la littérature, mais elle est également remise en cause. Hiltunen (2008a) critique le manque de consistance dans les définitions des signaux faibles. La seule caractéristique communément acceptée par les experts est le rôle du signal faible comme premier signe possible d'un changement futur. Il demeure une confusion sur les caractéristiques suivantes : la relation avec les phénomènes transitoires, la durée, la subjectivité, et la personne interprétant le signal. Selon Hiltunen (2008a), Pitkänen critique également le choix du concept de signal. Un signal nécessite un émetteur, et celui-ci manque (Pitkänen, 2006). Selon Rossel (2012), le concept de signal faible est une métaphore et reste à définir. Le processus par lequel un élément de contexte est transformé en information utile pour l'individu ou l'organisation n'est pas scientifiquement pris en charge (Rossel, 2012).

L'application de la notion de signal faible dans les organisations est également questionnée. Les organisations ont des raisons légitimes d'ignorer les signaux faibles, spécialement si les informations semblent vagues et infondées (Aven, 2011). L'interprétation des signaux peut également poser des difficultés. Un incident passé peut être interprété par l'entreprise comme le succès des mécanismes de sécurité, plutôt que comme le signal de l'existence d'un problème (Paté-Cornell, 2004). L'organisation se trouve face à une myopie qui ne lui permet plus de s'extraire de la situation problématique (Rossel, 2012). Le système de reporting joue aussi un rôle dans le management des signaux faibles. Celui-ci peut entrainer

un biais de reporting, qui ne permet plus au manager de faire la distinction entre une tendance précurseur reportée et une véritable tendance sous-jacente.

Amalberti propose trois raisons expliquant le manque de prise en compte des signaux faibles dans les organisations. Premièrement, l'interprétation du signal faible est rejetée sur une base rationnelle. Un incident sur un point jugé mineur par l'évaluation des risques renforcera cette analyse de risque. Deuxièmement, la posture adoptée par le lanceur d'alerte fait perdre en crédibilité le sens de l'alerte. Troisièmement, la prise en compte des signaux faibles nécessite des modèles d'analyses plus complexes (modèle de conjoncture, de percolation, qui associeraient dans un même contexte signaux et évènements mineurs) que les modèles classiques d'analyse des risques, et demandent du temps, des ressources, et une grande compétence de fond (Amalberti, 2013).

Des outils de gestion limités, mais complémentaires

Les outils de gestion sont des éléments de pilotage important pour le manager. Ils apportent des informations structurées, et contribuent à la construction de la représentation du manager. Leur dimension critique a été soulignée à plusieurs reprises dans la réalisation d'accidents industriels majeurs (Première partie), aussi bien à travers la prise en compte des résultats d'audits, de l'utilisation des indicateurs de gestion, ou encore de la place des signaux faibles. L'intérêt de la construction de la représentation du décideur a également été dans la deuxième partie de ce travail doctoral, lors de l'analyse des principaux modèles de production de sécurité. La plupart des modèles ont en effet mis en exergue l'importance du système d'information dans la gestion de la sécurité. Au regard de ces aspects, l'apport et les limites des outils de gestion doivent être précisés.

L'analyse comparative des trois outils de gestion sélectionnés – les audits, les indicateurs de gestion, et les signaux faibles – a permis de mettre en avant les limites de chaque outil, et les limites de l'approche par outil. Cette approche est doublement limitée pour le manager. La première limite concerne la capacité de l'outil à déclencher une décision. L'utilisation d'un type d'outil ne peut garantir la capture de la richesse de fonctionnement d'un système industriel. En conséquence, il peut se révéler d'une efficacité limitée dans la construction de la représentation du système, pour le manager, et notamment dans son rôle de décideur. La seconde limite concerne la légitimité de la décision. Une décision prise sur ce mode de gestion peut conduire à une remise en cause de sa fiabilité, et donc de son application.

En outre, notre analyse permet de tirer une seconde conclusion intéressante. Et c'est celle de la complémentarité entre chacun d'eux. Le tableau suivant (Tableau 11) propose une mise en perspective des trois outils, au regard de plusieurs critères : le niveau de formalisation, la capacité à donner du sens, le niveau de fiabilité, le niveau d'expertise nécessaire, le niveau de ressource nécessaire à leur utilisation, et enfin la dynamique propre à chaque outil.

	SIGNAUX FAIBLES	INDICATEURS DE GESTION	SYSTEME D'AUDIT
Niveau de formalisation	Faible, inexistant. (note, mail, discussions, évènements ponctuels…)	Moyen. Outils construits et personnalisé à l'activité. Ils donnent généralement l'état d'une variable du système.	Elevé. Rapports autoporteurs et construits. L'audit suit une grille d'analyse standardisée.
Capacité à donner du sens	**Faible.** **C'est le croisement de multiples informations qui crée le sens pour une personne donnée, dans un contexte donné.**	**Moyen.** **Décrit une seule variable du système.**	**Elevé.** **Plusieurs faits sont consolidés et mis en relief.**
Niveau de fiabilité	Faible. C'est un processus de construction du sens subjectif.	Moyen. Les indicateurs sont objectifs mais souffrent des limites de la mesure (capacité de détection, incertitudes…)	Elevé. Le standard est reconnu et approuvé par la communauté industrielle.
Niveau d'expertise nécessaire	**Elevé.** **Chacun doit « trouver » le sens des évènements.**	**Moyen.** **le manager doit posséder la culture technique nécessaire à la compréhension des variables et de leur état.**	**Faible,** **Le rapport d'audit est construit pour synthétiser des faits et argumenter des conclusions.**
Niveau de ressource nécessaire	Faible. Le recueil d'information est actif et passif, et ne met en œuvre que l'Homme, au quotidien.	Moyen. La construction des indicateurs nécessite un premier modèle, le reporting des valeurs et l'analyse des tendances nécessite du temps et des moyens.	Elevé. L'audit nécessite une connaissance du système de référence, et une capacité à confronté un système réel à cette référence. De plus, le processus d'audit peut nécessiter beaucoup de ressources (analyse du système, rédaction de la synthèse, analyse de la synthèse…)
Dynamique propre de l'outil	**Continue et aléatoire.** **Le sens émerge au fur et à mesure des évènements et des situations rencontrées.**	**Continue.** **Les mesures en continu permettent la construction de tendance à moyen et long termes.**	**Ponctuelle.** **Les audits sont réalisés ponctuellement, généralement annuellement.**

Tableau 11 : Comparaison des outils de gestion

Cette analyse met en lumière plusieurs éléments intéressants sur le champ d'efficacité de chacun des outils de suivi.

Les points forts des signaux faibles résident dans leur capacité à faire émerger des questionnements, au-delà de ceux soulevés par les outils formels d'analyses, comme l'analyse de risque, ou encore le retour d'expérience. Cet enrichissement est de plus réalisé de manière continue, au fur et à mesure des évènements et des situations rencontrées. Enfin, les signaux faibles ne demandent que peu de ressources. Cependant, l'utilisation des signaux faibles demande une grande expertise du système géré. Elle est nécessaire pour construire de nouveaux scénarios, sur la base d'informations incomplètes et disparates. D'autre part, la détection et l'analyse des signaux faibles est subjective, et dépend très fortement de la personne alertée. C'est un outil que ne possède donc aucune profondeur dans le temps de l'analyse. Par exemple, un changement de quart pourrait mettre fin à tout questionnement nouveau, parce que l'acteur quitte son poste. En conséquence, un outil de prise en compte des signaux faibles se révèlent un excellent outil d'anticipation de situations nouvelles et inattendues, et de mise en critique d'analyses plus formelles, nécessaire au bon déroulement des activités industrielles.

Les points forts des indicateurs de gestion reposent tout d'abord sur leur construction objective. Ils répondent à une méthodologie, et fournissent donc des résultats valides et acceptés de tous. Egalement, les indicateurs ont une capacité à formaliser des tendances précises à moyen et long terme sur l'évolution du comportement d'un élément du système. En outre, ces caractéristiques constituent également des limites de l'outil. En effet, un indicateur ne porte que sur un critère du système, et n'aborde donc aucun autre élément. Il ne permet d'identifier des causes associées à des phénomènes particuliers. Enfin, il nécessite d'être alimenté en continu par des données fiables et valides. L'indicateur de gestion constitue donc un outil formel de suivi en continue du système. Il est suffisamment objectif pour soutenir une argumentation. Il peut être très réactif lors des monitorings de valeurs physico-chimiques du processus techniques, mais peut être assez peu représentatif du comportement gestionnaire global d'un système.

Enfin, concernant le processus d'audit, l'analyse met en valeur des points forts portant sur plusieurs points. C'est un outil formel, qui permet de formaliser des phénomènes associés à leurs causes. Il répond une méthodologie. Il est donc fiable, et chaque nouvelle occurrence est comparable dans le temps avec les anciennes. Pour autant, c'est un processus lourd en temps et en ressource, qui demande une préparation et une grande disponibilité du système

audité. C'est donc un outil de remise en cause global. Il est ponctuel, et s'inscrit en long terme dans le fonctionnement du système.

De l'outil de gestion à l'aide à la gestion

Face aux limites individuelles de chaque outil de gestion, on peut conclure que fonder l'approche par outil, telle qu'elle est décrite ci-dessus, ne permet pas de répondre à la problématique de structuration de l'environnement décisionnel du manager opérationnel. En outre, l'analyse comparative réalisée entre trois des principaux outils de gestion utilisés pour le suivi du niveau de risque met en lumière tout l'intérêt d'un système d'information composé d'outils complémentaires. Face à des situations ambiguës, le manager doit avoir recourt à de multiples perspectives sur le système. Au-delà de l'outil de gestion, c'est une aide à la gestion qui doit être développée.

Enfin, cette aide à la gestion doit s'appuyer sur une approche systémique. En effet, ce type d'approche est intéressant parce qu'il permet de prendre en compte l'ensemble de facteurs qui influent sur un phénomène. C'est une perspective approche pertinente pour la prise en compte des multiples facteurs qui influent sur le manager opérationnel, et la prise de décision.

II. Développer l'écosystème décisionnel du manager

Face aux défis de la complexité, du temps, et de la décision, un nouveau regard décalé est nécessaire sur le manager et son environnement. Sur la base d'une approche systémique, cette seconde sous-partie propose une modélisation nouvelle à travers l'écosystème décisionnel du manager. Après avoir introduit le concept d'écosystème dans une première section, une deuxième section décrit le concept d'écosystème décisionnel. Enfin, une troisième section propose des pistes de réflexions sur la manière de développer l'écosystème décisionnel du manager opérationnel.

II.1 Le concept d'écosystème

Le terme écosystème fait référence à un concept qui fait l'objet de nombreuses utilisations dans différents champs scientifiques : psychologie, linguistique, informatique, réseau. Il a également servi de base métaphorique, ou théorique, à de nouveaux regards portés sur des objets déjà étudiés par ailleurs : écosystème de la croissance, écosystème des médias, écosystème d'innovation...

A l'origine, le concept d'écosystème a été forgé par Tansley (1935), dans le champ des sciences du vivant. L'écosystème est alors défini comme « unité écologique de base constitué du milieu et des organismes qui y vivent ». Il désigne un ensemble formé par l'association d'un biotope (environnement biologique, géologique...), et de la biocénose (communauté d'êtres vivants), qui interagissent pour assurer son équilibre. Un exemple peut être la forêt tropicale humide (Amazonie) et tous les êtres vivants qui y vivent (végétaux et animaux). Les éléments constituant un écosystème, développement un réseau d'échanges directs et indirects, d'énergie, et de matière, permettant le maintien et le développement de la vie (Spieth, 2013). Tansley met alors en avant les notions d'interdépendance, d'homéostasie, et d'évolution, comme trois caractéristiques de la stabilité d'un écosystème.

Moore (1993) théorise à nouveau le concept d'écosystème au monde des affaires. Il se place dans une démarche à la fois métaphorique et descriptive, pour décrire l'ensemble des acteurs qui se sont associés pour raisons d'affaires, et l'environnement dans lequel ils évoluent. Ces écosystèmes sont caractérisés par des relations de coopération et de

concurrence entre les membres qui les composent. L'idée sous-jacente de ces alliances entre des concurrents est d'éviter une menace plus grande, à savoir que d'autres écosystèmes d'affaires s'imposent (Calcei et al., 2009).

Un autre exemple du transfert du concept d'écosystème est celui de l'écologie industrielle. C'est une discipline définie par Robert Frosch (1995) comme « l'ensemble des pratiques destinées à réduire la pollution industrielle ». L'objectif de l'écologie industrielle est d'apporter des éléments de réponse à la très complexe équation du développement durable, et d'accompagner la transition de notre société industrielle contemporaine vers des modes de fonctionnement plus durables (Adoue, 2007). C'est une stratégie de développement qui s'appuie sur quatre principes du concept originel : le bouclage des flux, la diversification des acteurs, la proximité des ressources, et la logique de développement continu.

Ecosystème : définition et caractéristiques

Un écosystème peut être défini comme « unité écologique de base, caractérisée par sa structure et ses fonctions. Elle permet d'intégrer les relations entre différentes communautés biotiques, et les facteurs abiotiques » (Lévêque, 2001). La principale fonction d'un écosystème est d'assurer la pérennité. Les caractéristiques des écosystèmes sont décrites dans plusieurs ouvrages (Lévêque, 2001 ; Frontier et al., 2008).

Un écosystème est fondamentalement constitué de plusieurs entités :

- **Le milieu :** ou biotope. C'est le volume occupé par l'écosystème. Il est caractérisé par un ensemble de paramètres nécessaire à la présence d'une population d'acteurs, appelés facteurs écologiques (paramètres physico-chimique, réservoirs de matière, d'énergie...).
- **Les populations d'acteurs :** ce sont l'ensemble des acteurs qui composent l'écosystème. Elle est caractérisée par la diversité de types d'acteurs qui y résident, ainsi que leur nombre. Chaque acteur remplit une ou plusieurs fonctions.
- **Les flux :** ce sont des échanges réalisés entre plusieurs acteurs, et entre acteurs et milieu. Ils peuvent être de différentes natures : matière, énergie, et information.
- **L'environnement :** est composé d'entités écosystémiques collectives ou isolées, qui entourent l'écosystème. Il matérialise la limite de l'écosystème.

Selon la théorie des systèmes, les écosystèmes manifestent davantage de propriétés spécifiques (émergentes), que la simple addition ou superposition des propriétés de ses entités constitutives. De nombreux travaux ont cherché à décrire l'ensemble de ces propriétés. Elles peuvent être regroupées en trois familles : les propriétés liées à son organisation, ses interactions, et sa dynamique.

L'organisation de l'écosystème :

- **L'intégration :** un écosystème est composé de plusieurs niveaux d'organisation hiérarchisés. Chaque niveau fonctionnel supérieur est de complexité croissante (individu, population, communauté). Chaque niveau est caractérisé par ses propriétés, ses lois, et ses spécialistes.
- **L'auto-organisation :** Les écosystèmes sont auto-organisés dans la mesure où ce sont des systèmes ouverts sur le plan thermodynamique, et qui se maintiennent loin de l'équilibre thermodynamique. La régulation de l'écosystème est assurée par des boucles de contrôle. Ainsi, les résultats d'une action sont renvoyés à l'entrée du système sous forme d'informations. Une boucle peut être positive (amplification, effets cumulatifs), ou négative (stabilisation, ralentissement).
- **La diversité :** un écosystème est caractérisé par une diversité fonctionnelle et spécifique. La diversité fonctionnelle correspond à la présence de multiples entités aux fonctions particulières et différentes. Elle peut être quantifiée par la quantité d'informations contenue dans sa structure (Frontier, orange). A cette diversité fonctionnelle s'ajoute une diversité spécifique. Elle correspond au nombre de types d'acteurs présents. Un écosystème mature est généralement caractérisé par une grande diversité fonctionnelle et spécifique.

Les interactions au sein de l'écosystème :

- **L'ouverture :** il possède de nombreuses interactions, et échanges avec ses différents environnements.
- **Des liaisons fonctionnelles internes :** un écosystème possède des liaisons fonctionnelles entre ses entités internes (acteurs). Elles peuvent être caractérisées de plusieurs manières : directes ou indirectes, de différentes natures (matière, énergie, information), à sens unique (causalité classique), ou à double sens (action

réciproque, causalité circulaire), ou encore action d'un élément sur lui-même (autocontrôle, emballement), fortes ou faibles (caractérisé le degré de détermination d'une variable envers une autre, et le délai de réalisation), favorable ou défavorable, et multi-échelles.

La dynamique de l'écosystème :

- **Les contraintes** (facteurs écologiques) : le fonctionnement d'un écosystème est possible (et limité) par la présence de deux types de contraintes. Elles contrôlent l'organisation et la dynamique de l'écosystème. Les contraintes structurelles agissent sur les acteurs, et les contraintes fonctionnelles qui agissent sur les processus. Ces contraintes sont variables, et peuvent évoluer sous forme de gradient. C'est une variation continue d'un facteur écologique dans l'espace et dans le temps.
- **La recherche de la stabilité** : l'écosystème est susceptible de répondre à une perturbation et de revenir à son état initial de différente manière : homéostasie[8], résistance[9], réversibilité[10]. En l'absence d'agression, le résultat du développement n'est pas toujours une stabilisation de la composition et de la structure du système. La permanence de l'écosystème peut exiger des fluctuations importantes des acteurs, cycliques ou non, et des adaptations vis-à-vis des modifications périodiques ou chaotiques du milieu (climat par exemple). Un écosystème n'est jamais stable, son but est la pérennité.
- **L'hétérogénéité spatio-temporelle :** les écosystèmes sont adaptatifs, et ne sont intelligibles qu'inclus dans leur dimension historique et évolutive. Leur histoire est caractérisée par des évolutions déterministes, mais également par des basculements

[8] **L'homéostasie** (ou la résilience), traduit la capacité d'un écosystème à retrouver sa structure primitive après avoir été affecté par une perturbation. Cette résilience est fonction de plusieurs paramètres : l'intensité et de la fréquence des perturbations, du plus ou moins grand isolement du système, de la présence de substance toxique… On parle d'élasticité pour qualifier la vitesse de retour au stade original, et d'amplitude pour qualifier l'ampleur maximale de la perturbation qui permet encore un retour au stade original. On admet implicitement qu'au-delà du seuil de réversibilité, le système bascule vers un autre état.

[9] **La résistance**, (ou persistance, ou rémanence) : est la capacité d'un écosystème à rester constant ou à ne manifester qu'une réponse limitée aux variations de milieu. On peut également parler d'inertie pour qualifier la résistance aux perturbations.

[10] **La réversibilité/irréversibilité** : lorsqu'un écosystème ne peut revenir à son état antérieur, on dit qu'il a franchi un seuil de réversibilité. Ce concept est complémentaire à celui de la résilience, car il définit des limites à la capacité de réaction d'un écosystème.

soudains, non linéaires, qui rend l'histoire de chaque écosystème particulière et irréversible.

- **L'effet des perturbations[11] :** les perturbations rencontrées par l'écosystème modifient son fonctionnement. L'écosystème peut alors passer par plusieurs phases de vie : dégradé[12], juvénile[13], mature[14], vieilli[15]. En règle générale, des perturbations répétées (stress) ont tendance à rajeunir l'écosystème.
- **La variabilité temporelle de l'environnement :** elle s'exprime à diverses échelles d'espace et de temps : fluctuation qualitative, et quantitative de la nature de l'environnement.

Toutes ces caractéristiques systémiques décrivent le fonctionnement d'un écosystème. Parmi celles-ci, une seule propriété systémique est particulière à l'écosystème : sa dimension historique. Chaque écosystème est le résultat d'une évolution provoquée par une suite de perturbations et d'adaptations, et de ruptures. La connaissance de ces évènements permet de « raconter » l'histoire de l'écosystème. Cette caractéristique est importante à deux titres. Premièrement, elle permet de poser un principe de dissociation. Ainsi, deux systèmes initialement identiques peuvent avoir évolué différemment en fonction des perturbations rencontrées. Et deuxièmement, connaitre l'histoire de l'écosystème permet de mieux comprendre sa structure, et ses différentes fonctions.

[11] Une **perturbation** peut être définie comme un évènement qui induit une conséquence sur l'écosystème. Elles peuvent être caractérisées de différentes manières : le type (physique, biologique), le régime (fréquence, durée, intensité), et le contexte régional.

[12] **Ecosystème dégradé :** écosystème ayant subi de fortes perturbations, dépassant son seuil de réversibilité (surexploitation, incendie…).

[13] **Ecosystème juvénile :** peu d'acteur, robustes et à croissance et multiplication rapide, conditions agressives, système d'interaction simple, peu de régulation, flux de matière et d'énergie important, processus simple et linéaires. Variations de l'écosystème fortement contrôle par le milieu.

[14] **Ecosystème mature :** écosystème juvénile qui a subi une évolution de maturation : modification du milieu, complexification biologique (apparition d'espèces plus spécialisées, mais plus vulnérables, à croissance et multiplication moins rapide), accumulation d'informations internes reflétant l'acquisition d'une organisation optimale, création et entretien de structures de survie, augmentation de la diversité spécifique et du réseau d'interaction, spécialisation des besoins, apparition de relations d'antagonismes, et de mutualisme. Mise en place de recyclage de matière, stratégie d'économie, installation d'homéostasie. L'écosystème est régulé de l'intérieur.

[15] **Vieillissement de l'écosystème :** se produit lorsqu'un acteur favorisé échappe au contrôle exercé par l'auto-organisation, et accapare le milieu. Cela conduit à un effondrement de la diversité. Ce vieillissement perdure selon la persistance de l'écosystème, et s'arrête par la disparition de l'acteur considéré.

Si pour les managers, un « écosystème » est devenu un terme générique qui recouvre un ensemble hétérogène de pratiques (Fréry et al., 2012), le recours à ce concept est intéressant à plusieurs titres.

Tout d'abord, il convient de préciser qu'un écosystème n'a pas d'existence comme objet physique. C'est une manière de porter un regard sur une entité, ou un phénomène, avec une approche systémique. La construction d'un écosystème pour le manager prend alors ses distances avec la référence biologique, pour ne s'intéresser qu'aux propriétés écosystémiques. Or, notre analyse a par ailleurs montré l'importance de proposer une aide à la gestion pour le manager, bâti sur une réflexion systémique.

Egalement, le concept est intéressant au regard de sa dimension intégrative. Davantage que la définition de ses contours, c'est le lien entre acteur et système qui nous intéresse. Chaque acteur est interdépendant des autres, au sein d'un espace-temps commun, et constitue une communauté de destin. L'approche systémique n'est pas seulement la description structurelle et fonctionnelle du système, c'est surtout la reconnaissance mutuelle entre acteur et système.

