

► DIRECTION DES ETUDES ECONOMIQUES ET DE L'EVALUATION
ENVIRONNEMENTALE

► DOCUMENT DE TRAVAIL

LA CULTURE DU RISQUE ET DE LA SÛRETÉ

Patrick MOMAL

Série Méthodes

N° 03-M03



Site internet : <http://www.environnement.gouv.fr>

20 avenue de Ségur - 75302 Paris 07 SP

► RÉSUMÉ

Culture du risque et de la sûreté Patrick MOMAL

La notion de culture du risque est de plus en plus employée, par toutes sortes d'intervenants. Nous cherchons ici à réunir suffisamment d'éclairages et de documents pour que le lecteur termine cet ouvrage avec une idée claire de cette notion, qui reste trop souvent trop vague, et avec une vue renouvelée des questions de risques. C'est une notion vaste que nous envisageons ici dans le contexte des entreprises à risques : il s'agit de culture du risque et de la sûreté¹, ce qui couvre un champ étendu.

C'est ainsi qu'au fil des chapitres apparaissent : l'industrie nucléaire, l'aviation civile, les inondations, le contrôle des risques en entreprise, la culture de sûreté dans les laboratoires des universités américaines... D'autres secteurs auraient sans doute mérité d'être traités, comme la sécurité sanitaire, avec le contrôle très performant de la fabrication et de l'utilisation des médicaments, ou le contrôle déficient des résistances aux antibiotiques, résistances développées en grande partie en dehors du monde médical (antibiotiques utilisés inconsidérément dans les élevages ou dans les produits de ménage).

Comme la culture du risque et de la sûreté se décline en tous les lieux liés aux risques, on aborde aussi bien la culture des élites d'entreprise, que l'émergence de règles de gouvernance sur les risques, ou le rôle des différentes stratégies des autorités de contrôle.

Il s'agit en partie d'une collection de documents — l'introduction permettra au lecteur sélectif d'y faire son choix. Une thèse se dégage pourtant : une bonne gestion des risques est une question d'intelligence, c'est-à-dire qu'elle dépend d'une orientation volontariste vers toujours plus d'intelligence, de compréhension des risques. A cet égard, on peut se donner quelques repères :

- Le recours à la procédure dans les établissements à risques doit éviter d'être dogmatique : elle risquerait alors de réduire l'opérateur au rôle d'exécutant peu intelligent. Or, l'opérateur peu intelligent est une source avérée de catastrophes (incident nucléaire de Tokaï Mura, mais aussi de Tchernobyl et de nombreux autres désastres²). Mais on sait aussi que la procédure est un des fondements de la qualité (« dire ce que l'on fait et faire ce que l'on dit »). La solution consiste probablement à s'orienter, avec prudence, vers le modèle de l'organisation apprenante.

¹ On pourrait aussi s'intéresser à la culture du risque dans le public en général, avec les problèmes du tabagisme, de l'alcool, des prises de risques dans le sport, des attitudes parfois inconsidérées de la jeunesse, etc. On pourrait également envisager les aspects sanitaires de la culture du risque. Ou encore la culture du risque dans les entreprises en général, avec des réactions souvent insuffisantes à l'espionnage industriel.

² Voir, par exemple, *Les décisions absurdes*, de Christian Morel.

- Du côté de l'autorité de contrôle, on rencontre des dilemmes similaires. Contrôler par la norme est une solution relativement efficace, car les taux d'émissions et autres dispositifs de sûreté sont beaucoup plus facilement vérifiables que l'intelligence des opérateurs et du système de sûreté ! Mais nombreux sont les observateurs qui estiment que l'on est arrivé au bout de l'efficacité de ce type de contrôle. « Trop de norme tue la norme » entend-on ainsi. Et plus généralement, comme la procédure, la norme n'incite pas à l'intelligence : « Je suis dans les normes, le reste, je ne veux pas le savoir... » Elle n'incite pas à la responsabilisation, au contraire. Mais si l'on veut contrôler indirectement par l'intermédiaire d'un système de gestion des risques rendu obligatoire (comme dans l'aviation), encore faut-il disposer de contrôleurs et de méthodes de contrôle efficaces...

Ce document n'engage que ses auteurs et non les institutions auxquelles ils appartiennent. L'objet de cette diffusion est de stimuler le débat et d'appeler des commentaires et des critiques.