Enfin, le concept d'écosystème est intéressant pour ses dimensions explicatives, et communicatives. En effet, les caractéristiques de liaison fonctionnelle, de diversité, de stabilité, de perturbation, et d'évolution, sont autant de leviers d'explicitation et de compréhension de systèmes évolutifs par nature complexe.

II.2 Le manager opérationnel au cœur d'un écosystème décisionnel

L'écosystème décisionnel répond à un besoin d'un double regard porté sur le manager opérationnel dans un système de production industriel, soumis à la continuité d'activité.

En effet, le management opérationnel est une fonction peu décrite dans les principaux modèles de production de sécurité. Cet état peut s'expliquer par le fait que cette fonction possède des prérogatives à géométrie variable en fonction des organisations. Il est donc difficile de mesurer une catégorie de manager suffisamment générique pour correspondre à la réalité des entreprises. De plus, la sécurité industrielle s'inscrit dans une réflexion volontairement globale sur le système. On s'intéresse par exemple à sa capacité à identifier et canaliser ses dérives, sa capacité à faire face aux perturbations, ou encore sa capacité à prendre en compte les signaux du terrain... Cette approche globale qui permet de prendre en

compte l'ensemble des propriétés émergentes. Cependant, elle laisse de côté la focalisation sur un aspect en particulier, et notamment les niveaux managériaux intermédiaires.

Pourtant, au sein d'un système caractérisé de sociotechnique et complexe, le manager opérationnel joue un rôle essentiel de veilleur et de lanceur d'alertes pour le maintien d'un haut niveau de sécurité à long terme. A son niveau sont conçues et coordonnées l'ensemble des règles de gestion relatives à la mise en œuvre du couple processus technique / opérateur. Il est également en charge de la résolution des problématiques concernant l'adéquation entre les objectifs de production, les ressources allouées, et les contraintes associées. Sa position intermédiaire lui permet d'agir directement sur le processus de production, tout en gardant une vision globale du système. Il revêt également une capacité décisionnelle de proximité, de terrain, ce qui fait de lui un des tenants du dilemme entre production et sécurité. Par la décision d'initiative, il préserve ainsi le principe de continuité d'activité.

Le manager est également un des garants de la continuité d'activités des installations industrielles. Derrière le dilemme de la décision, réside toute l'ambiguïté du management, dans le maintien de l'équilibre entre rupture demandée par l'obligation de sécurité, et absence de rupture demandée par l'imposition de continuité d'activités.

Or, une analyse historique des principales catastrophes industrielles passées nous a permis d'identifier les contraintes qui s'imposent au manager. Complexité, temps et décision, sont trois défis qui dégradent peu à peu son environnement décisionnel. Sans réaction, cette dérive lente peut le conduire dans une situation de rupture managériale, pour laquelle la représentation qu'il a du système et de son fonctionnement, ne correspond plus à la réalité du terrain. La prise de décision d'anticipation n'est donc plus possible. La rupture managériale est également une rupture subie. Elle est imposée par le contexte, et s'exprime selon des scénarios qui peuvent être inconnues. Elle contribue à entériner des écarts aux normes de sécurité, créant des situations accidentogènes.

Il s'agit alors pour le manager de passer de la décision contrainte, à la décision d'initiative. Pour cela, la thèse défendue est celle du développement de l'écosystème décisionnel du manager opérationnel. C'est un espace critique, de prise de recul par rapport au fonctionnement du système. Un espace qui permet au manager de s'interroger, et de déclencher si nécessaire une décision de prudence. Ce processus peut s'accorder avec le souci industriel du principe de continuité. En comprenant l'écosystème, le manager opérationnel peut prendre des initiatives qui protègent le principe de continuité par un arrêt

momentané préparé, et sans rupture. C'est là, le point fort du manager opérationnel : une rupture acceptée permettant une meilleure reprise. La décision d'initiative n'est plus contrainte mais pensée, acceptée, et déployée à travers l'écosystème décisionnel.

En outre, la rupture d'initiative est importante car elle permet de reprendre le contrôle. Elle entérine le doute, dans un système qui cherche la sécurisation. Elle repositionne l'Homme au cœur d'un système de plus en plus automatisé, et au sein duquel la temporalité de la décision de l'ordinateur surpasse celle de l'Homme.

Dans ce cadre, la rupture managériale n'apparait plus comme une ambiguïté, mais comme un atout, l'obligation de continuité d'activités.

Définition de l'écosystème décisionnel

Face au défi de la complexité, du temps, et de la décision, l'écosystème décisionnel permet d'avoir un regard nouveau sur le manager opérationnel. Il permet une vision globale du système, centralisé sur le manager.

C'est un cadre de compréhension du rôle de la responsabilité de l'acteur envers le système, et réciproquement du rôle et la responsabilité du système envers l'acteur. Il permet de dépasser le clivage de l'erreur humaine, de la défaillance technique ou de la cause organisationnelle. L'accident apparait comme un état pris par le système, et est le résultat d'une dynamique fonctionnelle globale. A titre d'exemple, le boulon qui casse n'est que le résultat de l'échec d'un processus de gestion de la maintenance, et de connaissance de l'état des installations. Chaque élément du système joue un rôle dans cette évolution, et indépendamment de sa nature (technique, humaine, ou organisationnelle).

L'écosystème décisionnel du manager peut être défini comme une vision intégrative de la fonction de manager, dans son rôle de décideur. Il permet au manager de mieux appréhender son environnement pour intégrer des informations, construire, et reconfigurer une représentation du système global, afin d'améliorer la prise de décision. L'écosystème décisionnel regroupe l'ensemble des éléments qui peuvent avoir une influence sur la prise de décision du manager.

L'écosystème décisionnel du manager opérationnel est constitué de plusieurs éléments :

- **Un environnement externe :** c'est la société dans laquelle est immergé l'écosystème décisionnel. Elle est caractérisée par des modes de fonctionnement : économique, législatif, commercial...
- **Des acteurs :** ce sont l'ensemble des personnes impliquées dans le fonctionnement de l'écosystème. Elles sont internes (opérateurs, managers...), et externes à l'écosystème (clients, fournisseurs, consultants, représentants institutionnels...)
- **Des flux :** ce sont des échanges réalisés entre plusieurs acteurs, qu'ils soient internes et externes. Ce sont par exemple des flux d'information (compte-rendu, mesures, échanges téléphoniques...), ou encore des flux de matière (composants, matières premières...), et des flux d'énergie (électricité...).
- **Une organisation formelle :** l'écosystème décisionnel s'appuie sur une structuration formelle de l'entreprise, bien définie en termes de fonction, de latitude décisionnelle, et responsabilité. Elle est composée de différents niveaux hiérarchiques intégrés. Au sein de systèmes de production, elle est généralement de forme pyramidale, et comprend de nombreux niveaux décisionnels. Elle peut également se décliner localement, et temporairement sous des formes plus hybrides (matrice...).

L'écosystème décisionnel du manager opérationnel est également caractérisé par plusieurs propriétés fonctionnelles. Celles-ci sont décrites selon la même typologie de caractéristiques utilisées pour décrire le concept d'écosystème : celles liées à son organisation, ses interactions, et sa dynamique.

Organisation de l'écosystème décisionnel :

- **Des environnements managériaux internes :** le manager opérationnel fait partie intégrante de trois types d'environnement : l'environnement opérationnel, l'environnement managérial intermédiaire, et l'environnement managérial stratégique. Ces environnements matérialisent l'organisation informelle du système, dans laquelle a lieu les ajustements, les court-circuits procédurales, et les discussions non prévues, dans le but de maximiser l'efficacité opérationnelle.

L'environnement opérationnel :

Le manager est la tête de cet environnement. Il définit les règles d'action, et gère une équipe opérationnelle. Il possède une forte latitude décisionnelle, une autorité sur les niveaux hiérarchiques inférieurs, et assume les responsabilités associées à la gestion de cet environnement. Le manager prend ses décisions sur la base d'informations qu'il recueille. Il réalise des arbitrages. Il est amené à gérer plusieurs types de connaissances. Les métiers et les cultures présents sont proches. Les modèles et les informations sont partagés. Les acteurs présentent un fort niveau de collaboration.

L'environnement managérial intermédiaire :

Dans cet environnement, le manager côtoie d'autres managers et experts, de spécialités différentes, et issues d'autres services de l'entreprise. Chaque acteur possède sa propre perspective sur le système. Chacun possède ses propres informations, et ses propres modèles d'analyse. De plus, le niveau de collaboration est variable suivant les services concernés. Les rapports sont ambivalents. Ils sont à la fois fondés sur l'obtention de l'intérêt général commun, et le respect des zones de responsabilité de chacun. Ils font également l'objet de jeux de pouvoir, et de friction sur des décisions locales.

L'environnement stratégique :

Dans cet environnement, le manager revêt une posture opérationnelle. Il défend ses décisions, et effectue des demandes en termes de ressources. Il peut rentrer en compétition avec d'autres fonctions du système. Il doit être convaincant. Il fait remonter des informations sur le fonctionnement du système, et reçoit des orientations et des directives pour la suite des opérations. Il reçoit des arbitrages sur des enjeux conflictuels.

- **Une diversité des acteurs :** l'écosystème décisionnel est caractérisé par une diversité d'acteurs. Chacun est chargé d'assurer une ou plusieurs fonctions dans le système. Il existe une diversité des métiers, et des compétences, nécessaire au fonctionnement du système. Ces fonctions sont généralement regroupées en trois groupes : la production, supports (achats, gestion des ressources humaines, hygiène et sécurité...), et la direction.

Interactions au sein de l'écosystème décisionnel :

- **Un écosystème ouvert sur son environnement :** le manager opérationnel est intégré à un réseau d'acteurs externes à l'écosystème. Ce réseau contribue à développer l'écosystème décisionnel en fournissant une perspective externe au manager, formalisé par des échanges d'informations. Dans ce réseau sont en contact d'autres managers au sein d'autres entités (managers HSE par exemple), des clients, des fournisseurs, des intervenants ponctuels (experts, consultants), des acteurs institutionnels (services déconcentrés de l'Etat, ministère...).
- **Des liaisons fonctionnelles internes :** l'écosystème décisionnel est caractérisé par l'existence de liaisons fonctionnelles internes permettant des boucles de contrôle des processus de gestion et de production. Ces liaisons fonctionnelles sont caractérisées par deux types de flux : prescriptifs et descriptifs. Les flux prescriptifs sont des orientations, des ordres d'actions, des consignes, qui s'imposent au destinataire (par exemple, une consigne de réalisation d'une vérification, ou à l'inverse, une avalisation d'écart à une procédure). Les flux descriptifs sont des informations échangées entre deux acteurs, ou encore entre l'acteur et le système. Ces flux peuvent être de différentes natures (état de choses acquis lors d'une discussion, indicateurs de gestion, informations recueillies par un système d'information spécifique...). Ces liaisons fonctionnelles peuvent également être caractérisées par des niveaux d'intensité variables (influence, demande, prescription hiérarchique formelle...)

La dynamique de l'écosystème décisionnel :

- **Des contraintes de fonctionnement :** outre les contraintes externes qui s'imposent au système de production (économique, réglementaire, commerciales...), le fonctionnement de l'écosystème décisionnel est contraint par le milieu technique, et organisationnel dans lequel il évolue. Son évolution est avant tout contrainte par les degrés de latitude imposée par l'organisation formelle du système (le niveau d'autorité, les règles de fonctionnement, les possibilités d'accès du manager dans le système, le niveau d'information qu'il possède...). Egalement, l'évolution de l'écosystème décisionnel du manager est contrainte par le niveau de coopération existant entre les acteurs du système (résistance, échange, facilitation...).
- **Une histoire :** l'écosystème décisionnel du manager est le fruit d'une évolution fondée sur des adaptations, et des ruptures (par exemple, l'existence d'arbitrages passés sur le conflit sécurité production, l'affichage ou non d'une politique de sécurité, des changements organisationnels, des accidents passés...). La connaissance de cette histoire permet d'en comprendre les modes de fonctionnement. A titre d'exemple, l'occurrence dans le passé d'un accident industriel permet de mieux comprendre une politique interne complètement tournée vers la sécurité).

Une représentation de l'écosystème décisionnel du manager opérationnel est proposée page suivante (Figure 36).

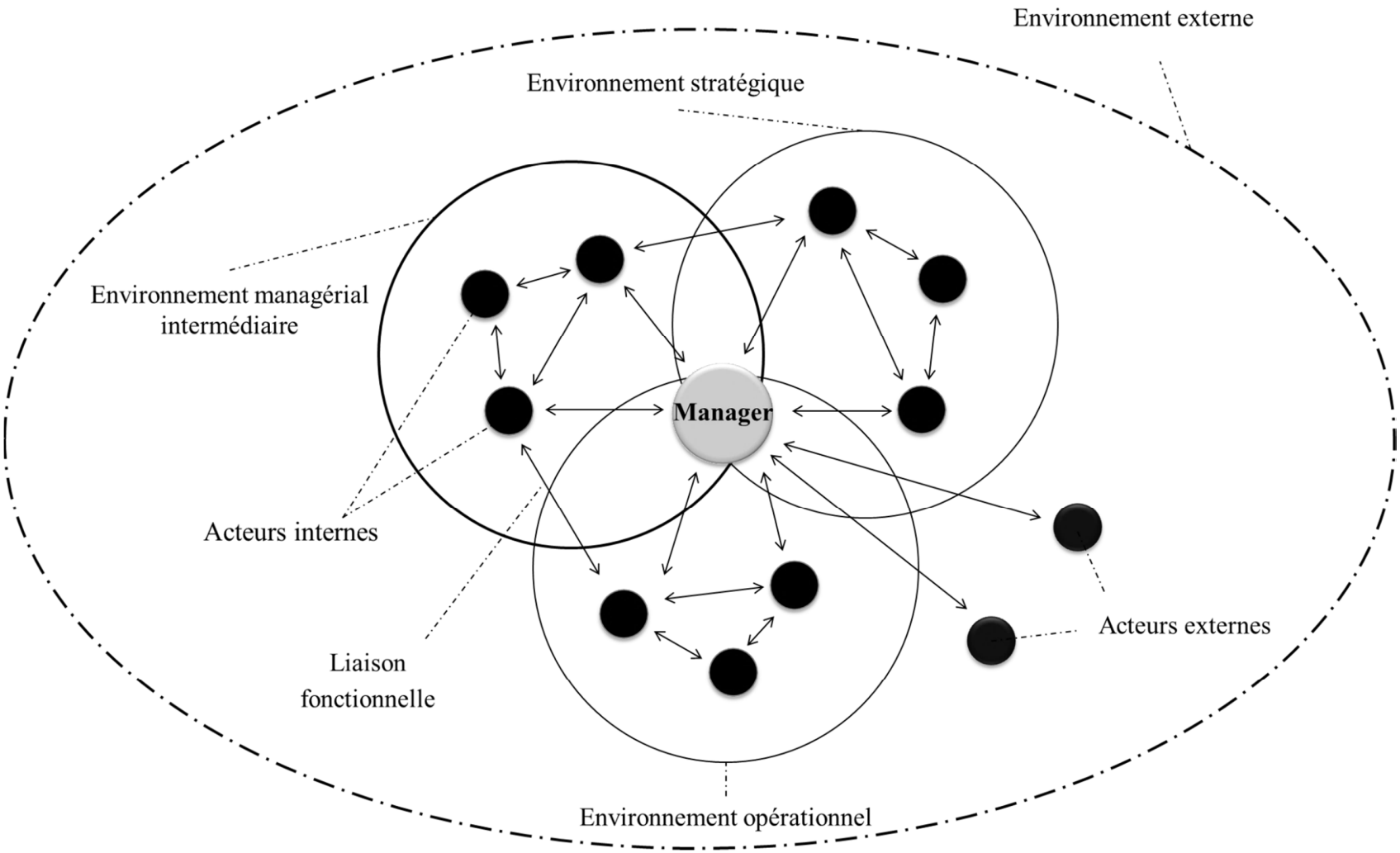


Figure 36 : L'écosystème décisionnel du manager

II.3 Dé complexifier la prise de décision

Au sein de systèmes industriels au fonctionnement structuré et fortement normé, la prise de décision d'initiative est difficile. Afin de garder une critique du système, le manager doit avoir une posture particulière. Il doit se repositionner, et acquérir de nouvelles perspectives. C'est une prise de recul nécessaire sur l'intensité du quotidien. C'est un espace critique qui lui permet d'affiner la compréhension qu'il a du système, et ainsi éviter la rupture managériale.

Comment développer cet espace critique ?

Mettre en place une réflexion systémique nous a permis d'identifier plusieurs aspects importants du fonctionnement des process de production à risque. Tout d'abord, elle apporte un regard décalé sur la manière d'en comprendre les rouages. Cela a permis de bénéficier d'une perspective à la fois globale sur le système, et centrée sur le manager. L'approche systémique a également permis de mettre à jour l'importance de la dynamique du système. Son histoire est jalonnée d'adaptations et de ruptures. Il a également un avenir, une orientation stratégique vers laquelle il souhaite se diriger. Ces deux perspectives influent sur son mode de fonctionnement du moment.

De cette analyse nous pouvons également identifier trois pistes de réflexion pour développer l'écosystème décisionnel. Elles constituent des leviers d'action complémentaires, à trois niveaux différents (Figure 37). Chaque piste de réflexion est décrite dans les pages suivantes.

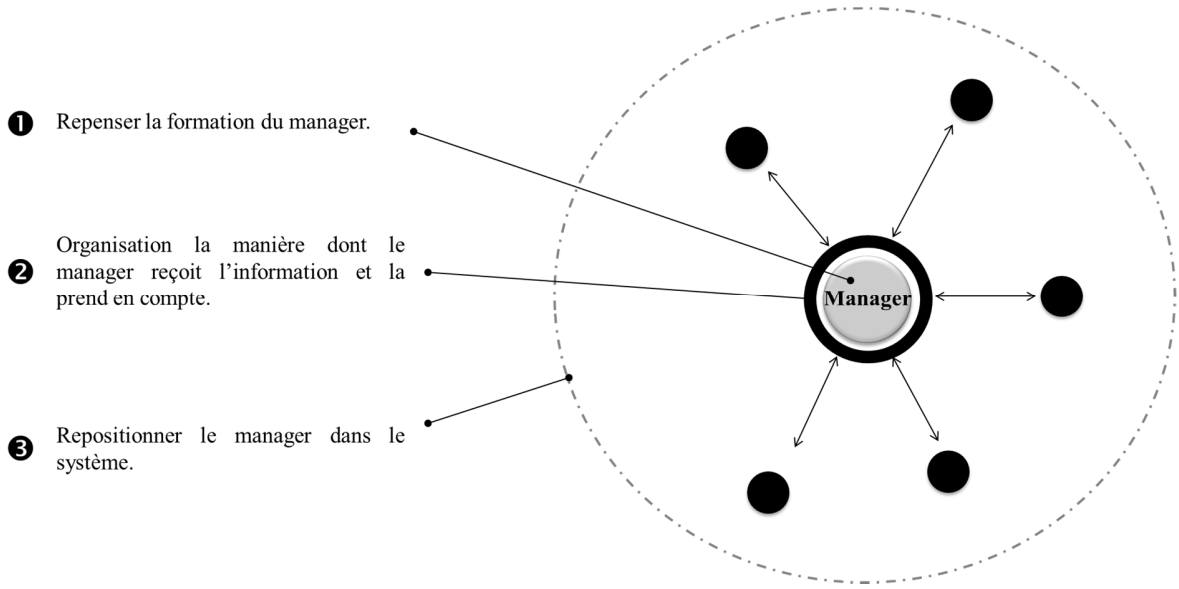


Figure 37 : Pistes de développement de l'écosystème décisionnel

Repenser la formation du manager

La première piste de réflexion porte sur l'élément central de l'écosystème décisionnel : le manager.

La première partie de ce travail a démontré toute la complexité qui s'impose au manager dans le cadre de ces activités de gestion. La dynamique du système est telle que le manager ne peut en appréhender l'ensemble modes de fonctionnement, et des scénarios possibles. La capacité à se représenter fidèlement et précisément l'état du système constitue alors un défi.

La dimension complexe des systèmes a également été soulevée dans la deuxième partie. Il s'agissait de se questionner sur la capacité des principaux modèles de sécurité à prendre en compte cette complexité, et apporter une réponse sur la manière de la gérer. Deux questions étaient restées sans réponse. La première question est celle de la définition d'une complexité située, du point de vue du manager opérationnel. Enfin, la seconde question est de la gestion de cette complexité.

Pour faire face à ce défi de la complexité, les managers sont principalement recrutés sur leur profil de compétences. En effet, la formation suivie est une garantie pour l'employeur de la

capacité à remplir sa fonction. Généralement, ce profil de formation est fondé sur trois familles de compétences acquises en formation initiale.

La première famille de compétences concerne la dimension scientifique et technique du métier. Il s'agit pour le manager d'acquérir des connaissances disciplinaires spécialisées. Dans ce cadre, le manager est formé à l'analyse de risque, aux sciences du danger, et à la sécurisation des systèmes industriels. Les connaissances acquises doivent alors permettre au manager de mettre en œuvre et de faire vivre un système de management de la sécurité relatif aux risques industriels.

La deuxième famille de compétences concerne la dimension managériale du métier. Il s'agit pour le manager d'acquérir les connaissances nécessaires à l'exercice de la fonction de cadre en entreprise. Pour cela, les enseignements sont généralement orientés vers le droit, l'économie, la conduite de projet, le management des Hommes, ou encore la gestion des profils et compétences.

Enfin, la troisième famille de compétence concerne la communication. Il s'agit pour le manager d'être capable d'appréhender les situations de travail qui s'imposent au rôle de cadre. Les enseignements portent principalement sur la communication écrite (rapport, synthèse...), la communication orale (présentation...), et les langues vivantes (anglais...).

Si ce profil est répandu, il a cependant des limites. :

- Elles se construisent autour des normes managériales (qualité, sécurité, environnement...). L'efficacité de cette approche réside dans sa capacité à appliquer une approche normative et générique dans le contexte particulier de l'entreprise.
- Elles abordent la notion de risque, sans aborder les process industriels. Même les formations en ingénierie ont des cursus poussés en mathématiques, mais ceux-ci servent majoritairement la sureté de fonctionnement.
- Elles ne mettent pas l'étudiant en situation de gestion. L'apprentissage est essentiellement théorique, ou porte sur une situation d'analyse de risque, ce qui ne constitue pas la majorité des activités de travail.

Face à ces limites, la nouvelle nature des systèmes de production a fait émerger de nouveaux besoins en termes de formation, et celle du manager doit être repensée. En effet, face au défi de la complexité, du temps, et de la décision, le manager doit s'armer de compétences diversifiées et complémentaires. Et son profil de formation doit évoluer, de deux manières.

Premièrement, les familles de compétences précédemment décrites doivent être renforcées par une « ingénierie des systèmes sociotechniques ». Il s'agit pour le manager de posséder les connaissances permettant la compréhension et le pilotage de ce type de système, complexe et évolutif. Celles-ci reposent sur plusieurs enseignements, tels que la gestion de la complexité, le management des connaissances, l'apprentissage organisationnel, ou encore la prise de décision dans l'incertitude.

La deuxième évolution du profil de formation d'un manager concerne les phases d'apprentissage. Qui aurait prédit la vulnérabilité liée à l'utilisation des smartphones dans les systèmes de production il y a seulement dix ans ? Certains managers expérimentés d'entreprise ont commencé leur carrière sans ordinateur. Ces exemples anodins démontrent à quel point le monde de l'entreprise, et la société, sont soumis à une accélération de son niveau de développement technologique. Face à cette dynamique, la remise en question régulière des modèles de compréhension et des outils de gestion est devenue aujourd'hui primordiale. Ainsi, le modèle classique fondé sur une formation initiale complète et unique doit être renforcé par un apprentissage en formation continue. Le manager aura alors la possibilité d'améliorer ses méthodes de travail, et de s'adapter aux nouvelles technologies.

Organiser la manière dont le manager reçoit l'information, l'assimile, et la transmet.

La deuxième piste d'amélioration de l'écosystème décisionnel porte sur la manière dont le manager reçoit l'information, l'assimile, et la transmet, par ses outils de gestion.

La première partie a mis en lumière cette question de l'utilisation des outils de gestion à travers l'étude des accidents passés. Par exemple, l'approche traditionnelle de construction d'indicateurs fondée sur la mesure a posteriori des incidents et accidents a été bousculée à la suite de l'explosion de la raffinerie de Texas City, en 2005. L'enquête a pointé une confusion entre les indicateurs relatifs à la protection des personnes et ceux relatifs au processus industriel, ainsi qu'entre les indicateurs réactifs (lagging indicators) et proactifs (leading indicators). De nombreuses réflexions et discussions ont émergé à propos de la bonne utilisation des indicateurs de performance pour mesurer le niveau de sécurité.

En outre, le début de cette troisième partie a montré toutes les limites d'une approche par outil générique. Audits, indicateurs, et gestion des signaux faibles ont été analysés. Et la littérature relative à la conception et à l'utilisation des outils de gestion est très riche. Elle embrasse aussi bien des aspects relatifs à l'ingénierie qu'à des aspects sociaux…. Ces outils sont utilisés pour aider le manager à comprendre le fonctionnement du système. Il s'agit de se représenter le plus

fidèlement possible son état actualisé. Notre analyse a également montré la complémentarité et les limites de plusieurs types d'outils de gestion. Chaque type possède ses forces et ses faiblesses. Il apporte une perspective particulière sur le système. Il répond en partie aux attentes du manager.

Face aux trois défis managériaux de la complexité, de l'érosion du temps, et de la décision, le manager opérationnel a plusieurs attentes en termes d'aide à la gestion :

- Des outils analytiques permettant l'intégration de dimensions multiples,
- L'actualisation régulière de sa représentation du système,
- Une définition du sens qu'il donne à son action,
- Une légitimation de ses conclusions sur la base de connaissances formelles,
- Une approche réflexive, intégrant la nécessité de réviser et d'adapter les outils utilisés.

Dans ce cadre, deux aspects semblent pertinents pour améliorer l'écosystème décisionnel du manager opérationnel par ses outils de gestion.

Le premier aspect concerne le recours équilibré à un triptyque d'outil (Figure 38). De nombreux challenges restent à relever concernant leur conception et la mise en œuvre. De plus, leur complémentarité apparait comme une propriété nouvelle intéressante. La littérature a beaucoup décrit chaque outil individuellement, mais peu de travaux se sont intéressés à leur utilisation croisée. Pourtant, il apparait que c'est dans le recours équilibré à chacun d'entre que le manager opérationnel peut chercher la représentation éclairée.

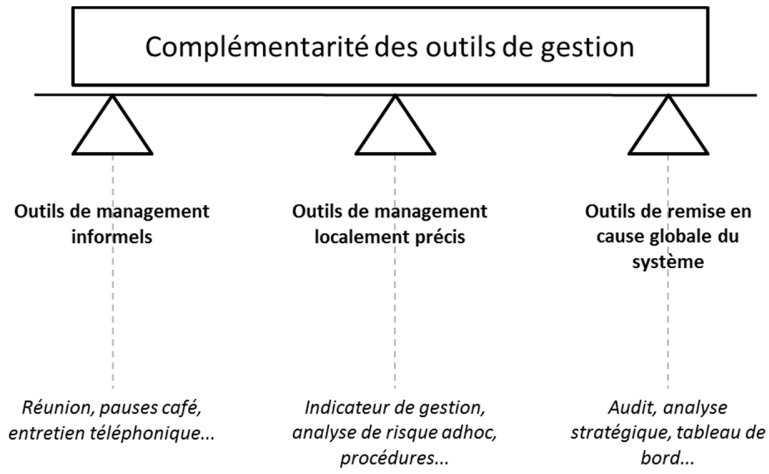


Figure 38 : Stratégie de complémentarité des outils de gestion

La caractéristique de complémentarité des outils de gestion peut être analysée en fonction de quatre critères : le nombre d'outil mis en jeu, la temporalité d'action, la nature des données utilisées, et enfin leur niveau de formalisation. Le nombre d'outils mis en jeu décrit le nombre d'outils de gestion utilisés pour alimenter la construction de la représentation du manager. Face à des situations ambiguës, le recours à un seul outil de gestion ne limite l'accès qu'à un seul type de données. La représentation du manager ne s'appuie donc que sur une seule perspective du système. Baser une analyse sur plusieurs outils en parallèle permet d'éviter ce biais. Le critère de temporalité d'action décrit la durée nécessaire à l'outil pour donner du sens aux données collectées. La détection des dérives de gestion, préliminaires à l'accident industriel, nécessite d'allier des outils de différentes temporalités. Les outils fondés sur le management informel permettent une analyse rapide, et peu de ressources, alors que les outils qui remettent en cause le système nécessitent davantage de ressources, et sont utilisés à des intervalles plus espacés. Un autre critère de complémentarité est le type de données utilisées par l'outil. Les situations rencontrées par le manager sont multidimensionnelles. Leur compréhension nécessite de recourir à des outils intégrant des dimensions variées : qualitatives, et quantitatives. Enfin, le dernier critère de complémentarité concerne le niveau de formalisation des outils. Ceux-ci doivent pouvoir appréhender l'ensemble des situations de travail, et des signaux qui les composent : depuis les discussions et évènements informels, jusqu'aux rapports d'analyse, autoporteur et construits.

Le second aspect concerne la manière dont le système d'information personnel du manager est construit, et évolue**.** La question de la construction des outils de gestion est un point central dans le développement de l'écosystème décisionnel. Sans reprendre les développements précédemment cités sur les limites des outils de gestion, et 10 ans jours pour jours après l'accident de Texas City, cette question est encore d'actualité. A l'heure actuelle, de nombreux outils existent, et sont disponibles pour aider le manager dans sa prise de décision. Dans la majorité des cas, celui-ci fait face à une étagère, et doit faire confiance à l'étiquette pour s'assurer de la bonne efficacité de l'outil, et de la bonne adéquation aux situations décisionnelles rencontrées.

Pourtant, la littérature converge vers l'importance de répondre à un certains nombres de questions lorsque l'on fait usage d'outils de gestion :

- Le choix de l'objet de la mesure : sécurité, risque, efficacité de processus... que cherche-t-on à mesurer ?
- Le type d'outil de mesure : audit, indicateurs... quelle est la méthode de mesure ?
- Le fonctionnement de la mesure : mode de déclenchement, périodicité... Comment mettre en œuvre cette mesure ?
- L'évolution des outils : péremption, obsolescence... Quand faire évoluer l'outil ?
- La variabilité de la mesure : comment permettre la mesure a long terme face aux besoins d'évolution ?
- La question de l'analyse des informations : destinataire, stockage, traitement, suppression, réaffectation... Comment analyser les résultats de la mesure ?
- La question de l'horizon décisionnel : entre création de sens temporalité, comment déclencher la prise de décision ?

Enfin, le troisième aspect concerne la diffusion de la décision dans son écosystème décisionnel. Prendre en compte toutes ces questions nécessite une démarche de construction structurée et méthodique. L'aide à la décision comme champ méthodologique représente alors un intérêt particulier. En effet, elle comporte deux propriétés intéressantes. Premièrement, il s'agit d'une démarche constructiviste. L'analyse est développée de manière réflexive entre le manager, tenant de la décision, et un analyste externe, garant de la méthode. Ainsi, le manager pourra s'appuyer sur un système d'aide à la gestion structurée, formel, et efficace. La seconde propriété intéressant

le manager est son architecture par étape d'analyse. Le résultat est le résultat d'une réflexion qui peut être partagée et opposée. Ainsi, la décision prise pourra être mise en balance dans un processus de négociation, ou de justification, sans souffrir de biais.

Repositionner le manager dans le système

La troisième piste de développement porte sur la place du manager dans le système. En effet, ce travail doctoral a montré toute la difficulté liée à la prise de décision de prudence, celle d'arrêter préventivement les activités de production.

Tout d'abord, l'étude des accidents industriels passés, décrite en première partie, ont mis en évidence l'existence de situations paradoxales pour le manager. A titre d'exemple, les rapports du naufrage de la plateforme Deepwater Horizon indiquent que les équipes opérationnelles travaillant sur la plateforme Deepwater Horizon ont été soumis à des pressions de production quotidiennes. Chaque opérateur avait conscience des surcoûts engendrés par des suspensions ou des retards dans le travail de forage. Cette pression a conduit les opérateurs à réaliser des compromis sur les mesures de prévention, et notamment à faire l'économie de barrières qu'ils ne jugeaient pas nécessaires. Ainsi, la responsabilité de la chasse aux coûts était descendue au plus bas niveau opérationnel. Cette dynamique a eu pour conséquences une réduction des investissements dans les moyens de maîtrise des risques, et la suppression de barrières de prévention jugées inutiles, mais nécessaires pour garder le contrôle du processus de forage.

Si l'argument des pressions de production est régulièrement avancé, son impact sur le manager opérationnel doit être précisé. La première situation paradoxale est le report des enjeux au plus bas niveau opérationnel. Le manager responsable de la production était également en charge des questions de sécurité. Ainsi, le manager se trouve dans une situation décisionnelle dans laquelle sécurité et production s'opposent, et où la sécurité est considérée comme un frein à la personne. Cette situation était structurellement imposée le système au manager, et déclinée au niveau individuel par plusieurs modes de fonctionnement :

- La présence d'incitations à terminer les opérations de forage le plus rapidement possible et en réduisant les coûts. Le projet comptait déjà 50 jours de retard et 100 millions de dollars de dépassement de budget.
- La décision imprévue de transformer le puit exploratoire en puit de forage, afin de réduire la durée et les coûts nécessaires à la réalisation ultérieure de cette étape, et permettre un retour sur investissement plus rapide.

- La focalisation du management sur la compétitivité et l'amélioration des performances des équipes de forage.
- La prise en compte dans les évaluations du personnel de leur capacité à respecter les budgets et réduire les coûts de production (en 2009, ce fut le cas pour 12 personnes sur 13 impliquées dans les opérations à Macondo).

La seconde situation paradoxale concerne la posture individuelle adoptée par le manager face à ces contraintes fonctionnelles. Bien que la responsabilité des conséquences repose sur le chef d'entreprise, le manager fait face à une dissonance entre la latitude décisionnelle, telle qu'elle est définie dans l'organisation formelle, et sa responsabilité de mise en œuvre. Le manager fait alors face à un questionnement éthique. C'est pour lui la formalisation d'un dilemme entre deux perspectives décisionnelles :

1. **La certitude imposée :** ce sont les décisions que le système lui impose de prendre, majoritairement orientée vers la production. Celles-ci peuvent également être masquées par un double discours 100% sécurité.
2. **Le doute individuel :** ce sont les décisions portées par un questionnement individuel sur le sens de la prise de risque qu'il impose, en tant que manager, à ses subalternes.

Ce choix place le manager en situation d'incertitude, voire de malaise. Sur la plateforme Deepwater horizon, il a été perceptible à de nombreuses reprises. Plusieurs documents et témoignages du personnel de la plateforme, pendant les semaines précédant l'accident, indiquent des inquiétudes relatives au changement d'organisation, et notamment dans les rôles et responsabilités des managers. Egalement, en mars 2010, la seconde perte de contrôle du puit a généré des tensions entre plusieurs managers, formalisées par des emails.

Externaliser le manager de risques ?

La question des arbitrages existant entre sécurité et production est largement prise en charge par les principaux modèles de production de sécurité. La deuxième partie de ce travail en a fait l'analyse. Elle est généralement formalisée par la notion de conflit en production et sécurité. Cependant, l'analyse reste focalisée sur la capacité du système à gérer ces conflits, sans décliner cette problématique au niveau du manager opérationnel.

Déclencher la prise de décision de prudence nécessite de garder toute la critique de l'action collective. Cependant, son niveau d'intégration et de contrôle du manager façonnent sa latitude décisionnelle. Ces éléments poussent à poser la question de la place du manager de risque dans

l'organisation. Quels sont ses prérogatives et latitudes d'action (niveau d'indépendance, positionnement hiérarchique et géographique...) ? Permettent-elles la prise de décision d'initiative ?

Ce travail doctoral n'a pu apporter de réponse à ces questions. Pour autant, il met en avant l'intérêt du positionnement dans l'organisation, et du cadrage éthique de l'action du manager, dont les conséquences peuvent être catastrophiques.

Conclusion de la Troisième Partie

Au sein de systèmes complexes et évolutifs, la sécurité est un processus dynamique. En son cœur, le manager opérationnel est un maillon critique. Dans la gestion du quotidien, il a la charge du bon déroulement des activités. Il est également un niveau décisionnel de premier plan de l'anticipation des accidents. Or, dans l'étape difficile de la décision, le manager est confronté à trois défis. Défis de la complexité, de l'érosion du temps, et de la décision s'imposent, et si le manager n'y prend pas garde, l'expose à la rupture managériale. Après avoir identifié les facteurs de cette rupture, la problématique abordée était la suivante. Quel type d'aide à la décision apporter au manager, au sein de systèmes socio-techniques complexes ?

Afin de répondre à cette question, deux parmi les principales approches de supports décisionnels ont été étudiées. Notre analyse s'est d'abord tournée vers l'aide à la décision, proposée dans une approche constructiviste. Bien qu'intéressante, cette méthodologie semble difficilement s'adapter à une prise de décision continue, immergée dans un flux de situations quotidiennes. La seconde approche visée est celle des outils de gestion. Plusieurs outils ont été regardés : système d'audit, indicateurs de gestion, prise en compte des signaux faibles. Notre analyse a montré toute la limite d'une approche par l'outil. Elle a également montré tout l'intérêt d'un système d'information personnel du manager construit sur la complémentarité des outils.

La situation spécifique du manager opérationnel, à l'interface entre contraintes opérationnelles et considérations stratégiques, nécessite de passer de l'aide à la décision, à l'aide à la gestion. Pour développer cette approche, une nouvelle perspective a été choisie. L'utilisation d'un raisonnement systémique a fait émerger un regard décalé et recentré sur le manager. Celui-ci est immergé dans un écosystème de vie et de décision, appelé écosystème décisionnel. C'est en développant cet écosystème que la capacité du manager à anticiper les situations accidentelles. Et plusieurs pistes ont été proposées : repenser la formation du manager, organiser la manière dont le manager reçoit l'information et la prend en compte, et repositionner le manager dans le système.

L'apport de cette troisième partie est donc la formalisation des facteurs de rupture managériale, la construction de l'écosystème décisionnel du manager opérationnel, et la proposition de pistes de réflexion pour le développement de cet écosystème.

Si ce travail est une contribution nouvelle à la prise de décision managériale, il a également des limites. En effet, chacune des pistes d'amélioration reste à l'état de réflexion. Chacune d'elle est

descriptive, et n'est pas opérationnelle. Ainsi, il serait intéressant dans un travail futur de reprendre ces trois axes, et d'approfondir une méthodologie de mise en œuvre de cette approche de l'écosystème décisionnel. Ce faible niveau d'application va de pair avec la seconde critique ce travail : le faible appui empirique. Egalement, il serait pertinent de tester les concepts de rupture managériale, et d'écosystème décisionnel, sur des situations réelles en entreprise.

Enfin, derrière la question de la prise de décision, nous avons effleuré la question de l'éthique managériale. Elle semble être une approche intéressante de la décision, qui permettrait de dépasser largement les questions de pression de production, et de dilemme production versus sécurité. Au sein de systèmes complexes, permettre au manager de garder la critique du système, apparait comme l'un des facteurs important de l'anticipation des accidents.

Résumé de la Troisième Partie

Après avoir identifié les limites des principaux modèles de production de sécurité, l'objectif de cette troisième partie est de se questionner sur la nature de l'aide à apporter au manager.

En effet, complexité, temps, et décision s'imposent, et si le manager n'y prend pas garde, l'expose à la rupture managériale, la perte d'initiative. Cette situation peut être définie comme la perte de maitrise du pilotage des activités. Le manager n'a plus la critique du système, et perd sa capacité d'anticipation. Après avoir identifié les facteurs de cette rupture, nous devons nous questionner sur l'écosystème du manager et sa capacité d'initiative au sein de systèmes sociotechniques complexes. Peut-il encore décider ?

Afin de répondre à cette question, deux parmi les principales approches de supports décisionnels ont été étudiées. L'aide à la décision tout d'abord, dans son approche constructiviste, constitue une voie intéressante. En effet, c'est une méthodologie qui contribue à structurer et faciliter la prise de décision, en apportant du contenu méthodologique externe, et en favorisant une posture de remise en question du décideur. Cependant, cette méthodologie repose sur des hypothèses qui ne correspondent pas au contexte décisionnel rencontré par le manager opérationnel. Bien qu'intéressante, cette méthodologie semble difficilement s'adapter à une prise de décision continue, immergée dans un flux de situations quotidiennes.

La seconde approche analysée est celle de l'utilisation des outils de gestion. Trois outils ont été analysés : système d'audit, indicateurs de gestion, et prise en compte des signaux faibles. Ceux-ci révèlent une plus grande efficacité dans un contexte de gestion quotidienne des activités. Cependant, notre analyse a montré la limite de l'utilisation individuelle de chaque outil, et notamment les challenges relatifs à leur conception et utilisation. Elle a également montré tout l'intérêt d'un système d'information personnel du manager construit sur la complémentarité des outils.

En conséquence, la situation spécifique du manager opérationnel, à l'interface entre contraintes opérationnelles, et considérations stratégiques, nécessite de passer de l'aide à la décision, à l'aide à la gestion. Pour développer cette approche, une nouvelle perspective a été choisie. L'utilisation d'un raisonnement systémique a fait émerger un regard décalé, et recentré sur le manager. Ainsi, une définition de l'écosystème décisionnel du manager opérationnel est proposée. L'écosystème décisionnel du manager peut être défini comme une vision intégrative de la fonction de manager, dans son rôle de décideur. Il permet au manager de mieux appréhender son environnement pour

intégrer des informations, construire, et reconfigurer une représentation du système global, afin d'améliorer la prise de décision.

Immergé dans la complexité, permettre au manager de garder la critique du système, apparait comme l'un des facteurs important de l'anticipation des accidents. Plusieurs pistes de réflexions complémentaires ont donc également été proposées pour développer l'espace critique du manager : repenser la formation du manager, organiser la manière dont le manager reçoit l'information et la prend en compte, et repositionner le manager dans le système.

Ainsi, c'est dans le développement de l'écosystème décisionnel du manager que se trouvent les leviers de progrès en matière de gestion des risques industriels.

Conclusion générale

Sans avoir la prétention de reprendre des formules Darwinistes ou essayer de démontrer la recherche de la perfection, l'évolution humaine va de pair avec la transformation de son environnement. Sommes-nous des prédateurs ou des constructeurs, ce n'est pas un débat que nous souhaitons ou pouvons ouvrir dans nos travaux. Or, il y a une certitude, nous nous caractérisons par un besoin d'avenir soumis au passé. Dans ce cadrage, entre deux temps, comment vivons-nous le temps présent ? Démontrer que toute situation a un avant et un après aurait permis de se servir de la mémoire humaine et de l'inscrire dans ce mouvement qui est permanent depuis le début de l'humanité. Et c'est bien de cela qu'il s'agit ! Comment doit-on ou peut-on acquérir le temps ? Et c'est sans doute cela qu'intuitivement nous avons voulu comprendre. Il est furtif, fuyant, fait de ruptures surprenantes et quelques fois brutales. Difficile à maîtriser, il est d'autant plus difficile à capitaliser. Pourtant, ses ruptures traumatisent la mémoire humaine. Une situation qui nous expose à la terreur et qui nous impose une prise de conscience. Capitalisation humaine unique et primordiale, c'est à partir de ce constat que notre société évolue en prenant des risques, en capitalisant les dangers et en mémorisant les crises. Dans ce processus, l'action et la réflexion sont intimement liées et si les avancées pour le progrès sont constantes. La recherche d'un équilibre entre avenir et mémoire du passé est constante. Au cours de ce processus, il arrive que la stabilisation soit remise en cause, et des équilibres entre le risque et sa gestion, fracture le temps par la crise. Et cette course au progrès est portée par l'Homme, mais aussi soutenue par les nouvelles technologies, et la maitrise constante des risques générés par ces mêmes activités. Or, pour en revenir au sujet qui nous préoccupe, si le monde s'accélère, que la fluidité et la complexité rythment les échanges, que l'Homme n'a jamais autant communiqué qu'aujourd'hui, la conséquence est cette énergie de mouvement est basée sur la vitesse, qu'elle représente une source d'évolution sans pareille, elle est basée sur un turnover permanent difficile à arrêter (Laclémence, 2012). Ce processus est d'autant plus marqué que l'industrialisation, la miniaturisation, les systèmes complexes et les réseaux de communications... ont intensifié le rythme et la permanence. Dans ce processus permanent, l'accident industriel majeur compte parmi les ruptures les plus destructrices et insupportables. Dans de nombreux cas, la catastrophe aurait probablement pu être évitée. Dans le flux continu du quotidien, les signes perceptibles de la dégradation des barrières de sécurité auraient dû alerter.