► SOMMAIRE

INTRODUCTION	7
I - CULTURE DU RISQUE ET CULTURE DE SÛRETÉ : DE QUOI PARLE-T-ON ?	15
1. Naissance du concept de culture de sûreté	18
2. L'exemple des laboratoires des universités américaines	26
3. Discussion de la notion de culture de sûreté	30
4. Importance et mesure de la culture du risque	36
5. Culture du risque et culture de sûreté	42
6. Exemple de défaut de culture du risque	48
II - INTELLIGENCE DU RISQUE	53
7. L'évolution des concepts de la sûreté	55
8. La notion d'intelligence du risque	61
9. Intelligence du risque dans l'aviation civile	65
10. Intelligence du risque et inondations	71
III - GOUVERNANCE D'ENTREPRISE	73
11. Intelligence du risque et gouvernance d'entreprise	77
12. La sûreté occupe une faible place au sein des risques de l'entreprise	85
13. Le risque n'est pas une affaire de spécialistes, mais l'objet de la vigilance de tous	87
14. Gouvernance et culture des élites : la crise de gouvernance aux États Unis	89
15. Objectifs de sûreté et objectifs de coût	101
16. La sûreté peut-elle être gérée de loin par objectifs financiers ?	105
17. Mondialisation et risque de moralité	117
IV - GÉRER LES RISQUES, CULTIVER LA SÛRETÉ	119
18. Analyse des risques et prise de décision	121
19. Gestion des risques et management de la qualité	131
20. La sûreté en termes économiques	135
21. Les systèmes de gestion de la sûreté en France	145
22. Le style d'intervention de l'administration	149
23. Résistances à la formation et au retour d'expérience	153
24. Les inspections sont-elles efficaces ?	157
ANNEXE 1 : Rapport du groupe consultatif international pour la sûreté nucléaire	161
ANNEXE 2 : Activité de la PME Dédale dans le domaine de la culture de sûreté	185
ANNEXE 3 : Le projet SCORE	197
ANNEXE 4 : Synthèse de « Prévention du risque de dommages liés aux inondations »	207
ANNEXE 5 : Le rapport Turnbull	213
ANNEXE 6 : « Plutôt prévenir que guérir » de Carey et Turnbull	227
ANNEXE 7 : Implementing Turnbull, Risks	233
ANNEXE 8 : Implementing Turnbull, Embedding the Process	241
ANNEXE 9 : Time magazine " Chainsaw AI Gets The Chop"	247
ANNEXE 10 : Articles de presse sur Toyota	253
ANNEXE 11 : Inspections et défaillances critiques	259

INTRODUCTION

I - Culture du risque et culture de sûreté : de quoi parle-t-on ?

Pourquoi les techniques du risque et de la sûreté, pourtant parfois simples et peu onéreuses, sont-elles souvent ignorées ou mal appliquées ? Les notions de culture du risque et culture de sûreté éclairent des facteurs situés en amont des techniques. Elles permettent d'examiner les façons d'aborder le risque, en général et avant toute approche technique. Ces façons d'aborder le risque peuvent influencer de façon cruciale sur l'adoption, ou non, de certaines techniques et sur l'application judicieuse, ou non, d'autres techniques.

La première partie de ce document est construite autour des définitions de la culture du risque et de la culture de sûreté. Elle aide à préciser l'origine de ces définitions et les débats qui les entourent. En outre, elle propose des exemples réels assez nombreux, car il ne s'agit pas de définir pour le plaisir des mots. Les définitions servent, en effet, à fixer une orientation du regard vers la réalité du risque. Elles aident à répondre à l'interrogation ci-dessus.

L'idée de culture de sûreté vient du terrain, plus spécialement du nucléaire, après l'accident de Tchernobyl. C'est pourquoi la première analyse de cette notion, par le nucléaire, est présentée en ouverture, au chapitre 1. En résumé, cette première analyse indique que pour assurer une bonne culture de sûreté dans l'organisation, les niveaux supérieurs de la hiérarchie doivent définir une politique de sûreté, assurer l'organisation de la sûreté (préciser les responsabilités, mettre en place les bonnes incitations), affecter les ressources nécessaires et faire pratiquer le contrôle et l'audit. Les niveaux opérationnels, quant à eux, doivent développer un professionnalisme de la sûreté qui combine attitude interrogative, démarche rigoureuse et prudente et pratique de la recherche et de la circulation de l'information.

Cette notion de culture de sûreté est ensuite illustrée par le cas des laboratoires des universités américaines (chapitre 2), qui suscite la question : « Faut-il agir par la procédure (ou la réglementation) ou bien en améliorant la culture de sûreté ? » La réglementation prescrit ce qu'il ne faut pas faire, alors qu'une bonne culture de sûreté fait adhérer à ce qu'il faut faire et incite à rechercher cette excellence. Elle est fondamentalement responsabilisante. Au contraire, la réglementation s'articule autour des dangers connus plutôt que des pratiques sûres et impose des obligations plutôt que de développer une culture de sûreté.

Les groupes acceptent rarement avec enthousiasme une culture imposée de l'extérieur. Se crée donc un hiatus entre les obligations réglementaires et la culture du groupe. Ce phénomène est bien connu au sein même des entreprises où l'on sait que les procédures décidées '*en haut*' sont souvent inapplicables et conduisent au développement d'une culture parallèle au sein des groupes concernés '*sur le terrain*'.