La question posée dans ce travail doctoral était alors celle de l'anticipation. Au sein de systèmes sociotechniques à hauts risques, et caractérisés par leur dynamique et leur complexité, quelles sont les voies à suivre pour devancer le déclenchement d'une séquence accidentelle ?

Pour répondre, notre approche s'est focalisée sur la prise de décision du manager opérationnel. En effet, les systèmes industriels à risques sont conçus sur un modèle de défense en profondeur,

dans lequel s'intègre la planification, la normalisation, la gestion, la prévention, la sûreté de fonctionnement, et les plans de secours et de continuité. Dans cet environnement contraignant, le manager opérationnel constitue un acteur particulier. Dans son environnement informationnel, ses outils de contrôle et ses possibilités d'action font de lui un décideur de premier plan pour l'anticipation.

De plus, son rôle est significatif et soulevé dans la plupart des rapports d'accidents. Les retours d'expérience réalisés sur des accidents majeurs montrent un décalage entre la vision qu'a le manager du système, et la réalité des opérations. On cherche à comprendre son environnement décisionnel, les informations connues, la manière dont il gérait les rapports humains, ses processus de prise de décision, ses seuils d'alertes... On cherche à comprendre pourquoi le système n'a pas été arrêté à temps, alors même que l'enquête post-accidentelle révèle des signes importants de dégradation de la sécurité.

Une analyse historique de plusieurs grands accidents industriels nous a permis de mettre en exergue les défis qui s'imposent au manager. Complexité, temps, et décision dégradent peu à peu son environnement, et masquent la compréhension globale qui aurait permis une prise de décision. Le manager est alors placé dans une situation délicate de rupture managériale subie entre son bassin fonctionnel, opérationnel et décisionnel. Celui-ci n'a plus la bonne vision des systèmes de protection qui assurent et rassurent les dirigeants sur la continuité d'activité. Cette situation trompeuse mérite d'être relevée pour assumer cette rupture entre perception et réalités. C'est bien là un facteur à risque maximum, celui de la conscience du décalage entre un bassin de décision qui se dégrade et qui remet en cause la sécurisation des systèmes.

Le manager se trouve alors dans une situation délicate pour maintenir la sécurité. Après la prise de conscience du risque, il est soumis à une forte tension entre la continuité d'activités et l'initiative de la rupture du système. Ce paradoxe s'est d'ailleurs manifesté dans de nombreux accidents, sous la forme d'incitation à réduire les temps de non production, de rémunérations individuelles corrélées à la productivité, ou encore de rapport de forces avérés entre manager de production, et manager des risques

Il s'agit alors pour le manager de garder un sens critique du système, et avec l'initiative de reprendre le contrôle des évènements. Pour cela, la thèse défendue ici est celle d'un manager disposant d'une vision large de son écosystème décisionnel, permettant une sensibilité aux risques dans le bassin de vie des systèmes. Comprendre la manière dont l'environnement influe sur sa prise de décision permet de passer d'une situation soumise à la rupture, à une situation où la décision d'initiative permet d'anticiper les conséquences. En comprenant son écosystème, le

manager opérationnel peut prendre des initiatives qui lui permettront de conserver le contrôle sur les mesures à prendre pour revenir à la continuité d'activités par un arrêt momentané et préparé, évitant la surprise. L'anticipation devient alors possible par le choix d'une rupture managériale choisie, préparée, acceptée, et déployée à travers l'écosystème décisionnel.

Dans ce cadre, la rupture managériale n'est plus celle de l'accident industriel, mais est une rupture d'initiative anticipée, qui vient renforcer le principe de continuité d'activités du système.

Mais au sein de systèmes industriels au fonctionnement structuré et fortement normé, la prise de décision d'initiative est difficile, et est bloquée par deux verrous. Le premier est celui de la compréhension du système. Il s'agit pour le manager de se construire une représentation actualisée de l'état réel de sécurité, qui prend en compte la complexité et la dynamique du système. Le deuxième verrou est celui de l'acceptation de la décision. Le doute porté par le manager doit être compris par les acteurs du système. Pour répondre à ce besoin, le manager doit être aidé. Ce support décisionnel dépasse le cadre de l'aide à la décision classique, pour s'orienter vers une aide à la gestion, intégrant le fonctionnement du quotidien.

Dans le but de développer l'espace critique et de disposer d'une vision réelle de son environnement décisionnel, trois principes sont proposés au manager. Premièrement, il s'agit de repenser la formation du manager pour lever les verrous de la décision inhérents à l'enfermement des processus décisionnels. Le deuxième principe porte sur la manière dont le manager reçoit l'information et l'assimile : la complémentarité de ses outils de gestion. Enfin, le troisième principe propose le repositionnement du manager dans le système, à travers ses latitudes d'action. Cette réflexion soulève l'intérêt du positionnement dans l'organisation, et du cadrage éthique de l'action du manager (Richard et al, 2013).

En proposant un écosystème décisionnel, nous avons levé certains verrous qui nous permettent de soumettre un processus décisionnel accompagnant le décideur. Tout d'abord, l'étude de cas appliquée aux accidents industriels majeurs peut être améliorée. En effet, si la méthodologie est structurée, il apparait que l'analyse de retours d'expérience et de rapports d'enquête peut être complétée. Les données secondaires sont parfois limitées, et les modèles d'analyses ne permettent pas d'expliciter les phases décisionnelles des scénarios. Le recours au retour d'expérience constitue donc une phase méthodologique nécessaire et pertinente, mais doit être renforcée par la suite par d'autres approches, davantage centrées sur le manager opérationnel et son environnement. A titre d'exemple, la conduite d'entretien, et l'observation directe, sur des managers opérationnels en situation de gestion quotidienne, constituent des voies méthodologiques complémentaires intéressantes.

Egalement, une deuxième perspective de recherche émane de l'analyse de la littérature relative aux principaux modèles de production de sécurité. En effet, parmi les nombreuses théories, nous en avons retenu cinq, les plus représentatives, afin de bénéficier d'éléments de comparaison. Si ce choix s'est affirmé nécessaire au regard du sujet et de son développement, il n'était pas possible de centrer tous les travaux sur ces éléments de comparaison. Dans le cadre de travaux futurs, il serait sans doute intéressant de poursuivre et développer l'étude des théories abordées, comme par exemple l'étude de la littérature relative à l'aide à la décision, afin d'améliorer la caractérisation de la situation décisionnelle rencontrée par le manager.

Enfin, la troisième perspective concerne la validation du modèle d'écosystème décisionnel proposé. La réflexion apportée propose un concept et des principes, qui, à ce jour, sont novateurs, et pourront faire l'objet d'une analyse critique permettant de rester fidèle à notre démarche fondée sur la remise en cause permanente des situations établies et la mise en application de propositions. En effet, une réflexion plus approfondie et spécifique sur chacun des trois principes proposés (réflexion sur la formation du manager, de ses outils de gestion, et son positionnement dans l'organisation) offre l'opportunité de dépasser le stade de la proposition pour l'action. Cette démarche est la suite logique et nécessaire de ce travail qui reste soumis à la mise en application. C'est la raison pour laquelle ce travail doctoral sera prolongé par une proposition de recherche/action déposée en gestion de crise afin de conserver le continuum réflexion/proposition/application. En outre, sur la base des travaux et propositions, chacune de ces dimensions ouvre de nouvelles pistes à un espace critique permettant de lever de nouveaux verrous scientifiques.

Le contexte du XXIème siècle sera celui d'une troisième révolution industrielle, fondée sur l'accélération des moyens de communication, les développements technologiques, et la complexification et interdépendance des systèmes. La représentation et définition du risque industriel vont évoluer, ainsi que les attentes et orientations du principe de continuité d'activités. Les points critiques ne seront plus les infrastructures lourdes, mais se concentreront dans des nœuds d'échange d'informations, de matières et de personnes. Le danger va également muter, pour dépasser le cadre de la matière. Biotechnologie, nanotechnologie, et systèmes d'informations constituent déjà un potentiel de développement pour lesquels les risques sont encore peu connus. Egalement, les bouleversements géopolitiques ont déjà déplacé le curseur de maitrise des technologies, en intégrant avec la sureté et la sécurité, la malveillance. A titre d'exemples, énergies et transports sont repositionnées comme des cibles potentielles d'actes de malveillance, et constituent de nouveaux défis de maitrise des risques sociétaux. Enfin, la mondialisation des échanges, et l'ouverture des marchés transcontinentaux à venir, intensifieront

encore les échanges et la compétitivité entre les entreprises. Dans ce cadre, le rapport entre coût de la sécurité et rentabilité se posera et la question du choix de la défense en profondeur, comme doctrine de sécurisation privilégiée, ouvrira la voie à de nouvelles orientations et choix.

La prochaine étape de l'évolution est-elle de sortir l'Homme du système industriel ?

Automatisation, robotisation, informatisation, et intelligence artificielle sont les leviers de la production de demain. Ils permettent une exécution des tâches plus rapide, plus efficace, et plus fiable. Ainsi, les progrès technologiques repositionnent petit à petit l'Homme hors du système. Il devient un client final, et porte la responsabilité des conséquences de machines qu'il ne peut plus appréhender. C'est déjà le cas avec l'informatique décisionnelle. L'ordinateur recueille les données, analyse, et propose des schémas d'action, que l'Homme n'a plus qu'à entériner.

Le monde de demain sera plus complexe, plus rapide. La planification aura de nouvelles limites, dans un monde plus difficile à appréhender. La sécurité doit alors trouver de nouvelles voies de progrès à travers l'anticipation. Le développement de la capacité d'anticipation des managers de risques sera alors plus que jamais d'actualité. Elle constituera un levier de réactivité, et contribuera à placer la sécurité comme une véritable valeur ajoutée, avec L'Homme au centre du système.

La machine intelligente et autonome n'a pas d'émotion, ni de doute. Or, ce qui caractérise l'Homme, c'est sa capacité à se questionner et se remettre en question, à douter du bien-fondé de son action et à découvrir le monde qui l'entoure. Dans ce processus, il a développé un sens critique en donnant du sens à son action. C'est dans doute cela que j'ai voulu réintégrer dans le processus de décision, le sens. Le débat est alors posé.

Quelle est la place de l'Homme dans le monde de demain ?

Références

Ouvrages et chapitre d'ouvrage

- Albero, B. (2010). L'étude de cas: une modalité d'enquête difficile à cerner. Enjeux et dilemmes de l'autonomie. Une expérience d'autoformation à l'université. Etude de cas, 15-25.
- Amalberti, R. (1996). La conduite de systèmes à risques: le travail à l'hôpital. Presses universitaires de France.
- Amalberti, R. (2013). Piloter la sécurité: Théories et pratiques sur les compromis et les arbitrages nécessaires. Springer Science & Business.
- Aven, T. (2014). Risk, Surprises and Black Swans: Fundamental Ideas and Concepts in Risk Assessment and Risk Management. Routledge.
- Bignell, V., & Fortune, J. (1984). Understanding Systems Failure. Manchester University Press.
- Bouyssou, D., Marchant, T., Pirlot, M., Perny, P., Tsoukiàs, A., Vincke, P. (2006). Evaluation and decision models with multiple criteria. Stepping stones for the analyst. Springer.
- Dekker, S., 2002. The Field Guide to Human Error Investigations. Ashgate Publishing Ltd., Aldershot.
- Frontier, S., Pichod-Viale, D., Leprêtre, A., Davoult, D., & Luczak, C. (2008). Écosystèmes - 4ème édition - Structure, Fonctionnement, Évolution. Dunod.
- Gagnon, Y., C. (2005). L'étude de cas comme méthode d'analyse de recherche, presse universitaire de Quebec, ISBN 2-7605.
- Guyot, C. (1969). Initiation à la maintenabilité. Dunod.
- Hale, A., & Heijer, T. (2006). Is resilience really necessary? The case of railways. Resilience engineering: concepts and precepts, 125-148.
- Heger, D. (2006). An introduction to operational research. Austin, USA.
- Heinrich, H.W. (1931). Industrial accident prevention. McGraw-Hill, New York.
- Herrera, I., Woltjer. R. (2008). Comparing a multi-linear (STEP) and systemic (FRAM) method for accident analysis Safety, Reliability and Risk Analysis: Theory, Methods and Applications, Taylor & Francis.
- Hollnagel, E. (2004). Barriers and accident prevention. Aldershot: Ashgate.
- Hollnagel, E. (2006). Resilience: the challenge of the unstable. Resilience Engineering–Concepts and Precepts. Ashgate, Aldershot, 9-17.

- Hollnagel, E. (2011a). Prologue: the scope of resilience engineering. Resilience engineering in practice: A guidebook, xxix-xxxix.
- Hollnagel, E. (2011b). To learn or not to learn, that is the question. Resilience engineering in practice: A guidebook, 193-198.
- Hollnagel, E. (2011c). Epilogue – the Resilience Analysis Grid. Resilience engineering in practice: A guidebook, 275-296.
- Hollnagel, E., Paries, J., David, D. W., & Wreathall, J. (2010). Resilience engineering in practice: A guidebook.
- Hopkins, A., & Andrew, H. (2000). Lessons from Longford: the Esso gas plant explosion. North Ryde, New South Wales, Australia: CCH Australia limited.
- Kervern, G. Y., Rubise, P., Cousteau, J. Y., & Laborit, H. (1991). L'archipel du danger : introduction aux cindyniques. Editions Economica.
- Kjellén, U. (2000). Prevention of accidents through experience feedback. CRC Press.
- Laclémence, P. (2010). Psychoses d'hier, stratégie du lendemain. Défense Nationale et Sécurité Collective. Edition Française, (735), 27.
- Laclémence, P. (2012). Les comportements collectifs de panique : éléments de réflexion. In: Marret J.-L., Clavaud E., et Verneuil L. « Terrorisme NRBCE - les nouveaux défis opérationnels ». Ed. Paris : FRS et ENSOSP, p. 94-99., 350 pages.
- Laclémence, P. (2013). La sécurité globale : regards croisés et « hypervision éthique », dans Debove, Frédéric, Renaudie, Olivier (dir), Sécurité intérieure – les nouveaux défis, Vuibert.
- Lagadec, P. (2012). Du risque majeur aux mégachocs. Éditions Préventique.
- Lekka, C. (2011). High reliability organisations: A review of the literature. Health and Safety Laboratory, United Kingdom.
- Leplat, J. (1985). Les représentations fonctionnelles dans le travail.
- Lévêque, C. (2001). Ecologie. De l'écosystème à la biosphère.
- Llory, M. (1999). L'accident de la centrale nucléaire de Three-Mile Island, Éditions L'Harmattan, Paris.
- Mintzberg, H. (1984). Manager au quotidien, Les dix rôles du cadre. Les éditions d'organisation.
- Morin, E. (2011). La voie: pour l'avenir de l'humanité. Fayard.
- Paté-Cornell, E., (2004). On signals, response, and risk mitigation: A probabilistic approach to the detection and analysis of precursors. Dans J. R. Phimister, V. M. Bier & H. C. Kunreuther (Eds.), Accident Precursor Analysis and Management: Reducing

Technological Risk through Diligence (pp. 45-59). Washington, DC: The National Academies Press.

- Paries, J. (2011). Resilience and the ability to respond. Resilience engineering in practice: A guidebook, 3-8.
- Perrow, C. (1984). Normal accidents: Living with high risk systems. Basic Books, New York.
- Perrow, C. (2007). Disasters ever more? Reducing US vulnerabilities. In Handbook of disaster research (pp. 521-533). Springer New York.
- Power, M., (2008). Organized Uncertainty: Designing a World of Risk Management. Oxford University Press, Oxford.
- Rasmussen, J., & Svedung, I. (2000). Proactive risk management in dynamic society.
- Reason, J. (1990). Human error. Cambridge university press.
- Reason, J. (1997). Managing the risks of organizational accidents (Vol. 6). Aldershot: Ashgate.
- Roe, E., Schulman, P. (2008). High reliability Management. Stanford University Press.
- Rosa, H. (2010). Accélération. Une critique sociale du temps. Paris, La découverte.
- Roux-Dufort, C. (2000). La gestion de crise: un enjeu stratégique pour les organisations. De Boeck Supérieur.
- Roy, B. (1985). Méthodologie multicritère d'aide à la décision. Edition Economica, Paris.
- Roy, B., Bouyssou, D. (1993). Aide multicritère à la décision: méthodes et cas. Edition Economica, Paris
- Sfez, L. (1976). Critique de la décision. Presses de la Fondation nationale des sciences politiques.
- Simon, H. (1947). Administrative behaviour: a study of decision making processes in administrative organizations. Mac Millan, New York.
- Simon, H. A., Greffe, X., Dauzat, P. E. (1983). Administration et processus de décision. Economica.
- Thiétart, R. A. (2001). Management et complexité: concepts et théories.
- Tsoukiàs, A. (2006). De la théorie de la décision à l'aide à la décision. Dans Bouyssou, D. Dubois, D., Pirlot, M., Prade, H. Concepts et méthodes pour l'aide à la décision.
- Turner, B. A., & Pidgeon, N. F. (1978). Man-made disasters. Wykeham Publications (London).
- Vaughan, D. (1996). The Challenger launch decision: Risky technology, culture, and deviance at NASA. University of Chicago Press.

- Vaughan, D. (2001). La normalisation de la déviance: une approche d'action située. Organiser la fiabilité, 201-234.
- Villemeur, A. (1988). Sûreté de fonctionnement des systèmes industriels.
- Weick, K.E. (2001). Making Sense of the Organization. Blackwell Publishing, Oxford, UK.
- Weick, K. & Sutcliffe, K.L. (2007). Managing the unexpected. Second Edition. San Francisco, CA: Jossey- Bass.
- Wreathall, J. (2011). Monitoring – A critical ability in resilience engineering. Resilience engineering in practice: A guidebook, 61-68.
- Woods, D. (2011). Resilience and the ability to anticipate. Resilience engineering in practice: A guidebook, 121-125.
- Yin, R. K. (2003). Case study research: Design and methods (3rd ed.). Thousand Oaks, CA: Sage.

Articles de journal périodique

- Adoue, C. (2007). Mettre en œuvre l'écologie industrielle. Revue d'économie industrielle 1/2008 (n° 121), p. 126-126.
- Agulhon, S., & Guarnieri, F. (2014). L'injonction de sécurité comme dispositif de conquête de territoires organisationnels. Prospective et Stratégie, 4, 81-100.
- Akinci, C., & Sadler-Smith, E. (2012). Intuition in management research: A historical review. International Journal of Management Reviews, 14(1), 104-122.
- Alcouffe, S., Berland, N., & Levant, Y. (2009). «Succès» et «échec» d'un outil de gestion. Revue française de gestion, (8), 291-306.
- Allford, L. (2009). Process safety indicators: response to Andrew Hopkins. Safety Science, 47, 466.
- Arnaudiès, J.M. (2005). La Catastrophe de Toulouse. Natures Sciences Sociétés 13, 421-425.
- Arnott, D. (1998). A taxonomy of decision biases. Monash University, School of Information Management and Systems, Caulfield.
- Aven, T., (2011). On risk governance deficits. Safety Science, 49(6), 912-919.
- Bliss, J. P., Gilson, R. D., (1998). Emergency signal failure: Implications and recommendations. Ergonomics, 41(1), 57–72.
- Bourguignon, A., Jenkins, A. (2004). Changer d'outils de contrôle de gestion ? De la cohérence instrumentale a la cohérence psychologique. Finance/Contrôle/Stratégie Volume, (7), 31-61.
- Calcei, D., M'Chirgui, Z., & Ohana, M. (2009). Sexes, mensonges et vidéo. Liaisons et déliaisons dans les écosystèmes d'affaires des formats de stockage vidéo. Management & Avenir, (9), 88-88.
- Canet, E., Roux, L., Szpirglas, M. (2012). De la place de l'intuition dans la décision: le cas des équipes médico-sociales des conseils généraux. Management & Avenir, (9), 150-171.
- Carroll, J. S., & Fahlbruch, B. (2011). "The gift of failure: New approaches to analyzing and learning from events and near-misses." Honoring the contributions of Bernhard Wilpert. Safety science, 49(1), 1-4.
- Chapanis, A. (1963). Engineering psychology. Annual review of psychology, 14(1), 285-318.
- Dammak, A. (2013). L'intuition des dirigeants : essai de définition et conceptions managériales. Scientific Bulletin-Economic Sciences, 12(2), 67-84.

- Dane E., Pratt, M.G. (2007). Exploring intuition and its role in managerial decision making. Academy of Management Review, Vol. 32, No.1, p. 33-54.
- David, A. (1998). Outil de gestion et dynamique du changement. Revue Française de Gestion, Juillet, pp. 44-59.
- Detchessahar, M., Journé, B. (2007). Une approche narrative des outils de gestion. Revue française de gestion, (5), 77-92.
- De Vaujany, F. X. (2006). Pour une théorie de l'appropriation des outils de gestion: vers un dépassement de l'opposition conception-usage. Management & Avenir, (3), 109-126.
- Fahlbruch, B., & Wilpert, B. (1997). Event analysis as problem solving process. After the Event–From Accident to Organisational Learning, Pergamon, 113-130.
- Fréry, F., Gratacap, A., & Isckia, T. (2012). Les écosystèmes d'affaires, par-delà la métaphore. Revue française de gestion, (3), 69-75.
- Frosch, R. A. (1995). Industrial ecology: Adapting technology for a sustainable world. Environment: Science and Policy for Sustainable Development, 37(10), 17-37.
- Grant, J., Brown, D., (2005). The inspector cometh. Canadian HR Reporter 18, 13–17.
- Hale, A. R. (2003). Safety management in production. Human Factors and Ergonomics in Manufacturing & Service Industries, 13(3), 185-201.
- Hale, A. R., & Hovden, J. (1998). Management and culture: the third age of safety. A review of approaches to organizational aspects of safety, health and environment. Occupational injury: Risk, prevention and intervention, 129-165.
- Hale, A. (2009). Why safety performance indicators? Safety Science, 47(4), 479-480.
- Hansson, S. O. (2012). Safety is an inherently inconsistent concept. Safety science, 50(7), 1522-1527.
- Hiltunen, E., (2008a). Good sources of weak signals: a global study of where futurists look for weak signals. Journal of Futures Studies, May 2008, 12(4): 21 – 44.
- Hiltunen, E., (2008b). The future sign and its three dimensions. Futures, Volume 40, Issue 3, Avril 2008, Pages 247–260.
- Hinze, J., Thurman, S., & Wehle, A. (2013). Leading indicators of construction safety performance. Safety science, 51(1), 23-28.
- Hohnen, P., & Hasle, P. (2011). Making work environment auditable, A 'critical case' study of certified occupational health and safety management systems in Denmark. Safety Science, 49(7), 1022-1029.
- Hollings, J. (2013). Let the story go: The role of emotion in the decision-making process of the reluctant, vulnerable witness or whistle-blower. Journal of business ethics, 114(3), 501-512.

- Hollnagel, E. (2008). Risk+ barriers= safety? Safety Science, 46(2), 221-229.
- Hollnagel, E. (2014). Is safety a subject for science? Safety Science, 67, 21-24.
- Hopkins, A. (2009). Thinking about process safety indicators. Safety Science, 47(4), 460-465.
- Hopkins, A. (2009). Reply to comments. Safety Science, 47(4), 508-510.
- Journé, B., Grimand, A., & Garreau, L. (2012). Face à la complexité. Illusions, audaces, humilités. Revue française de gestion, (4), 15-25.
- Katsakiori, P., Sakellaropoulos, G., & Manatakis, E. (2009). Towards an evaluation of accident investigation methods in terms of their alignment with accident causation models. Safety Science, 47(7), 1007-1015.
- Keller, W., & Modarres, M. (2005). A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late Professor Norman Carl Rasmussen. Reliability Engineering & System Safety, 89(3), 271-285.
- Kongsvik, T., Almklov, P., Haavik, T., Haugen, S., Vinnem, J. E., & Schiefloe, P. M. (2015). Decisions and decision support for major accident prevention in the process industries. Journal of Loss Prevention in the Process Industries.
- Laflamme, L. (1990). A better understanding of occupational accident genesis to improve safety in the workplace. Journal of Occupational Accidents, 12(1), 155-165.
- Le Coze, J. C. (2013). New models for new times. An anti-dualist move. Safety science, 59, 200-218.
- Le Coze, J. C. (2013). Outlines of a sensitising model for industrial safety assessment. Safety science, 51(1), 187-201.
- Lehto, M., & Salvendy, G. (1991). Models of accident causation and their application: review and reappraisal. Journal of Engineering and Technology Management, 8(2), 173-205.
- Leveson, N. (2004). A new accident model for engineering safer systems. Safety Science, 42 (2004), pp. 237–270.
- Leveson, N., Dulac, N., Marais, K., & Carroll, J. (2009). Moving beyond normal accidents and high reliability organizations: a systems approach to safety in complex systems. Organization Studies, 30(2-3), 227-249.
- Llory, M. & Dien, Y. (2010). Systèmes complexes à risques : Analyse organisationnelle de la sécurité. Techniques de l'ingénieur. Théorie et management des systèmes complexes, Editions T.I.

- Midgley, E., and Pierce, F.T., 1926, "The Weakest Link Theorems on Strength of Long and of Composite Specimens," Journal of the Textile Institute, vol. 17, no. 2, pp. T355-T368.
- Moore, J. F. (1993). Predators and prey: a new ecology of competition. Harvard business review, 71(3), 75-83.
- Moorkamp, M., Kramer, E. H., van Gulijk, C., & Ale, B. (2014). Safety management theory and the expeditionary organization: A critical theoretical reflection. Safety Science, 69, 71-81.
- Nilsen, P., Hudson, D. S., Kullberg, A., Timpka, T., Ekman, R., & Lindqvist, K. (2004). Making sense of safety. Injury Prevention, 10(2), 71-73.
- Ochanine, D. (1978). Le rôle des images opératives dans la régulation des activités de travail. Psychologie et éducation, 2(3), 63-79.
- Øien, K., Utne, I.B., Tinmannsvik, R.K., Massaiu, S. (2010). Building Safety Indicators. Part 2-Application, practices and results Safety Science, 49 (2) (2010), pp. 162–171.
- Øien, K., Utne, I. B., & Herrera, I. A. (2011). Building safety indicators: Part 1–theoretical foundation. Safety science, 49(2), 148-161.
- Oiry, E. (2011). Usages imprévus et dynamique des instruments de gestion. Réflexions à partir du cas d'un instrument de gestion des compétences. Management international/International Management/Gestiòn Internacional, 15(2), 11-22.
- Phimister, J. R., Oktem, U., Kleindorfer, P. R., & Kunreuther, H. (2003). Near-Miss Incident Management in the Chemical Process Industry. Risk Analysis,23(3), 445-459.
- Power, M., (1996). Making things auditable. Accounting Organizations and Society 21, 289–315.
- Power, M., 2003. Auditing and the production of legitimacy. Accounting Organizations and Society 28, 379–394.
- Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. Safety science, 27(2), 183-213.
- Reason, J., Hollnagel, E., & Paries, J. (2006). Revisiting the «Swiss cheese» model of accidents. Journal of Clinical Engineering, 27, 110-115.
- Reiman, T., Pietikäinen, E. (2012). Leading indicators of system safety–monitoring and driving the organizational safety potential. Safety science, 50(10), 1993-2000.
- Roberts, K. H. (1990). Some characteristics of one type of high reliability organization. Organization Science, 1(2), 160-176.
- Robson, L. S., Bigelow, P. L. (2010). Measurement properties of occupational health and safety management audits: a systematic literature search and traditional literature

synthesis. Canadian Journal of Public Health/Revue Canadienne de Santé Publique, S34-S40.

- Robson, L. S., Macdonald, S., Gray, G. C., Van Eerd, D. L., & Bigelow, P. L. (2012). A descriptive study of the OHS management auditing methods used by public sector organizations conducting audits of workplaces: Implications for audit reliability and validity. Safety science, 50(2), 181-189.
- Rochlin, G. I. (1993). Defining "high reliability" organizations in practice: a taxonomic prologue. New challenges to understanding organizations, 11-32.
- Rochlin, G.I. (1999). Safe operation as a social construct. Ergonomics, 42 (11), pp. 1549–1560.
- Rossel, P., (2012). Early detection, warnings, weak signals and seeds of change: A turbulent domain of futures studies. Futures, 44(3), 229-239.
- Rouleau, L. (2005). Micro-practices of strategic sensemaking and sense giving: how middle managers interpret and sell change every day. Journal of Management Studies, 42(7), 1413-1441.
- Sadler-Smith E., Shefy, E. (2004). The intuitive executive: Understanding and apply 'gut feel' in decision making. Academy of Management Executive, Vol. 18, no. 4, p. 76-91.
- Saleh, J. H., Marais, K. B., Bakolas, E., & Cowlagi, R. V. (2010). Highlights from the literature on accident causation and system safety: Review of major ideas, recent contributions, and challenges. Reliability Engineering & System Safety, 95(11), 1105-1116.
- Scherpereel, C. M. (2006). Decision orders: a decision taxonomy. Management Decision, 44(1), 123-136.
- Sklet, S. (2004). Comparison of some selected methods for accident investigation. Journal of hazardous materials, 111(1), 29-37.
- Slovic, P., Finucane, M. L., Peters, E., MacGregor, D. G. (2007). The affect heuristic. European journal of operational research, 177(3), 1333-1352.
- Spieth, G. (2013). Les doléances citoyennes vers un écosystème, au service de l'innovation des politiques publiques de la Métropole Nice Côte d'Azur ? Management & Avenir, 62(4), 188-208.
- Strathern, M., (2000). Introduction: new accountabilities. In: Strathern, M. (Ed.), Audit Cultures: A Tropological Studies in Accountability, Ethics and Academy. Routledge, London and New York.
- Tanner Jr, W. P., & Swets, J. A. (1954). A decision-making theory of visual detection. Psychological review, 61(6), 401.

- Tansley, A. G. (1935). The use and abuse of vegetational concepts and terms. Ecology, 16(3), 284-307.
- Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. science, 185(4157), 1124-1131.
- Vinodkumar, M. N., & Bhasi, M. (2011). A study on the impact of management system certification on safety management. Safety Science, 49(3), 498-507.
- Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: Processes of collective mindfulness. Crisis management, 3, 81-123.
- Wilde, G. J. (1982). The theory of risk homeostasis: implications for safety and health. Risk analysis, 2(4), 209-225.
- Woodside, A. G., & Wilson, E. J. (2003). Case study research methods for theory building. Journal of Business & Industrial Marketing, 18(6/7), 493-508.

Thèse, mémoire de recherche et rapport

- Baker, J., Leveson, N., Bowman, F., Priest, S., Erwin, G., Rosenthal, I., Wilson, L. D. (2007). The report of the BP US refineries independent safety review panel. BP US Refineries Independent Safety Review Panel.
- Barthelemy, F., Hornus, H., Roussot, J., Hufschmitt, J.P., Raffoux, J.F. (2001). Rapport de l'Inspection générale de l'environnement. Usine de la société Grande Paroisse à Toulouse - Accident du 21 septembre 2001. Conjoint avec l'inspection des poudres et avec le concours de l'INERIS.
- Bell, J., & Holroyd, J. (2009). Review of human reliability assessment methods. Health and Safety Laboratory, United Kingdom.
- British Government Report (1912). Loss of the Steamship « Titanic ».
- Bureau d'analyse des risques et des pollutions industrielles, (2006). Fiche n°5692, Explosion de la Poudrerie de Grenelle, Ministère chargé de l'environnement.
- CCPS, (2010). Guidelines for process safety metrics. Wiley.
- Daniellou, F., Boissières, I., & Simard, M. (2010). Les facteurs humains et organisationnels de la sécurité industrielle: un état de l'art.
- Deepwater Horizon Study Group, (2011). Final report on the investigation of the Macondo well blowout, 126p.
- Gauthey, O. (2005). Le retour d'expérience. État des pratiques en milieu industriel. Collection Cahiers de la Sécurité Industrielle, (2).
- Gayon, A. (2001). Importance de la sécurité dans les entreprises. Techniques de l'ingénieur. Sécurité et gestion des risques, (AG4600), AG4600-1.
- Health and Safety Executive, Chemical Industries Association, (2006). Developing Process Safety Indicators. A Step-by-step Guide for Chemical and Major Hazard Industries.
- Health and Safety Laboratory, (2011). High reliability organisations, A review of literature. Health and safety Executive.
- ISO 31000, Management du risque – Principes et lignes directrices, ISO (2009).
- Hopkins, A. (2007). The problem of defining high reliability organisations. National Research Center for Occupational Safety and Health Regulation. January.
- Luxhøj, J.T., Kauffeld, K. (2003). "Evaluating the Effect of Technology Insertion into the National Airspace System". The Rutgers Scholar.

- Mazars-Chapelon, A., Cazes-Milano, P. (2000). Techniques et outils de gestion : Un même concept ? Cahier n° 281. Mars 2000.
- Mazri, C. (2007). Apport méthodologique pour la structuration de processus de décision publique en contexte participatif: le cas des risques industriels majeurs en France (Doctoral dissertation, Université Paris-Dauphine).
- Mbaye, S. (2010). Le retour d'expérience, analyse comparée des pratiques de rex dans les industries chimiques et nucléaires. Collection Cahiers de la Sécurité Industrielle, (5).
- Menessier. M. (2009). AZF : il y a eu deux explosions le 21 septembre 2001. Publié le 17/04/2009. www.lefigaro.fr.
- Mevel, O., (2004). Du rôle des signaux faibles sur la reconfiguration des processus de la chaîne de valeur de l'organisation: l'exemple d'une centrale d'achats de la grande distribution française. Mémoire de Doctorat. Université de Bretagne occidentale-Brest.
- Ministère de l'écologie, du Développement Durable, et de l'Energie, (2013). Rapport sur la sécurité aérienne 2013.
- Mogford, J., (2005), Isomerization Unit Explosion Final Report: Texas City. Fatal Accident investigation Report.
- NASA National Aeronautics and Space Administration, (2003). Report of the Columbia Accident Investigation Board.
- Øien, K., (2001). Risk Control of Offshore Installations. A Framework for the Establishment of Risk Indicators. Department of Production and Quality Engineering, PhD thesis. Norwegian University of Science and Technology (NTNU), Trondheim, Norway.
- Office for Nuclear Regulation., (2011), Japanese earthquake and tsumani: implications for the UK nuclear industry – Final Report.
- Pitkänen, R., (2006). interviewed by Jari Koskinen in an article: Tulevaisuuden tutkimuksesta kilpailuetua-Opponentti (Competitive advantage from futures research—an opponent), Yritystalous—Walk About-Stories from Flat World.
- Raymond, V. (1952). Cause des accidents de travail: le geste néfaste. Archives des maladies professionnelles, 13(5), 450-452.
- Rigaud, E. (2011). La résilience, analyse étymologique. Collection Cahiers de la Sécurité Industrielle.
- Shannon, C. E. (1948). Bell System Tech. J. 27 (1948) 379; CE Shannon. Bell System Tech. J, 27, 623.

- Shappel, S. A., & Wiegmann, D. A. (2000). The human factors analysis and classification system--HFACS (No. DOT/FAA/AM-00/7). US Federal Aviation Administration, Office of Aviation Medicine.
- Transportation Safety Board of Canada, (2014). Lac-Mégantic runaway train and derailment investigation summary.
- United States President's Commission on the Accident at Three Mile Island (1979). The need for change, the legacy of TMI: report of the President's Commission on the Accident at Three Mile Island. The Commission.
- Urfalino, P. (2005). La décision fut elle jamais un objet sociologique ? Document de travail. CESTA (EHESS-CNRS).
- Valeurs actuelles. (2003). AZF : l'hypothèse de la double explosion relancée. Publié le 24 janvier 2003.

Actes de congrès, conférences et colloques

- Ansoff, H. I. (1975). Managing Strategic Surprise by Response to Weak Signals. California management review, 18(2).
- Dechy, N., Dien, Y., & Llory, M., (2008). Les échecs du retour d'expérience: problématiques de la formalisation et de la communication des enseignements tirés, Actes du 16ème Congrès de maîtrise des risques et sûreté de fonctionnement, Avignon.
- Delatour, G., Laclémence, P., Calcei, D., Mazri, C. (2013). Blind Managers, Systems Complexity and Weak Signals. Proceedings of 22nd International Business Research Conference. World Business Institute Australia.
- Delatour, G., Laclémence, P., Calcei, D., Mazri, C. (2014a). Système de gestion de la sécurité : quel espace critique pour la décision d'anticipation ? Congrès Lambda Mu 19.
- Delatour, G., Laclémence, P., Calcei, D., Mazri, C. (2014b). Safety Performance Indicators: a questioning diversity. Chemical Engineering Transactions 36, 55–60. The Italian Association of Chemical Engineering, 2014.
- Frantzen, C., (2004). Tango on Asymptote. SRA-E Annual Conference, November 15–17, Paris.
- Hollnagel, E. (2002). Understanding accidents-from root causes to performance variability. In Human factors and power plants, 2002. proceedings of the 2002 IEEE 7th conference on (pp. 1-1). IEEE.
- Le Coze, J. C., Plot, E., Prats, F., Salvi, O., & Vince, A. S. (2002). Development of the ATOS concept, analysis of technical and organisational safety. In Congrès ESREL 2002" Aide à la Décision et Maîtrise des Risques".
- Lesca, H., Blanco, S., (2002). Contribution à la capacité d'anticipation des entreprises par la sensibilisation aux signaux faibles. 6ème congrès international francophone sur la PME, pp. 10-1.
- Mazri, C., Delatour, G., Laclémence, P., Calcei, D., (2014). De l'émergence dans les risques émergents, Actes du 19ème Congrès de maitrise des risques et sûreté de fonctionnement Lambda Mu, Dijon.
- Mazri, C., Delatour, G., Laclémence, P., Calcei, D., (2014). Indicators in Safety Management: a cartography of Approaches and Applications. Proceedings of the Spring Meeting & 10th Global Congress on Process Safety.
- Moisdon, J. C. (1997). Du mode d'existence des outils de gestion. Actes du séminaire Contradictions et Dynamique des Organisations-CONDOR-IX, 6.

- Øien, K., (2008). Development of early warning indicators based on accident investigation. In: International Probabilistic Safety Assessment and Management Conference PSAM9. Hong Kong, China, 18–23 May 2008.
- Qureshi, Z. H. (2007). A review of accident modelling approaches for complex socio-technical systems. In Proceedings of the twelfth Australian workshop on Safety critical systems and software and safety-related programmable systems-Volume 86 (pp. 47-59). Australian Computer Society, Inc.
- Rasmussen, J. (1983). Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models. Systems, Man and Cybernetics, IEEE Transactions on, (3), 257-266.
- Richard P.H., Laclémence P. (2013). Ville intelligente et sécurité globale. Convergences, avantages et limites pour de nouveaux paradigmes. Communication au Workshop Interdisciplinaire sur la Sécurité Globale WISG'12 – 22 & 23 janvier 2013, Troyes.
- Roberts, K. H., & Rousseau, D. M. (1989). Research in nearly failure-free, high-reliability organizations: having the bubble. Engineering Management, IEEE Transactions on, 36(2), 132-139.
- Saltmarsh, E.A., Saleha J.H., Mavris, D.N. (2012). Accident precursors: critical review, conceptual framework, and Failure machanisms. 11th international probabilistic safety assessment and management conference and the annual European safety and reliability conference.

Crédits iconographiques

- Edvard Munch, *Le Cri*, 1893, Peinture sur toile, 91 x 73 cm, National Gallery, Oslo

Liste des Figures

Figure 1 : Structure méthodologique du mémoire 19
Figure 2 : La sécurité à travers à la prévention et la protection, adapté de Hollnagel (2008)..... 29
Figure 3 : Démarche de réalisation de l'étude de cas 38
Figure 4 : Répartition spatiale et temporelle des cas sélectionnés pour l'analyse 51
Figure 5 : Types d'action mis en œuvre pour la sécurisation des systèmes technologiques..... 53
Figure 6 : Familles de causes des accidents industriels majeurs..... 56
Figure 7 : Modélisation d'un système sociotechnique complexe, tiré de Rasmussen et al. (2000) 70
Figure 8 : Identification de l'espace de contrainte décisionnel du manager opérationnel 77
Figure 9 : Les multiples niveaux hiérarchiques d'un système industriel..... 80
Figure 10 : Correspondance entre développements scientifiques, réglementaires, et les accidents industriels..... 94
Figure 11 : Les grands développements scientifiques du XXème siècle, relatifs à la sécurité industrielle 102
Figure 12 : Taxinomie des modèles d'accidents selon Lheto et al. (1991) 109
Figure 13 : Evolution de la recherche dans le nucléaire, selon Fahlburgh et al. (1997)..... 110
Figure 14 : Evolution des idées relatives aux modèles d'accident, selon Saleh et al., (2010)..... 111
Figure 15 : Relation entre le danger, les défenses, et les pertes, traduit de Reason (1997)..... 117
Figure 16 : Durée de vie d'une organisation hypothétique, dans l'espace production protection, traduit de Reason (1997)..... 118
Figure 17 : Trajectoire accidentelle traversant les barrières de défense, adapté de Reason (1997) 120
Figure 18 : Etapes dans le développement et l'enquête d'un accident organisationnel, tiré de Reason, (1997)..... 121
Figure 19 : Courants agissant dans l'espace de sécurité, traduit de Reason (1997) 122
Figure 20 : Résumé des principaux facteurs impliqués pour la navigation dans l'espace de sécurité, traduit de Reason (1997)..... 124
Figure 21 : Sous-systèmes organisationnels de sécurité sous-jacents au process primaire, traduit de Reason (1997)..... 126
Figure 22 : Principaux processus et caractéristiques relatifs aux HRO, traduit de Lekka (2011) 132
Figure 23 : Modélisation d'un système sociotechnique complexe, tiré de Rasmussen et al. (2000) 142
Figure 24 : Migration du système au-delà des limites de performance acceptable, adapté de Rasmussen (1997) 143

Figure 25 : Système de contrôle adaptatif connectant la production, la sécurité, et l'économie, traduit de Rasmussen et al. (2000) 145
Figure 26 : La gestion de la sécurité, comme résolution d'un problème à trois niveaux, traduit de Hale (2003) 150
Figure 27 : Le cycle de vie de la gestion de la sécurité, traduit de Hale (2003) 152
Figure 28 : Système de gestion de la sécurité, résolution de problème et feedback, traduit de Hale (2003) 153
Figure 29 : La sécurité au prisme de l'ingénierie de la résilience, tiré de Rasmussen (2011) 160
Figure 30 : Les quatre pierres angulaires de la résilience, adapté de Hollnagel (2011) 161
Figure 31 : Modèle classique de théorie du contrôle, adapté de Wreathall (2011) 165
Figure 32 : Diagramme en étoile agrégé, adapté de Hollnagel (2011c) 168
Figure 33 : Dynamique d'émergence de la rupture managériale 209
Figure 34 : Processus d'aide à la décision, adapté de Tsoukiàs (2006) 214
Figure 35 : Modèle conceptuel des facteurs affectant la fiabilité et la validité des audits des systèmes de gestion de la sécurité, adapté de Robson et al. (2012). 222
Figure 36 : L'écosystème décisionnel du manager 250
Figure 37 : Pistes de développement de l'écosystème décisionnel 252
Figure 38 : Stratégie de complémentarité des outils de gestion 256
Figure 39 : Familles de causes des accidents industriels majeurs 327

Liste des Tableaux

Tableau 1 : Intérêts et limites de l'étude de cas, adapté de Gagnon (2005) 37
Tableau 2 : Modèle de grille d'analyse des accidents 46
Tableau 3 : Principaux accidents industriels majeurs parmi les plus marquants depuis ces 50 dernières années 47
Tableau 4 : Principaux accidents de transport parmi les plus marquants depuis ces 50 dernières années 48
Tableau 5 : Description de l'échantillon d'accidents sélectionnés pour l'analyse 50
Tableau 6 : Description des conséquences des principaux accidents majeurs 104
Tableau 7 : Liste des principaux modèles de production de sécurité sélectionnés 113
Tableau 8 : Typologie des résultats possibles, traduit de Hollnagel (2011c) 159
Tableau 9 : Synthèse des limites des modèles sélectionnés 191
Tableau 10 : Principaux référentiels relatifs aux indicateurs de gestion 227
Tableau 11 : Comparaison des outils de gestion 235

Annexes

Annexe n°1 : Analyse de 10 accidents industriels majeurs passés

L'accident de Delft

L'explosion de la poudrière de Delft est l'un des plus anciens accidents industriels répertoriés. Elle s'est produite le 12 octobre 1654 dans le sud de l'actuel Pays-Bas. Vers 10h du matin, un entrepôt renfermant 90000 livres de poudre à base de nitrate explose. Le nombre précis de victimes n'a jamais été établi, mais les historiens estiment que la catastrophe aurait causé au moins une centaine de morts. Un chiffre de «quelques centaines» n'est pas à exclure, au regard des destructions visibles sur les toiles peintes à la suite de la catastrophe. Avec cette ancienneté, ce cas souffre d'une quantité faible de références, qui interdit toute analyse approfondie. Il est donc difficile de déterminer une représentation fidèle de la chaine accidentelle. Pour autant, plusieurs éléments relatifs aux conséquences de l'explosion, et à ses origines, ont été rapportés.