Les notions de culture du risque et de culture de sûreté sont ensuite discutées avec quelque détail (chapitre 3). Cette discussion souligne leur intérêt pour sortir des limites de la sûreté technique, limites qui ne sont que partiellement repoussées quand la technique est combinée aux analyses de l'erreur humaine. Nous avons retenu trois critiques principales adressées aux notions de culture du risque et de culture de sûreté. La culture de sûreté correspondrait à une culture unique ; cette critique ne nous paraît recevable que pour des utilisations impropres de ces notions destinées à faire porter aux opérateurs l'essentiel de la responsabilité des risques. La notion de culture de sûreté s'appuie sur des concepts flous ; cette critique ne nous paraît pas décisive quand on songe que des notions comme la confiance des consommateurs donnent

lieu à des indicateurs chiffrés entourés de beaucoup d'attention. Enfin, la notion de culture de sûreté n'est pas opératoire ; nous pensons que cette critique est infondée — sinon nous n'y aurions pas consacré cet ouvrage ! Nous donnons dès ce chapitre deux exemples concrets d'actions qui réfèrent presque explicitement à ces notions, mais le chapitre suivant ainsi qu'une bonne partie de ce travail montre qu'elle est sous-jacente dans tout le domaine des risques sauf peut-être dans les aspects strictement techniques — et cela resterait à prouver...

Le chapitre 4 montre l'importance des concepts discutés ci-dessus et comment ils peuvent donner lieu à des actions de management. L'organisation peut évaluer sa culture de risque par sondage, en recueillant l'opinion des collaborateurs sur la culture et l'environnement en matière de risque, et se donner ainsi un miroir, notamment sur quatre points principaux :

- (1) les valeurs de l'organisation, sa mission et ses objectifs (leadership) ;
- (2) la capacité à responsabiliser, à mesurer l'efficacité et à récompenser la performance ;
- (3) le partage des connaissances et de l'information et le développement des compétences ;
- (4) l'évaluation des risques ; la capacité à prendre des mesures de contrôle des risques.

Cette mesure reste probablement souvent grossière, et peut-être plus facilement praticable en Amérique que dans le contexte français. Néanmoins, elle permet de discerner les disparités de culture du risque entre services et de comparer le sentiment de maîtrise de la direction à la perception des employés 'sur le terrain'.

Nous proposons ensuite (chapitre 5) une définition de la culture du risque, à savoir :

La culture du risque est la façon de penser, de ressentir et d'aborder le risque dans l'organisation concernée. C'est la fondation mentale sur laquelle se bâtit le risk management. Elle est donc essentielle.

et une définition de la culture de sûreté :

La culture de sûreté est la partie de la culture du risque qui se rapporte à la technologie utilisée par l'organisation considérée, spécialement à ses usages risqués pour les employés, les riverains, l'environnement.

Nous suggérons que ces notions pourraient être repérées par les réponses aux questions suivantes : quels sont nos risques ? Quelle est l'importance relative de nos risques (d'un point de vue subjectif) ? Quelle quantité de risque sommes-nous prêts à prendre ? Comment traitons-nous les risques que nous acceptons de prendre ?

Une organisation dotée d'une forte culture du risque s'engage à *connaître et traiter* ses risques. Leur exploration systématique fait progresser la culture du risque. Il est généralement reconnu qu'une bonne culture du risque se fonde sur une certaine homogénéité des sous-cultures. Au delà de la gestion des risques, renforcer la culture du risque profite à la culture de l'entreprise en général.

Enfin nous terminons par un exemple de défaut de culture du risque : la rupture d'une digue à Aramon dans le Gard, lors des inondations de septembre 2002 (chapitre 6). C'est l'ignorance du risque qui prédomine avant le désastre, l'incompréhension après. Ainsi, la culture du risque est une exigence d'intelligence et de connaissance.

II - Intelligence du risque

À ce stade, les notions de culture du risque et de culture de sûreté sont devenues plus claires et l'on comprend qu'une bonne culture du risque implique une exigence d'intelligence et de connaissance des risques. C'est cet aspect qu'aborde la deuxième partie, en commençant assez naturellement par le secteur nucléaire, un secteur généralement en avance dans ce domaine — pour d'excellentes raisons, évidemment.

Les concepts de la sûreté nucléaire (chapitre 7) comportent notamment : la défense en profondeur, une attitude de prudence et de pessimisme dans l'étude des accidents possibles, un retour d'expérience systématique, des études probabilistes de sûreté. Dans l'ensemble, on constate que les concepts ont nettement évolué depuis les premières études de sûreté. Le domaine de la sûreté n'a acquis sa légitimité et sa maturité actuelle que de façon progressive. Pour réduire la complexité des tâches, on avait commencé par se donner un champ d'investigation et des hypothèses trop restreints. En particulier, les études, conduites par des ingénieurs, ont eu tendance à privilégier les aspects les plus 'nobles' d'un point de vue d'ingénieur en négligeant parfois certains aspects qui auraient été jugés essentiels par un risk manager. La prise en compte des facteurs humains s'est développée de façon progressive dans les études probabilistes de sûreté.