1. Principales étapes accidentelles	2. Faits	3. Ecart entre le système de gestion de la sécurité et la réalité
Explosion de 90000 livres de poudre.	• le gérant de la poudrière est entré dans le lieu d'entreposage pour y chercher un échantillon d'explosif. Quelques étincelles projetées de sa lanterne auraient alors atteint la poudre. • A l'époque, des règles de maitrise des risques existaient déjà. La réalisation des poudrières répondait à des règles de conception, telles que la construction souterraine, des dimensions restreintes, et des murs de pierre très épais.	Analyse des risques : malgré la dangerosité des produits chimiques utilisés par le process, des sources d'inflammation ont été introduites sans mesures particulières. De plus, les moyens de protection existants n'ont pas été suffisamment dimensionnés pour contenir le scénario accidentel du jour de l'accident.

L'accident de Grenelle

La catastrophe de la *Poudrière de Grenelle* se déroula au cœur de la nouvelle ville industrielle de Grenelle, en périphérie de Paris. En pleine révolution française, La Convention cherche à développer la production de poudre à canon, et reconvertit le Château de Grenelle. Le 31 août 1794, à 7h15 du matin, 65000 livres de poudre explosent dans le magasin de poudre. Le bruit engendré par l'explosion est entendu jusqu'à Fontainebleau. Les hôpitaux sont débordés par une arrivée massive de blessés. L'explosion cause d'importants dommages matériels. Sa puissance est telle que les maisons du quartier sont ébranlées, les ponts lézardés. Cette catastrophe entraîne la mort de plus de 1000 personnes.

1. Principales étapes accidentelles	**2. Faits**	**3. Ecart entre le système de gestion de la sécurité et la réalité**
Explosion de 65000 livres de poudre.	• Le château de Grenelle était situé au cœur du village. Lors de l'explosion, les habitants, proches, ont été directement impactés par le souffle. • la poudrerie de Grenelle a fait l'objet d'un récent changement des méthodes de travail, dans le but d'accroitre la production journalière. En effet, les besoins en poudre sont tels que des moyens plus productifs, mais aussi plus dangereux sont privilégiés. Les ouvriers broyaient les ingrédients à la force des bras dans des tonneaux tournants remplis en partie de billes de bronze. Le mélange séquentiel des composants et le broyage mécanisé à l'aide de pilon à fait place à un mélange simultané et un mélange manuel. • Les nouvelles méthodes de travail multiplient la production journalière de salpêtre. Celle-ci passe de 8000 à 35000 livres par jour. • Les conditions de travail n'étaient pas adaptées à la manipulation de poudre explosive : l'ambiance de travail était surchauffée, 2000 ouvriers étaient entassés dans l'atelier, et aucune mesure de protection n'était utilisée. • A plusieurs reprises, le directeur de la fabrication, docteur en chimie, a émis des inquiétudes sur les risques générés par ce changement rapide d'organisation. Il n'a cessé d'exposer au Comité de Salut Public que cette rapide progression ne peut se faire sans risque majeur.	La maitrise de l'urbanisme : l'implantation d'une poudrerie dans le château conduit à placer une activité dangereuse à proximité de zone d'habitation et de population. Le jour de l'accident, cette proximité a conduit à des conséquences catastrophiques. La gestion du changement : le changement de méthode de production et de rythme de travail a été réalisé sans tenir compte des impacts sur les risques générés par le process. L'analyse des risques : le mélange simultané et manuel des composants à un induit une perte de stabilité chimique de la poudre. Les signaux faibles et lanceurs d'alerte : plusieurs signaux d'alertes ont été émis par une autorité scientifique. Pour autant, l'organisation n'a pas été en mesure d'entendre ces signaux, annonciateurs de l'accident.

L'accident d'Oppau

Située au sud-ouest de l'actuelle Allemagne, la ville d'Oppau accueille en 1911 un site de synthèse d'ammoniac. Celui-ci est reconverti deux ans plus tard en site de production de nitrate d'ammonium. 8000 personnes travaillent à la production d'engrais azoté. Le 21 septembre 1921, alors qu'un opérateur prépare des trous pour réaliser des tirs d'explosif, une explosion non maitrisée se produit dans un silo contenant environ 4000 tonnes de produits. Les dégâts sont considérables. Le nuage de poussière laisse place à un cratère 90 m de large, 125 m de long et 20 m de profondeur. Le bilan humain officiel de cette catastrophe fait état de 561 morts, 1 952 blessés et 7 500 personnes sans-abris.

1. Principales étapes accidentelles	**2. Faits**	**3. Ecart entre le système de gestion de la sécurité et la réalité**
Explosion de 4000 tonnes de produits chimiques dangereux.	• Lors d'essais préalables réalisés en 1919, l'exploitant avait conclu que les mélanges de sulfate et de nitrate d'ammonium renfermant moins de 60 % de nitrate d'ammonium n'étaient pas susceptibles d'exploser. En conséquence, cet engrais était traité comme une matière ne présentant aucun danger. Il était donc stocké en très grande quantité sur le site. A titre d'exemple, l'un des bâtiments de stockage possède une capacité de stockage de 50000 tonnes. L'exploitant a également sous-estimé le rôle de paramètres tels que la composition du mélange, et certains paramètres physiques (densité, humidité…) sur la capacité d'un mélange à exploser. • Dans les mois précédant l'accident, des modifications ont été apportées au procédé de fabrication : le mélange fabriqué renferme moins d'humidité qu'auparavant (2 % au lieu de 3 à 4 %) et présente une densité un peu plus faible. Les experts ont conclu que ces modifications rendaient plus facile l'explosion du mélange. De plus, lors de la modification du procédé en 1921, des tests auraient dû être réalisés sur le nouveau mélange, afin de vérifier la bonne stabilité du produit. Mais ces tests n'ont pas été réalisés. • 2 mois avant l'accident d'Oppau, l'explosion d'un wagon de nitrate d'ammonium à la suite d'un amorçage à l'explosif, à Kriewald (Allemagne), avait fait 19 morts.	Analyse des risques : l'analyse des risques n'a pas pris en considération le potentiel réel de danger du produit stocké. En conséquence, les mesures de prévention mis en œuvre, sous-estimées, n'ont pas joués leur rôle de barrière de sécurité. Gestion du changement : des tests étaient théoriquement prévus après la modification du procédé en 1921. La non-réalisation de ces tests n'a pas permis d'identifier le niveau réel de risque du process. Retour d'expérience : l'occurrence d'un accident majeur similaire aurait dû être l'occasion de s'interroger le niveau de dangerosité et de stabilité des stockages de produits composés de nitrate d'ammonium.

	• Le jour de l'accident, alors que l'opérateur prépare les trous pour réaliser les tirs du jour, une explosion se produit dans un silo contenant environ 4000 tonnes.	

L'accident de Texas City

L'explosion du cargo français *Grandcamp* eu lieu le 16 avril 1947, dans le port marchand de la ville de Texas City, aux Etats-Unis. L'explosion du chargement de nitrate d'ammonium fut entendue dans un rayon de 240 km, et fit au moins 581 morts et plus de 3000 blessés. Approximativement 1000 habitations et immeubles ont été détruits ou ont subi des dommages structurels importants. Pratiquement toutes les fenêtres exposées au souffle ont explosé. Des morceaux de métal issus du cargo ont été retrouvés à quatre kilomètres. Le coût des destructions terrestres est estimé à 40 millions de dollars.

1. Principales étapes accidentelles	2. Faits	3. Ecart entre le système de gestion de la sécurité et la réalité
Explosion d'un cargo de transport de produits chimiques dangereux.	La cargaison présente dans le cargo avait été fabriquée à partir de surplus de poudre de guerre reconditionnée. Celle-ci présentait donc probablement des impuretés. Aucune instruction n'était imprimée sur les sacs de nitrate d'ammonium, concernant l'explosivité du produit et ses conditions de manipulation et de stockage. La dangerosité de la cargaison du bateau à quai n'était pas connue de l'ensemble des autorités du port, et notamment des services de secours. De plus, le port ne possédait pas de plan d'urgence intégrant les moyens de secours disponibles (pompiers, hôpitaux...). **L**e rapport d'accident met en lumière le problème de maitrise des points chauds lors de la manipulation des cargaisons dangereuses. La consommation de cigarettes, et l'usage de flammes nues ne faisaient pas l'objet d'une règlementation strictement appliquée, alors que c'est une source probable d'explosion. Parmi les nombreuses destructions, le cargo *High Flyer*, situé à proximité, a explosé seize heures après l'explosion du *Grandcamp*. Plusieurs accidents majeurs ont eu lieu pendant la première moitié du XXème siècle, et mettant en cause le même produit chimique dangereux : En 1918 à	<u>Documentation sécurité :</u> l'imprécision de l'étiquetage des contenants de nitrate d'ammonium a généré une prise de risque non consciente lors des opérations de manipulation du produit. <u>Maitrise de l'urbanisation :</u> la forte proximité des installations de stockage et entreprises chimiques a permis l'occurrence d'effets dominos au sein du port. <u>Retour d'expérience :</u> une grande quantité de nitrate d'ammonium a été stockée et transportée lors de la dernière guerre, et aucun accident de grande ampleur n'a eu lieu. En conséquence, le nitrate d'ammonium a reçu peu d'attention au regard de son potentiel de danger.

	Morgan, aux Etats-Unis ; en 1921 à Oppau, en Allemagne ; ou encore en 1924 à Nixon, aux Etats-Unis.	

L'accident de Feyzin

Le 4 janvier 1966, la raffinerie de Feyzin explose, faisant 18 morts et 77 blessés. Lors d'une manœuvre de routine, une fuite de propane répand un nuage de gaz à l'extérieur du site. Au contact des véhicules passant sur l'autoroute, le gaz explose, entrainant l'incendie des sphères de stockage. Au-delà de la raffinerie, les dégâts matériels incluent des toitures endommagées jusqu'à 2,2 km, et des vitres brisées à plus de 8 km. L'explosion a été perçue jusqu'à 16 km en aval de la raffinerie.

1. Principales étapes accidentelles	2. Faits	3. Ecart entre le système de gestion de la sécurité et la réalité
Exploitation de la sphère et identification de signaux de risques.	Plusieurs difficultés ont été soulevées par les employés dès la réalisation des premières purges sur la sphère de stockage, sans générer de modifications : La conception de l'installation provoquait un givrage presque simultané des deux vannes lors de la détente du gaz. La commande des vannes par clé mobile présentait des risques en cas de chute d'une des clés. Le diamètre élevé des vannes, associé au givrage, les rendaient difficile à manœuvrer, et à fermer. La position basse du puisard (au pied de l'opérateur) occasionnait régulièrement des jets de liquide sur les opérateurs (brûlures au visage et aux mains). L'accès aux vannes était rendu difficile par la présence de canalisations que les opérateurs devaient enjamber. Deux accidents graves ont eu lieu dans les années précédentes : En août 1964, une fuite massive non contrôlée de matière lors d'une purge d'une sphère de butane a conduit à la blessure d'un opérateur. En février 1965, le même scénario accidentel a conduit à la blessure d'un opérateur. Ces deux accidents ont conduits à la publication d'une procédure « Ory » encadrant la réalisation de purge	Analyse des risques : le calcul du niveau de risque théorique était basé sur les référentiels normatifs de l'époque. Un niveau de sécurité satisfaisant était donc présent. Cependant, les pratiques de terrain ne correspondaient pas aux procédures théoriques. Bien que respectant les normes, la conception de la sphère (type d'équipements, positions des flux et des accès) présentait des difficultés de mise en œuvre de la procédure de purge. La phase de conception du système n'a fait l'objet que d'un développement ergonomique limité. Signaux faibles et lanceurs d'alerte : les difficultés liées à la conception dangereuse des installations ont été soulevée à plusieurs reprises par des membres du personnel. Les demandes de modification issues des opérateurs n'ont pas été prises en compte, manquant ainsi une opportunité d'améliorer le niveau de sécurité du système avant l'occurrence de l'accident. Formation du personnel : bien que connue des opérateurs, une procédure critique pour la sécurité n'a pas fait l'objet d'un processus de formation abouti. cette procédure ne remplissait donc pas sa fonction de sécurité, créant un écart entre le niveau de risque théorique, et la réalité du terrain.

	des sphères. Cette note était connue par le personnel, mais n'avais pas fait l'objet de démonstration. Aussi, cette procédure n'était pas appliquée par l'ensemble des opérateurs.	
Purge de la sphère pour une prise d'échantillon.	Le jour de l'accident, la manœuvre de purge a été réalisée à 6h40 du matin, dans la nuit noire, sous une lumière diffuse, à une température proche de zéro degré Celsius. Ces conditions sont contraires à celles définies dans la note de service « Ory ». La manœuvre des vannes a été effectuée d'une manière non conforme aux ordres donnés à l'opérateur. Les vannes présentaient des manques de lubrification. Cependant, cet aspect n'a pas été retenu comme contributeur de l'accident, le froid facilitant la manœuvre des leviers. Un dispositif d'écrou était prévu afin de bloquer la vanne de purge dans la position souhaitée, le temps des manœuvres, tout en évitant les chutes de clés de manœuvre. Ce dispositif n'était pas en place sur la sphère le jour de l'accident.	Règles et procédures : la manœuvre réalisée le matin de l'accident, et mise en cause dans la chaine accidentelle, n'a pas respecté la procédure opérationnelle. Ainsi, les mesures de sécurité initialement prévues n'étaient pas présentes pour remplir leur rôle. Formation du personnel : les opérateurs n'ont pas respecté les procédures de travail, traduisant l'échec du processus de formation. Intégrité mécanique : le manque de lubrification des vannes, mineur dans l'occurrence de l'accident, traduit cependant un manque d'efficacité du processus de maintenance des équipements, et notamment des vannes, qui sont critiques pour la sécurité du système. Analyse des risques : des dispositifs étaient prévus pour garantir la sécurité des équipements lors de la réalisation de manœuvres de purges de la sphère. Concrètement, ces équipements n'étaient pas installés.
Incendie et blève de la sphère.	La perte de contrôle des vannes a généré un nuage explosif. Celui-ci a été mis à feu par un véhicule qui passait sur l'autoroute, à proximité du site de stockage. Plusieurs éléments des systèmes d'urgence ont fait l'objet de difficultés lors de la conduite des opérations de secours : La réserve de poudre (1500 kg) a été épuisée en quelques minutes sans réussir à éteindre le foyer. La mise en œuvre du camion-mousse était impossible en raison du manque d'eau et de pression disponible. En constatant le début d'incendie, les agents de sécurité ont ouvert simultanément les systèmes de refroidissement des réservoirs contigus. De plus, la société voisine, branchée sur le même réseau d'eau, a également déclenché par précaution à son tour le	Analyse des risques : la présence de sources d'inflammation (autoroute) proche du site de stockage remet en cause les modèles d'analyse de risques utilisés pour la conception de la sphère. Préparation aux situations d'urgence : plusieurs éléments ont été une source de difficultés dans la lutte contre l'incendie : réserves d'agents d'extinction limitées, véhicules difficiles à mettre en œuvre, manque d'information des secours externes. Ainsi, même si des moyens adaptés étaient prévus en théorie, des défauts lors de leur mise en application (type de matériel, entretien, simulation d'intervention...) ont conduit à limiter leurs effets de manière importante.

	système de refroidissement de ses deux sphères de propane et les arrosait avec une lance à incendie. Ces ouvertures simultanées ont largement dépassé les capacités d'alimentation du réseau d'eau, privant les pompiers du débit et de la pression nécessaire à la gestion de l'incendie. Devant ces difficultés, la décision a été prise de mettre en œuvre un véhicule spécialisé dans la lutte contre les feux d'hydrocarbures. Cependant, cette manœuvre a été plus longue que prévue, du fait de l'absence d'accès aménagés. Le véhicule s'est enlisé et a été dépanné après une vingtaine de minutes d'efforts. Les secours externes étaient insuffisamment informés des risques et entraînés à ces pratiques. Par ailleurs, l'absence d'un point de commandement unique coordonnant l'action des différentes entités et services a été ressentie.	

L'accident de Bhopal

La catastrophe de Bhopal se déroula dans la nuit du 3 décembre 1984, à l'usine de pesticide de l'Union Carbide India Limited. Une réaction chimique incontrôlée dans un réservoir de stockage à conduit à la libération d'un nuage toxique à l'extérieur du site. Celui-ci survola la proche ville de Bhopal dans les heures qui ont suivies. Plus de Cinq cent mille personnes ont été exposées au nuage mortel, et au moins 10000 sont directement décédés.

1. Principales étapes accidentelles	**2. Faits**	**3. Ecart entre le système de gestion de la sécurité et la réalité**
Ralentissement des activités de production.	L'accident de 1984 est le dernier d'une série d'évènements critiques. Il y a eu six accidents au sein de l'usine de Bhopal entre 1978 et 1983, dont la plupart furent fatals. Dans les années précédant l'accident, plusieurs audits internes ont pointé des problèmes significatifs de sécurité (Juillet 1979, Mai 1982, Septembre et octobre 1982, Juin 1984). De plus, les autorités de contrôle n'étaient pas en mesure d'auditer efficacement les conditions de mise en œuvre des process industriels (dans les années 1980, seulement 15 inspecteurs devaient contrôler les 8000 usines de la province, et les deux inspecteurs mandatés pour l'usine de Bhopal n'étaient pas formés à l'ingénierie chimique). Pour faire face à ses difficultés financières, le management a fortement réduit le personnel sur le site de Bhopal (de 1350 à 950 personnes en quatre années, avec une part croissante d'opérateurs intérimaires). De plus, la plupart des employés ne parlaient pas l'anglais, qui était la langue opérationnelle, et notamment celle des consignes de sécurité. Quelques jours avant l'accident, les opérateurs ont transféré 42 tonnes de produit chimique dangereux dans un réservoir de stockage. Du fait d'une défaillance d'une valve, ce réservoir n'a pas été pressurisé à l'azote.	Retour d'expérience : l'accident de 1984 est la réplique d'un accident qui eut lieu quelques années auparavant. Les leçons de ce premier évènement n'ont pas été tirées. Audit : les forces d'audit et de contrôle, internes et externes, n'ont pas été en mesure d'infléchir les décisions relatives à la baisse de performance sécurité du process industriel. Formation du personnel : le personnel n'était pas suffisamment formé à la mise en œuvre des procédures opérationnelles. De plus, la baisse du personnel a été effectuée en contradiction des spécifications de mise en œuvre du process industriel, tel que la suppression de fonctions nécessaires. Intégrité mécanique : la fiabilité des équipements ne correspondait pas au minimum requis pour la sécurité.
Réalisation d'une opération de maintenance des conduites.	Plusieurs procédures et systèmes de sécurité ont été modifiés dans les semaines qui ont précédé l'accident : la fréquence de surveillance de l'état des	Analyse des risques : l'analyse des risques initiale ne couvrait pas l'ensemble des modifications réalisées par les opérateurs. Ces modifications ont largement

	réservoirs de stockage a été abaissée ; Arrêt du système de surveillance à distance, et absence de redondance dans la surveillance du système de pression. Tous ces changements ont été réalisés sans procédure de gestion des changements. Il n'existait aucune procédure d'urgence applicable en cas de surpression des réservoirs de stockage. Le niveau de maintenance des valves et conduites était faible. Lors du nettoyage des canalisations, aucun obturateur n'a été utilisé, contrairement aux procédures prévues. Des problèmes de communication entre le personnel ont eu lieu (registre partiellement rempli). Le personnel de management direct, ainsi que le responsable de la maintenance, étaient absents lors de la séquence accidentelle.	contribué au déroulement de la chaine accidentelle. De plus, les modalités de surveillance des réservoirs de stockage ont été modifiées la semaine précédant l'accident, accroissant le délai de détection en cas de situation anormale. <u>Règles et procédures :</u> les procédures opérationnelles définies lors de la conception du système ont été modifiées sans application d'une procédure de gestion des changements. <u>Préparation aux situations d'urgence :</u> les opérateurs n'ont pas été capables de détecter et reconnaitre les premiers signes de la situation accidentelle, et n'ont pas déclenché de réponse adaptée.
Rejet d'un nuage toxique jusqu'à la ville voisine.	Plusieurs barrières de sécurité ont été défaillantes, ou désactivées, et n'ont pas permis de stopper la séquence accidentelle (système de réfrigération, torche de brûlage, neutralisateur de gaz). Aucun opérateur n'a eu conscience de la réaction chimique non prévue en cours dans le réservoir de stockage. Aucune procédure d'urgence n'a été mise en œuvre. De plus, les équipes de secours internes n'étaient pas qualifiées et entrainées pour faire face à un scénario de rejet massif d'un nuage toxique. La procédure de transfert des gaz vers le neutralisateur de gaz en cas d'urgence n'était pas connue des opérateurs. Les opérateurs n'avaient pas connaissance de la présence d'un réservoir vide disponible pour le transfert et la mise en sécurité des produits chimiques dangereux. L'alerte de la population a été réalisée tardivement, à deux heures du matin, bien que la fuite ait été identifiée vers 23h45. La population ne connaissait pas la conduite à tenir face au déclenchement de la sirène d'alerte. Aucun plan d'évacuation de la population n'a été préparé. Les autorités n'ont pas été informées de l'arrivée d'un nuage sur la ville, et de son extrême	<u>Règles et procédures :</u> la suppression des barrières de sécurité prévue lors de la conception du système a largement augmenté le niveau de risque réel, et contribué au déroulement de la chaine accidentelle. <u>Formation du personnel :</u> le personnel n'était pas conscient du risque de réaction chimique imprévue et incontrôlée dans le réservoir de stockage. Les opérateurs n'ont pas été capables de détecter la présence d'une situation accidentelle, et donc de déclencher les mesures d'urgence. <u>Préparation aux situations d'urgence :</u> les procédures d'urgence n'étaient pas adaptées à l'occurrence d'un accident majeur, comme peut l'être le rejet d'un nuage toxique. Les conduites à tenir n'étaient connues ni du personnel interne à l'entreprise, ni des autorités. <u>Documentation sécurité :</u> les informations relatives à la dangerosité des produits utilisés dans l'entreprise étaient indisponibles. En conséquence, les secours médicaux ont été inefficaces face aux symptômes développés par la population.

	toxicité. L'effet à long terme du produit était inconnu des autorités. Les secours médicaux n'avaient pas connaissance de la conduite à tenir en cas d'exposition au composé toxique.	

L'accident de la plateforme Piper Alpha

La plateforme de production gazière Piper Alpha, installée en mer du Nord, explosa le 6 juillet 1988, faisant 167 morts, et engendrant une perte financière approchant les 3 milliards de dollars. A la suite d'une activité de maintenance, la remise en route dangereuse d'un équipement a créé une atmosphère explosive à bord de la plateforme. Non conçue pour résister aux explosions, les équipements de secours furent détruits, et ne purent empêcher le naufrage de la station dans les heures qui ont suivi.

1. Principales étapes accidentelles	2. Faits	3. Ecart entre le système de gestion de la sécurité et la réalité
Fonctionnement de la station de forage en mode dégradé.	En période estivale, le management est principalement composé de personnes promues à titre provisoire, en remplacement des titulaires, en congés. Le jour de l'accident, l'équipe postée était composée de cinq personnes, nombre minimum requis. La plateforme était configurée dans un mode « dégradé », qui exige de la part du personnel d'exploitation une compétence et une expérience supérieure à celle nécessaire pour conduire la plate-forme en mode normal. Les caractéristiques majeures de ce mode résident, entre autres, dans la différence de pression du gaz qui est très supérieure à celle du mode normal (environ 2,5 fois plus grande). Précédemment, des problèmes dans la gestion des permis de travail a conduit à un accident fatal. Cependant, aucune amélioration significative n'a été réalisée.	Analyse de risques : bien qu'en effectif réduit, le nombre de personnes présentes correspondaient au minimum requis. Bien que « dégradé », le mode de fonctionnement de la station était pris en charge par l'analyse de risques. Ces deux circonstances, indépendamment gérées par les modes de gestion de la sécurité, se sont superposées, créant ainsi des conditions défavorables. Retour d'expérience : un accident grave passé à déjà remis en cause l'efficacité de la gestion des risques sur la plateforme. Cet évènement aurait dû être le déclencheur d'un processus de retour d'expérience, afin de progresser dans la connaissance du système, et mettre en place des mesures afin d'éviter son renouvellement.
Défaillance de la première pompe.	Le comportement anormal d'une vanne conduit à une demande de maintenance. Lors de cette phase, plusieurs éléments ont contribué à la dynamique accidentelle : Les opérateurs réalisent la dépose de la pompe. Ils procèdent à l'obturation des deux conduites, sans effectuer de test d'étanchéité, et alors que la station est configurée en mode dégradé, au sein duquel le test est non obligatoire.	Analyse de risques : bien que non obligatoire, le test d'étanchéité était critique pour la sécurité, car constituait une barrière importante aux fuites de gaz. L'absence de ce test s'est ajoutée à un mode de fonctionnement du process où la pression en gaz est plus élevée que la normale, augmentant le risque de fuite. Ainsi, l'analyse de risques n'a pas pris en considération la superposition de facteurs accidentogènes lors de la définition des barrières de

	L'indisponibilité de la grue oblige les opérateurs à reporter le montage au lendemain. Bien que l'opérateur ait suivi la procédure de permis de travaux, aucune indication du problème n'a été remontée au management, qui n'a procédé à aucune revue indépendante du système. Ces lacunes dans la procédure de permis de travail avait déjà fait l'objet d'inquiétudes exprimées par un opérateur dans l'année précédente. La procédure de permis de travail était régulièrement non respectée (manque de signature, absence de revue indépendante avant la remise en service, absence de clôture du permis, pas d'échange en vis-à-vis sur le suivi des permis lors des changements d'équipe).	sécurité, comme par exemple le test d'étanchéité. Règles et procédures : existante, mais non respectée, la procédure de gestion des permis de travail ne remplissait pas sa fonction de sécurité, et notamment celle de s'assurer que l'ensemble des acteurs concernés sont informés des modifications réalisées sur le process.
Changement d'équipe, et défaillance de la seconde pompe.	Après le changement d'équipe, la défaillance de la seconde pompe à conduit à l'initiation de la chaine accidentelle. Plusieurs éléments ont contribués : Bien que le permis de travail ait été rempli, le changement de quart n'a pas fait l'objet de consigne particulière. La nouvelle équipe ne sait pas que la valve de sécurité de la pompe est démontée, et cette information n'a pas été inscrite sur le cahier de quart. Afin de palier à la défaillance de la seconde pompe, la première pompe est déconsignée, et remise sous tension par le rondier. Ce dernier ne peut pas s'apercevoir que la valve est démontée ; car elle se situe à un étage au-dessus de la pompe en mezzanine. Aussi l'opérateur de salle de contrôle la remet-il en service. Aucun ne sait que la valve de sécurité de la pompe A n'a pas été remontée, car les deux exemplaires du bon de travail relatif à la valve ont été retirés de la salle de contrôle et du bureau du responsable d'entretien. De plus, la mention de ce retrait n'a pas été inscrite sur le cahier de quart.	Communication : l'absence de communication, écrite et orale, sur l'état de la pompe à conduit à une interprétation faussée du manager du quart montant. Cette méconnaissance de la situation réelle a directement contribué à la chaine accidentelle. Règles et procédures : plusieurs règles, absentes ou en défauts, n'ont pas permis d'assurer la continuité d'information entre les deux équipes de quart. Ce fut le cas pour la gestion des bon de travaux, ou encore le contenu du cahier du quart. Ainsi, la situation comprise par le management de l'équipe montante ne correspondait pas à la réalité du process.
Explosion du nuage de gaz.	A l'origine conçue pour l'exploitation pétrolière, l'activité de la plateforme a été réorientée vers l'extraction de gaz. Le principal risque n'était plus l'incendie, mais l'explosion en cas de fuite. Le soir de l'accident, les protections pare-feu n'ont pas été efficaces face aux explosions de gaz. La salle de contrôle a été abandonnée moins de quatre minutes	Analyse de risques : La modification du process a été mise en œuvre sans modification des barrières de sécurité. En conséquence, le niveau de protection du process ne correspondait pas au niveau de risque réel.

	après la première explosion. Un système pare-feu de résistance minimale aux flammes et fumées étant de 15 minutes. Les principaux systèmes électriques ont été détruits lors de l'explosion, rendant inopérant la plupart des systèmes de sécurité. C'était par exemple le cas du système d'alerte par haut-parleur. Contrairement aux recommandations issues d'audit interne, les pompes d'incendie étaient configurées en mode « manuel », à cause de la présence de plongeurs au pied de la plateforme. Lors d'une vérification précédente, il avait été suggéré une procédure soit mise au point pour maintenir les pompes en mode automatique, comme c'était le cas sur d'autres plateformes, mais sans succès. Les têtes de sprinkler étaient corrodées et bouchées, réduisant l'efficacité du système d'extinction. Ce problème était connu depuis 1984. Plusieurs projets avaient été initiés pour résoudre ce problème, sans aboutir complètement. En mai 1988, un test a montré que 50 % des têtes de sprinkler étaient bouchées. Le module de formation aux procédures d'urgence était hâtif et non uniformément suivi. Une formation était nécessaire pour le personnel absent depuis plus de six mois de la plateforme. Cependant, les modules étaient souvent annulés si le personnel avait déjà travaillé à bord de la station. Plusieurs survivants ont indiqués qu'ils ne savaient pas où étaient situés les *lifeboats*, et n'avaient jamais été formés à leur utilisation. Les exercices d'évacuation n'étaient pas réalisés chaque semaine comme l'exigeait les procédures. 13 exercices ont été enregistrés sur une période de six mois. Aucun exercice d'évacuation globale de la plateforme n'a été réalisé dans les trois années précédentes. Les managers de la plateforme n'étaient pas formés aux conduites à tenir en cas d'urgence sur la plateforme, ou sur une plateforme voisine. Un an avant l'explosion, un audit interne a alerté le management sur les potentielles conséquences catastrophiques d'un feu de gaz sur l'évacuation du personnel. Cependant, le management a remis en	<u>Audit :</u> des audits avaient pointés des écarts entre les procédures prévues, et celles qui étaient mises en œuvre. Ces alertes n'ont pas été en mesure de déclencher des modifications relatives à la sécurité du process. <u>Formation du personnel :</u> contrairement aux exigences de formation, le personnel n'était pas suffisamment formé pour faire face aux situations d'urgence. Il existait un écart entre les compétences nécessaires pour intervenir sur une plateforme pétrolière, et les compétences réelles détenues par le personnel de la station. <u>Intégrité mécanique :</u> plusieurs équipements de sécurité n'ont pas été maintenus en état de fonctionnement au cours du temps. Le jour de l'accident, ils n'étaient pas en mesure d'assurer leur fonction de sécurité. <u>Préparation aux situations d'urgence :</u> le personnel de la plateforme n'était pas préparé à faire face à une situation d'urgence, comme le prévoyait le règlement.

	question la probabilité d'un tel évènement, en citant les moyens de protection existant.	

L'accident de Texas City

L'accident de Texas City eut lieu le 23 mars 2005, au sein de l'unité d'isomérisation de la raffinerie BP. A la suite d'une période de maintenance, le débordement de la tour d'isomérisation généra un nuage explosif. Celui-ci fut mis à feu par un véhicule stationné proche du site. 15 personnes furent tuées, et 180 furent blessées.

1. Principales étapes accidentelles	2. Faits	3. Ecart entre le système de gestion de la sécurité et la réalité
Placement des baraquements temporaires proche de l'unité d'isomérisation.	Le placement des baraquements proche de l'unité d'isomérisation est le résultat d'une sous-estimation des risques. Plusieurs causes ont contribué à ce résultat : La méthode « what if » utilisée pour réaliser l'analyse des risques était basée sur un référentiel et des critères de risques obsolètes. La procédure de gestion du changement n'a pas été correctement mise en œuvre. L'équipe chargée de réaliser cette procédure n'a pas été correctement formée à l'utilisation du référentiel BP.	Plusieurs problèmes ont conduit à sous-estimer le risque associé au positionnement des baraquements. Premièrement, l'hypothèse du taux d'occupation a été falsifiée. En effet, prévu pour une utilisation temporaire, les baraquements ont été utilisés de manière semi-permanente. Deuxièmement, la méthode utilisée pour réaliser l'analyse de risques n'a pas été correctement réalisé, à cause d'un manque de formation du personnel. Troisièmement, la procédure de gestion du changement a été appliquée à une partie des baraquements seulement.
Réalisation d'activités de maintenance, et de la procédure *Pre Start-up Safety Review* à l'unité d'isomérisation.	Avant chaque étape de démarrage, le référentiel de la raffinerie impose une revue de sécurité rigoureuse. La veille de l'accident : Cette procédure n'a pas été correctement mise en œuvre : le retrait du personnel n'a pas été vérifié, la revue de démarrage par les opérateurs et superviseurs n'a pas été réalisée. Durant la vérification des équipements techniques du process, plusieurs éléments ont été identifiés comme défaillants (indicateur de niveau, valve de pression) et n'ont pas été réparés.	La défaillance du processus de gestion des règles et procédures à conduit à l'inefficacité de la procédure *Pre Start-up Safety Review,* qui est critique pour contrôler le niveau de sécurité du process industriel. De plus, plusieurs équipements ont été identifiés comme défaillants, et n'ont pas été réparés, compromettant ainsi l'intégrité mécanique du process industriel.
Démarrage de l'unité d'isomérisation.	Lors du démarrage de l'unité : La procédure de démarrage a été réalisée sans supervision complète et efficace. Le personnel opérationnel était en sous-effectif, créant ainsi un niveau de fatigue élevé chez les opérateurs. La procédure de démarrage a été modifiée à plusieurs	Plusieurs processus de gestion de la sécurité ont été impliqués dans le déroulement de la séquence accidentelle : Retour d'expérience : plusieurs évènements similaires n'ont pas été analysés, manquant ainsi l'opportunité d'améliorer les connaissances relatives à la mise en

	reprises sans appliquer de procédure de gestion des changements, et sans tenir compte des incidents passés. Les pratiques opérationnelles ont été modifiées par les opérateurs les plus anciens afin de réduire les délais de démarrage. Cependant, ces pratiques n'ont jamais été remises en cause et confrontées aux procédures opérationnelles théoriques. Les écarts aux procédures étaient une pratique courante (des écarts constatés lors des 18 derniers démarrages d'unités identiques). Plusieurs défauts de communication ont eu lieu entre les membres du personnel (instructions manquantes, registre minimal et imprécis). Plusieurs défaillances techniques sont apparues : indicateur de niveau, et alarme de niveau haut défaillante, fenêtre de contrôle inutilisable. L'affichage du système de contrôle informatisé a fourni des données indirectes, ce qui a conduit à une erreur d'interprétation de l'opérateur à propos de l'évolution interne du process. Les opérateurs n'ont pas été correctement formés. Les scénarios utilisés pour la formation des opérateurs de conduite étaient incomplets. L'utilisation de salle de simulation a été écartée par la direction de l'entreprise, afin de réduire les coûts associés aux programmes de formation.	œuvre du process industriel. <u>Intégrité mécanique :</u> l'état des équipements était en dessous des minimums définis lors de la conception du process. Plusieurs équipements ont été défaillants. <u>Analyse des risques :</u> le système de contrôle automatisé ne permettait pas aux opérateurs d'avoir une information directe sur le niveau réel de matière dans la tour. Combiné avec d'autres facteurs (fatigue, surcharge de travail, sous-effectif), un écart a émergé entre la représentation de l'opérateur sur la situation, et la réalité. <u>Formation du personnel :</u> le programme de formation n'incluait pas toutes les situations possibles lors d'activités normales et anormales. Les personnels n'étaient pas correctement préparés à faire face à une situation accidentelle. <u>Règles et procédures</u> : les procédures de travail n'étaient plus à jour et adaptées à l'état réel et aux possibles évolutions du process industriel. La conception et la mise en œuvre des procédures ne permettait pas le maintien d'un haut niveau de sécurité (le management ne s'assurait pas de la bonne mise à jour des procédures, des instructions spécifiques nécessaires en cas de situation anormales étaient manquantes, les marges de sécurité opérationnelles n'étaient pas indiquées pour le niveau de remplissage de la tour).
Surremplissage de la tour et explosion du nuage de gaz.	Plusieurs facteurs ont conduit à la création et à la mise à feu d'une atmosphère explosive : La conception des barrières de sécurité n'étaient pas adaptées aux conditions opérationnelles actuelles (le réservoir de purge était sous-dimensionné, la conception du système d'urgence ne permettait pas la prise en compte d'une large libération de matière en cas de surremplissage de la tour, la tour n'était pas équipée d'un système d'arrêt automatique déclenché par un niveau de remplissage trop élevé). Plusieurs défaillances techniques ont eu lieu (indicateur de niveau de liquide, capteur de niveau bas et de niveau haut défaillants, fenêtre de	Plusieurs processus de gestion de la sécurité ont été impliqués l'explosion : <u>Analyse des risques :</u> l'augmentation du potentiel de danger du process n'a pas été prise en compte par une mise à jour de l'analyse des risques. Des équipements de sécurité étaient sous-dimensionnés ou manquants. Tous les scénarios accidentels crédibles n'ont pas été identifiés. <u>Intégrité mécanique</u> : plusieurs équipements de sécurité ont été défaillants, et n'ont pas permis d'identifier et de contenir la situation anormale. <u>Retour d'expérience :</u> plusieurs évènements similaires ont eu lieu dans le passé. Cependant, le système n'a

	niveau inutilisable). Le management n'a pas identifié tous les scénarios crédibles de surpression et de surremplissage de la tour. Dans les 15 années précédant l'accident, plusieurs propositions ont été faites pour remplacer le réservoir de purge, mais aucune n'a été réalisée. La source probable d'allumage de l'atmosphère explosive est un pick-up stationné à côté du réservoir de purge. La gestion des véhicules sur le site n'a pas permis de contrôle la présence des véhicules d'activités opérationnelles.	pas été capable de tirer des leçons de ces évènements afin d'améliorer le niveau de connaissance relatif à la sécurité du process industriel. Règles et procédures : la gestion des véhicules sur le site n'a pas été correctement appliquée, ajoutant une source potentielle de perturbation non prise en compte dans l'analyse de risques.

L'accident d'Institute

L'explosion de l'usine agro-pharmaceutique d'Institute, aux Etats-Unis, se déroula le 28 août 2008. Vers 22h30, le redémarrage non maitrisé d'une unité de production conduit à la rupture d'un réservoir de traitement. Les vapeurs inflammables explosent immédiatement, conduisant à la destruction d'une partie de l'unité de production. Deux personnes sont tuées, et huit sont blessées. Des maisons, entreprises et véhicules sont endommagés par l'effet de pression qui entraîne des dégâts structurels mineurs et des bris de vitre jusqu'à 2,5 km du centre de l'explosion.

1. Principales étapes accidentelles	2. Faits	3. Ecart entre le système de gestion de la sécurité et la réalité
Modification de l'unité de production.	Plusieurs facteurs relatifs à la modification du process et de sa mise en œuvre ont contribué à l'accident : Entre 2004 et 2007, l'organisation des activités de production a été restructurée. Cette réorganisation a eu pour conséquence de diminuer fortement la disponibilité du personnel d'assistance technique, et notamment lors des phases critiques de démarrage. Les jours précédant l'accident, l'unique conseiller technique avait travaillé 15 à 17 heures par jour et 10 heures d'affilée la veille de l'accident. Cette réorganisation a également eu pour conséquence de remplacer le mode de gestion hiérarchique par une autogestion des équipes de productions. L'unité de contrôle à fait l'objet d'un changement de système de commande du process. Ce nouveau système, plus complexe, et basé sur une représentation différente du process, n'était pas connu des opérateurs. Ce nouveau système de commande du process a été implémenté sans formation adéquate des opérateurs. Le projet de révision du système de commande du process n'a fait l'objet d'aucune revue de sécurité avant redémarrage. En août 1993, un accident similaire eut lieu au sein su même site. Les recommandations, portant sur l'amélioration de la surveillance de l'utilisation des organes de sécurité, n'ont pas été suivies d'effets.	Analyse des risques : les conditions de mise en œuvre de l'analyse des risques (délai, composition de l'équipe, outils utilisés) n'étaient pas adaptées aux caractéristiques du process étudié. En conséquence, elle n'a pas réussi à identifier le scénario du jour de l'évènement. Gestion du changement : l'implémentation d'un nouveau système de commande pour un démarrage, sans dispositif particulier de surveillance de la transition, a conduit à brouiller la représentation des opérateurs, qui ont alors perdu le contrôle du process. Audit : avec une nouvelle organisation à base d'équipes autogérées, la direction ne pouvait, ni conseiller, ni contrôler directement les étapes du redémarrage de l'unité. De fait, son éloignement de l'exploitation lui a fait ignorer que les opérateurs suivaient rarement certaines procédures d'exploitation et que certains court-circuitaient des dispositifs critiques de sécurité. Formation du personnel : le personnel n'a pas acquis les compétences nécessaires pour la conduite du process, après remplacement de l'interface de contrôle. Retour d'expérience : l'occurrence d'un même évènement dans le passé n'a pas permis d'améliorer la conception du process, et donc le niveau de sécurité du système.

Redémarrage de l'unité.	Devant la demande grandissante de produits, l'unité doit être redémarrée au plus vite. Plusieurs composants du process ont été remplacés. Pourtant, ils n'ont pas fait l'objet d'une revue de sécurité adéquate. De plus, cette procédure de sécurité était réalisée sans impliquer directement les opérateurs et les spécialistes concernés. Le nouveau système de commande du process constituait un challenger pour les opérateurs, insuffisamment formés. Ce système était par ailleurs calibré différemment (temps de réponse du système modifié, unités de mesure des solvants en gallons et non en % de volume total…), pour faire fonctionner le process dans les meilleures conditions. De nombreux problèmes liés au matériel empêchent le personnel de surveiller le réservoir de traitement. Ceux-ci oublient de le remplir avec du solvant propre. De plus, à l'encontre des procédures écrites, mais avec l'accord de l'agent de maîtrise (il s'agit d'une pratique courante sur le réservoir et son système de chauffage), les opérateurs décident de contourner le dispositif de sécurité en entrant un mot de passe sur le nouveau système informatique. Des analyses du contenu du réservoir ne sont pas réalisées en début de démarrage. Face au grand nombre de difficultés techniques, le statut du réservoir n'est pas noté lors du changement d'équipe, aussi bien par oral que sur le carnet de bord. Lors du déclenchement de l'alarme de pression haute du réservoir, L'opérateur en salle de contrôle croit, à tort, que l'augmentation de la pression résulte du colmatage du tuyau d'évacuation, phénomène qui s'est déjà produit plusieurs fois auparavant.	Gestion du changement : la modification du process, sans prise en compte des acteurs principalement concernés, et la mauvaise calibration du système de commande a placé le système dans des conditions de fonctionnement propices à l'accident. Règles et procédures : plusieurs manquements aux règles d'exploitations, et procédures de travail, ont contribué au déclenchement de l'accident, mais n'ont également pas permis de détecter la dynamique accidentelle en cours. Intégrité mécanique : plusieurs composants défaillants n'ont pas assurés leur fonction de sécurité. Ils ont également focalisé l'attention des opérateurs, ce qui a empêché la détection de la dynamique accidentelle. Communication : l'absence de communication entre les deux équipes sur un aspect critique du process a généré une rupture dans la transmission d'information.
Explosion du réservoir.	A 22h33, la réaction s'est emballée et n'est plus maitrisable. Les clapets de décharge du réservoir s'ouvrent, puis se rompent brutalement, entrainant la destruction d'une partie de l'unité. Plus de 8 m^3 de substances inflammables et toxiques se déversent sur le sol et dans l'unité ; les vapeurs inflammables s'enflamment aussitôt au contact d'étincelles	Préparation aux situations d'urgence : contrairement aux dispositifs locaux d'urgence préétablis, les délais dans la transmission d'information à réduit l'efficacité des secours.

	produites par des câbles électriques. La communication d'informations vis-à-vis des différents acteurs et notamment des autorités locales a été défaillante : manque d'information sur les origines et la gravité de l'explosion, sur les besoins en moyens de secours, et sur l'existence d'un possible nuage toxique, et la nécessité de confiner les riverains.	

L'accident de Deepwater Horizon

La plateforme Deepwater horizon fit naufrage le 20 avril 2010, à 80 kilomètres au large des côtes américaines. Lors d'une phase d'exploration pétrolière, une remontée incontrôlée de pétrole à travers la conduite de forage a créé une atmosphère explosive à bord de la plateforme. L'explosion, probablement causée par les pots d'échappement, n'a pu être évitée. 11 personnes ont été tuées, et 16 autres blessées. L'intensité de l'explosion à cause l'incendie de la plateforme, puis son naufrage le lendemain. Sans contrôle, le forage a engendré l'une des plus grandes pollutions maritimes de l'histoire des Etats-Unis.

1. Principales étapes accidentelles	**2. Faits**	**3. Ecart entre le système de gestion de la sécurité et la réalité**
L'intégrité du puit n'est pas établie, ou a été perdue.	Selon le rapport d'accident, plusieurs facteurs sont à l'origine de la perte de contrôle du puit : Les modèles numériques utilisés pour concevoir le puit ont été basés sur des hypothèses techniques incorrectes, relatives à la pression de l'hydrocarbure, aux centralisateurs, à la densité des boues de forage. Le cimentage du puit a été réalisé avec plusieurs changements, en contradiction avec les bonnes pratiques industrielles (changement sur le process de cimentage, et des équipements utilisés). Le cimentage a été réalisé sans certains équipements critiques pour la sécurité (capteur de flux).	Analyse des risques : les hypothèses pris en compte pour la modélisation de l'analyse des risques ne correspondaient pas à la réalité de la configuration géologique du puit. De plus, plusieurs équipements critiques pour la sécurité n'ont pas été utilisés, rendant la détection d'une situation accidentelle difficile pour les opérateurs. Communication : plusieurs problèmes de communication ont eu lieu entre les différentes entreprises impliquées dans le forage, générant ainsi un écart entre les représentations de chacun, et la réalité de la situation de terrain.
La remontée de pétrole dans le puit n'est pas détectée, et le contrôle du puit est perdu.	Plusieurs facteurs sont potentiellement à l'origine de la perte de contrôle du puit : Plusieurs évènements similaires liés au contrôle du puit (détection tardive de remontée d'hydrocarbure) ont eu lieu dans les jours précédant l'accident, mais aucun retour d'expérience n'a été réalisé. Le matériel utilisé pour fermer le puit a été modifié, en contradiction avec la procédure. Cela a conduit à une mauvaise interprétation des tests par les opérateurs, qui par ailleurs n'étaient pas correctement formés aux situations particulièrement ambiguës. Lors de la phase finale du forage, la remontée d'hydrocarbure a été masquée par une conjonction de	Analyse des risques : l'analyse des risques théorique ne prenait pas en compte la réalisation simultanée d'activités multiples, et critiques pour le contrôle du puit. Ces activités simultanées ont généré un écart entre l'analyse des risques initiale, et la réalité de la situation. Règles et procédures : Plusieurs barrières de sécurité ont été déconnectées, contrairement aux spécifications énoncées lors de la conception du système. De plus, les procédures de réalisation des tests de pression étaient imprécises, ou manquantes. Ce défaut a conduit à une mauvaise interprétation de l'opérateur sur la situation réelle dans le puit.

	plusieurs activités. Les tests critiques pour la sécurité ont été mis en œuvre sans procédure précise, et réalisés simultanément à d'autres activités à bord (transbordement de boue de forage). Déconnectées, les barrières de sécurité n'ont pas joué leur rôle d'alerte (court-circuit du capteur de flux, alarme générale en mode «inhibé », et le système de découplage d'urgence de la plateforme n'était pas programmé pour se déclencher automatiquement en cas de détection d'une atmosphère explosive). L'équipage n'a pas été capable d'identifier l'origine et la gravité du problème associé au puit. La décision d'utiliser le séparateur de boue afin de contenir le pétrole a conduit à la création d'une atmosphère explosive.	Retour d'expérience : plusieurs retours d'expérience n'ont pas été réalisés, manquant ainsi l'opportunité d'améliorer les connaissances des opérateurs sur le comportement du puit et des installations de forage. Préparation aux situations d'urgence : les opérateurs ont eu des difficultés à déclencher les mesures d'urgence, et à les mettre en œuvre. Ils n'étaient pas prêts à affronter une situation de remontée de pétrole telle qu'elle fut le jour de l'accident.
Mise à feu de l'atmosphère explosive sur la station.	L'utilisation du séparateur de boue a généré une atmosphère explosive. Celle-ci a été très probablement mise à feu par les pots d'échappement de la station. Plusieurs facteurs ont contribués à cette explosion : L'arrivée d'air nécessaire à la salle des moteurs était située proche de la structure de forage. Cette salle n'était pas classifiée comme une atmosphère potentiellement explosive. La séquence d'arrêt d'urgence n'a pas été initiée à causes de plusieurs défaillances : l'arrêt automatique des moteurs en cas de surrégime n'a pas fonctionné. La procédure « stop work » n'a pas été mise en œuvre, malgré la réception de 20 alarmes indiquant une concentration élevée de gaz explosif. Le management ne s'est pas assuré que tous les systèmes d'urgence (arrêt automatique des moteurs par exemple) n'ont pas été réellement testés.	Analyse des risques : les modèles d'analyse des risques utilisés ne couvraient pas le scénario accidentel du jour de l'accident (importance de la classification en atmosphère explosive, rôle des pots d'échappement). Règles et procédures : des procédures spécifiques doivent être mises en œuvre en cas d'urgence, ou de doute sur l'occurrence d'un évènement critique concernant le puit de forage. Malgré un nombre élevé d'alertes, ces procédures n'ont pas été réalisées.
Le *Blow-Out Preventer* n'a pas réussi à sceller le puit.	Plusieurs facteurs ont contribué à la défaillance du *Blow-Out Preventer :* Le mode automatique de déclenchement a été défaillant.	Analyse des risques : les systèmes d'urgence n'étaient pas conçus pour faire face à la configuration particulière du puit, telle qu'elle fut lors de l'accident. Intégrité mécanique : des équipements d'urgence ont été défaillants. Ils n'ont pas su jouer leur rôle de mise

	Le mode manuel s'est correctement activé, mais la configuration du puit, associés aux conditions de forte pression, a déplacé la conduite. En conséquence, l'action du BOP a été inefficace.	en sécurité du process au moment le plus critique.

Annexe n°2 : Typologie des causes issue de l'analyse d'accidents industriels majeurs

Chaque accident est unique. Il est unique parce que les faits accidentels ne sont jamais identiques. Il est le fruit de multiples facteurs : défaillances techniques, comportements humains inadaptés, facteurs organisationnels accidentogènes, ou encore instabilités issues de l'environnement. Pourtant, si chaque accident possède sa propre histoire, notre analyse historique identifie au moins 12 grandes familles. La Figure n°4 décrit cette typologie de causes.

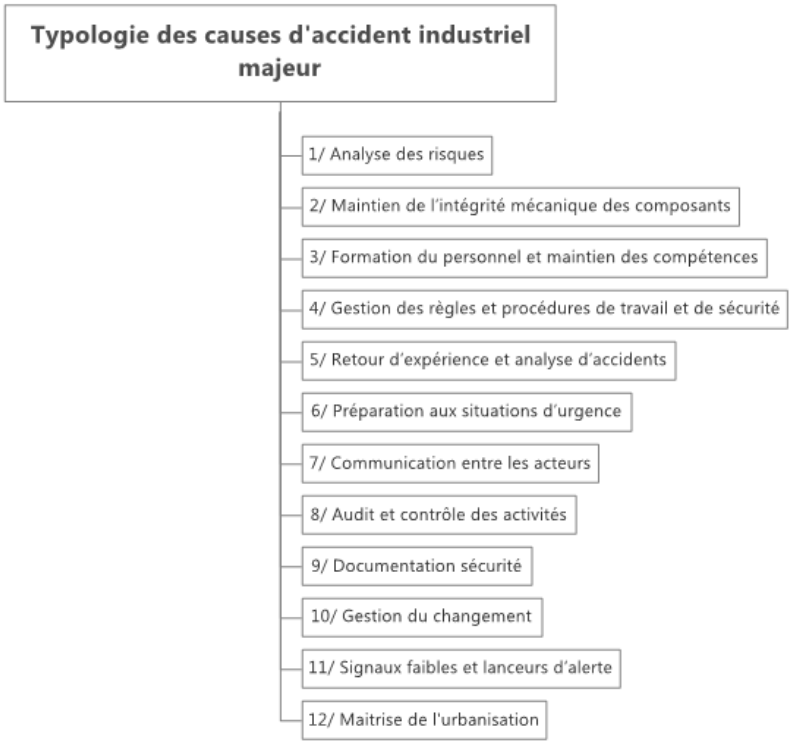


Figure 39 : Familles de causes des accidents industriels majeurs

La description de la typologie est présentée de la manière suivante. Chaque type regroupe sous une même appellation les causes de nature similaires. Les regroupements sont thématiques. Chaque type est abordé dans les pages suivantes.

1/ L'analyse des risques :

Les causes liées à l'analyse des risques comprennent la manière dont l'étude a été réalisée, c'est-à-dire sa méthodologie et ses résultats, ses conditions de mise à jour, ainsi que les circonstances dans lesquelles l'analyse des risques a été réalisée. Plusieurs points intéressants ont été soulevés :

- *Les circonstances de réalisation de l'étude :* les délais alloués à la réalisation de l'analyse de risques sont trop courts, l'équipe chargée de l'analyse n'est pas compétente.
- *Les outils d'analyse utilisés :* le modèle d'analyse n'est pas adapté au type de process industriel mis en œuvre, les hypothèses de travail sont erronées, ou ne correspondent pas à la réalité, les critères de risques sont obsolètes.
- *Le choix des scénarios d'accident retenus :* certains scénarios ne sont pas pris en compte, les scénarios ne prennent pas en compte des activités multiples simultanées, ou la conjonction de plusieurs facteurs accidentogènes.
- *L'évaluation des risques :* l'évaluation est sous-estimée, elle ne couvre qu'une partie du process. Des sources de danger proches du site ne sont pas prises en compte.
- *La conception des barrières de sécurité :* les barrières sont sous-dimensionnées ou manquantes, elles ne sont pas conçues pour faire face à des situations accidentelles, l'ergonomie n'est pas prise en compte, générant des difficultés de manipulation des produits.
- *La mise à jour de l'analyse des risques :* le process est modifié sans mise à jour de l'analyse des risques et des barrières de sécurité, la mise à jour régulière n'est pas réalisée, les modalités de surveillance du process sont modifiées, sans prise en compte dans l'analyse de risques.

2/ Le maintien de l'intégrité mécanique des composants :

Ce type de causes renvoi à l'incapacité d'éviter une défaillance d'un composant technique. Indirectement, c'est la manière de préparer et de mettre en œuvre le programme de maintenance qui est mis en cause.

- *La programmation de la maintenance :* le programme de maintenance est sous-dimensionné, il ne possède pas les ressources nécessaires, il n'est pas mis en œuvre.

- *La maintenance préventive :* les équipements ne sont pas entretenus, ils n'assurent pas leurs fonctions, ou ne sont pas en mesure de mettre le système en sécurité en cas de situation anormale.
- *La maintenance curative :* des équipements identifiés comme défaillants ne sont pas réparés ou remplacés.

3/ La formation du personnel et le maintien des compétences :

Cette thématique regroupe les cas où le personnel n'a pas été en mesure de réagir à une perte de maitrise de la situation. Deux aspects sont mis en exergue :

- *La préparation du programme de formation :* le programme de formation est sous-dimensionné, il est incomplet, il n'est pas mené à son terme, il n'est pas remis à jour après une évolution de process industriel.
- *Les compétences du personnel :* les opérateurs n'appliquent pas les procédures, ils méconnaissent les risques associés au process industriel, leur niveau de compétence est en dessous des prérequis attendus.

4/ La gestion des règles et procédures de travail et de sécurité :

Les problèmes liés à l'application des règles et procédures sont une des causes les plus largement partagées dans les cas étudiés. Leur conception, leur mise en œuvre, et leur évolution sont pointées du doigt :

- *La conception des procédures :* Les procédures sont inexistantes, imprécises, manquantes, elles ne sont pas adaptées à l'état réel du process industriel.
- *La mise en œuvre des procédures :* les procédures ne sont pas mises en œuvre, ou de manière non adéquate, ou partielle.
- *L'évolution des procédures :* les procédures ne sont pas mises à jour. Les procédures sont modifiées par les opérateurs sans processus d'analyse de risques et de gestion du changement.

5/ Le retour d'expérience et l'analyse d'accidents :

Les problèmes liés au retour d'expérience peuvent être décrits au regard de deux aspects. Le premier concerne le fait de déclencher un processus de retour d'expérience après l'occurrence d'un évènement. Le second aspect s'intéresse aux conséquences d'une analyse accidentelle sur les pratiques de sécurité.

- *La réalisation d'un retour d'expérience :* aucun processus de retour d'expérience n'est réalisé à la suite d'un accident externe, ou interne à l'entreprise, sur un processus accidentel similaire. L'absence d'évènement marquant lié au même type de process génère une sous-estimation du risque. Plusieurs évènements similaires avant l'accident mais sans conséquence ne conduisent à aucun processus de retour d'expérience.
- *La modification des règles de sécurité :* les processus de retour d'expérience restent sans effet et ne déclenchent pas d'évolution des règles de travail.

6/ La préparation aux situations d'urgence :

La préparation aux situations d'urgence est un élément critique de la récupération de situations accidentelles. Plusieurs causes d'inefficacité ont été identifiées :

- *La préparation des mesures d'urgence :* les procédures d'urgence sont inexistantes. Elles ne sont pas adaptées à l'état du process. Elles ne sont pas adaptées à l'occurrence d'un accident majeur.
- *La préparation du personnel :* Absence d'essais ou d'exercices de mise en situation. La conduite à tenir en cas d'accident est inconnue des opérateurs et des autorités.
- *La détection de la dynamique accidentelle et la mise en œuvre des mesures d'urgence :* l'activation d'une chaine accidentelle n'est pas détectée. La mise en œuvre des mesures d'urgence et la transmission des informations aux autorités sont réalisées avec des délais importants, qui réduisent d'autant leur efficacité.

7/ La communication entre les acteurs :

Les causes liées à la communication portent sur deux types de canaux : les canaux de communication entre des acteurs internes à l'entreprise, et la communication entre plusieurs acteurs indépendants travaillant sur le même site.

- *Canaux de communication internes :* Le manque de communication, orale ou écrite, pendant les changements d'équipe créent des ruptures de transmission d'informations critiques pour la sécurité du process.
- *Canaux de communication entre plusieurs acteurs indépendants :* la multiplication du nombre de parties prenantes dans le process industriel (experts, sous-traitants, managers, opérateurs...) génèrent des difficultés de transmission des informations (multiplication des flux, sélection des informations en fonction de la qualité de l'interlocuteur...).

8/ L'audit et contrôle des activités :

La mise en avant des audits et contrôle dans l'occurence d'un accident tient à deux éléments principaux. Le premier concerne la prise en compte des audits, qu'ils soient internes ou externalisés. La mise en lumière d'écarts entre le référentiel et la réalité aurait dû conduire à une modification des pratiques. Le second point concerne le contrôle des activités prescrites.

- *L'audit des activités :* Des écarts aux procédures détectés lors d'audits ne sont pas corrigés. Les alertes sur le niveau élevé de risque et les mauvaises conditions de mise en œuvre du process ne sont pas suivies de remise en cause de la gestion de la sécurité. Les recommandations issues d'audit internes et externe ne sont pas suivies d'effets.
- *Le contrôle des activités :* la réorganisation du travail, conduisant à une autogestion des équipes et à un éloignement du management, empêche le contrôle de la bonne réalisation des activités de travail par la direction.

9/ La documentation sécurité :

L'élément principal soulevé par cette famille de causes est celui de la disponibilité des informations liées à la sécurité, telles que les procédures à mettre en œuvre, ou encore les informations relatives à la dangerosité des produits.

- *La disponibilité des informations sécurité :* L'étiquetage des produits chimiques dangereux est imprécis ou manquant. Les informations relatives à la dangerosité ou au niveau de risques sont inexistantes, indisponibles, ou non communiquées aux acteurs concernés.

10/ La gestion du changement :

Les causes liées à la gestion des changements apparaissent à de nombreuses reprises. Au sein de l'entreprise, des changements relatifs au process et aux méthodes de travail sont mis en œuvre, sans prendre en compte leurs impacts sur le niveau de sécurité du système.

- *La modification du process industriel :* des modifications sont apportées au process industriels, sans prendre en compte l'avis des acteurs directement concernés. Aucune remise en cause de l'analyse des risques n'est effectuée à la suite de ces changements. Ces changements sont réalisés sans dispositif particulier de surveillance de la mise en œuvre du nouveau système. Aucun test ou essai n'est réalisé à la suite des changements afin de s'assurer de l'efficacité des barrières de sécurité.

11/ Les signaux faibles et lanceurs d'alerte :

La question des signaux faibles et des lanceurs d'alerte n'apparait pas directement dans la majorité des rapports d'accidents. Pour autant, la majorité des rapports font état de signaux non pris en compte.

- *La prise en compte des signaux de risques :* les lanceurs d'alerte ne sont pas entendus par leur hiérarchie. Les modifications demandées par les opérateurs pour sécuriser le process industriel restent sans réponses.

12/ La maitrise de l'urbanisation :

La maitrise de l'urbanisation réfère à la présence de cibles vulnérables à proximité de process industriels. Celle-ci fait état de la population installée en périphérie de zones industrielles, mais également d'autres sites à hauts risques, exposant la zone à des accidents en séries.

- *La proximité de cibles vulnérables :* Le site industriel est implanté à proximité d'une zone d'habitations. Il est situé proche d'autres sites industriels à hauts-risques.

Il est important d'indiquer ici que cette typologie ne peut pas être exhaustive. En effet, elle résulte de deux analyses consécutives. La première est celle des enquêteurs, qui ont mené les investigations post-accidentelles. Elle s'appuie sur des modélisations contemporaines de l'accident. Il existe donc une variabilité liée à la date d'occurrence de l'évènement. A titre d'exemple, les premiers rapports d'accidents ne prenaient pas en compte les facteurs organisationnels de l'accident. Ceux-ci sont apparus vers la fin du XX^{ème} siècle. La création de

connaissances nouvelles en matière de retour d'expérience conduira à prendre en compte de nouveaux facteurs d'accidents, inconnus jusque-là. La seconde analyse est le regroupement thématique en douze familles. Et cette seconde analyse est intéressante dans la mesure où elle nous permet de constater l'importance du rôle du management dans l'obtention de résultats sécurité : gestion des formations, préparation des plans de maintenance, prise en compte des signaux faibles... sont autant de problématiques qui relèvent avant tout du management, parce qu'elles croisent acteurs, ressources, objectifs, dans un but de planification efficace.

Guillaume DELATOUR

Doctorat : Développement Durable

Année 2015

L'écosystème décisionnel du manager : une contribution au défi d'anticipation de la crise

L'accident industriel majeur compte parmi les crises les plus destructrices et insupportables. Dans de nombreux cas, les retours d'expérience constatent que la catastrophe aurait probablement pu être évitée. La problématique posée est alors celle de l'anticipation. Au sein de systèmes sociotechniques à hauts risques, quelles sont les voies à suivre pour devancer le déclenchement d'une séquence accidentelle ?

Pour répondre à cette problématique, notre approche s'est focalisée sur la prise de décision. Placé dans un environnement contraignant, le manager opérationnel constitue un acteur particulier. Une analyse historique réalisée sur des accidents majeurs montre un décalage entre la vision qu'a le manager du système, et la réalité des opérations. Celui-ci se trouve en situation d'ambigüité, car il doit assurer le compromis entre la rupture demandée par l'obligation de sécurité, et l'absence de rupture imposée par la continuité d'activités. Les défis de la complexité, du temps, et de la décision alors dégradent peu à peu l'environnement décisionnel, et bloquent la prise de décision.

La thèse soutenue s'intéresse à comprendre la manière dont l'environnement influe sur sa prise de décision, dans le but de permettre au manager de passer d'une situation contrainte à une situation d'initiative. En décidant un arrêt momentané et préparé, sans rupture subie, il renforce ainsi la capacité d'anticipation des accidents industriels majeurs. Ainsi, en comprenant son écosystème décisionnel, le manager opérationnel peut donc prendre des initiatives assurant le principe de continuité d'activités.

Mots clés : risques industriels - prise de décision - accidents, prévention - gestion du risque.

Decision Ecosystem of Manager: A Contribution to the Challenge of Crisis Anticipation

Industrial accident is one of the most destructive and unbearable crisis. In many cases, experience feedbacks show that the disaster could probably have been avoided. In this context, we come up the question of anticipation. In socio-technological systems with high-risk technology, what are the pathways to detect and prevent an accident sequence?

To address this problem, our approach is based on decision making. Placed in a restrictive environment, operational management is a particular actor. A historical analysis of major accidents shows a gap between the vision of the manager, and the reality of operations. The manager is placed in a situation of ambiguity, in which he has to ensure the balance between the rupture requested by the safety requirement, and the absence of rupture imposed by the continuity of activities. Then, the challenges of complexity, time, and decision gradually degrade the decision-making environment and block the decision.

Our thesis proposes an understanding and a modelisation of the decision ecosystem of the operational manager, in order to pass from a stressed situation to a situation where the decision becomes initiative. By make the decision of a prepared interruption, the manager strengths his anticipation capacity of major industrial accidents. By understanding its decision ecosystem operational manager can take initiatives that protect the continuity principle.

Keywords: accidents, prevention - decision making – risk management.

Thèse réalisée en partenariat entre :

Grand Troyes Communauté d'Agglomération — Groupe ESC Troyes en Champagne "mixer les cultures, ouvrir les futurs" — INERIS "maîtriser le risque pour un développement durable" — utt université de technologie Troyes

Ecole Doctorale "Sciences et Technologies"