D'une façon générale, la sûreté est largement inscrite dans la connaissance et l'intelligence des risques — au niveau global de 'la' connaissance, mais aussi dans l'intelligence spécifique des risques dans tel établissement, telle équipe ou chez telle personne. Dans cette optique, une gestion de la sûreté qui se donne pour objectif de satisfaire a minima les normes en vigueur ne développe pas la culture de sûreté. Si elle a pour résultat de faire diminuer l'intérêt porté aux questions de sûreté, de limiter la connaissance et les échanges d'information à ce sujet, on peut considérer qu'elle est dangereuse. Cette vision est esquissée au chapitre 8.

Le chapitre 9 développe cette analyse dans le cas de l'aviation civile. Dans ce secteur, la responsabilisation des compagnies est un maître mot du contrôle. Evidemment, les accidents y sont excessivement coûteux et, d'une façon générale, les compagnies sont motivées à développer la sécurité de leurs opérations. Cette responsabilisation amène à superviser le système de gestion de la compagnie et non les opérations elles-mêmes. Les systèmes d'information jouent un rôle capital et, dans de nombreuses compagnies, l'on procède maintenant à l'analyse systématique des 'boîtes noires'. La gestion de l'inspection et de la formation joue un rôle important. Aux côtés des opérateurs (les compagnies aériennes), les constructeurs d'aéronefs sont tenus de suivre leurs produits pendant toute la durée de vie de ces derniers.

L'intelligence du risque se décline évidemment dans une multitude de secteurs, avec des spécificités parfois très marquées, le cas de l'aviation restant probablement représentatif et utile pour de nombreux autres secteurs. Il serait passionnant de couvrir une grande partie de ces efforts, mais cela dépasserait le cadre de cet ouvrage. On a voulu signaler, néanmoins, un travail assez remarquable dans le domaine du risque inondation, un domaine important en raison du poids économique des dommages et du fait qu'il relève non pas d'entreprises privées comme les compagnies d'aviation, mais d'un ensemble d'acteurs publics. Ce rapport de la Commission Internationale pour la Protection du Rhin incarne un véritable effort d'intelligence et de diffusion de la culture du risque dans ce domaine. On ne peut qu'en recommander la lecture complète, le chapitre 10 se contentant ici d'y introduire le lecteur.

III - Gouvernance d'entreprise

Un mouvement se dessine en faveur d'une gouvernance des risques dans les entreprises. En Grande Bretagne, pays le plus avancé dans ce domaine, probablement en raison de l'émoi suscité par la faillite de la banque Barings, le rapport Turnbull (1999) explicite les exigences de base d'une telle gouvernance. Il décline la *nécessaire intelligence* des risques au niveau du Conseil, de la Direction et de l'ensemble des employés et montre qu'elle implique d'intégrer la gestion des risques au sein de l'activité ordinaire, tout en restant lucide sur l'impossibilité d'éliminer totalement le risque (chapitre 11). En particulier, le rapport détaille les caractéristiques d'un système de contrôle interne et propose une intéressante série de questions relatives à l'intelligence du risque, aux contrôles (l'organisation interne), à la communication et au suivi. Enfin nous discutons le rapport Turnbull à partir des questions suivantes : une approche purement financière est-elle valable ? une approche de la gouvernance uniquement dirigée vers les actionnaires est-elle équilibrée ? quelle est l'efficacité d'un code de gouvernance, particulièrement après l'affaire Enron et les autres scandales de gouvernance d'entreprise au États Unis ? et enfin, quelle communication peut-on mener autour des risques ?

Le rapport Turnbull a suscité de nombreuses questions sur sa mise en oeuvre. L'institut des comptables britanniques a publié des documents explicatifs qui sont autant de développements pratiques du rapport. Ces documents révèlent, en particulier, la faible place des risques technologiques et environnementaux dans les entreprises en général, c'est-à-dire y compris les entreprises n'opérant pas d'installations à risques (chapitre 12). Le rapport Turnbull suggère que le traitement des risques doit être intégré dans les activités et impliquer l'ensemble du personnel (chapitre 13). Contrairement à d'autres fonctions, il est mauvais de vouloir l'externaliser ce qui suggère que la théorie s'appliquant à des activités ordinaires (nettoyage des locaux, maintenance informatique, etc.) n'est pas pertinente en matière de risque. Une remarque de poids, car on aurait pu penser que, se plaçant au niveau des Directions d'entreprise et des Conseils d'administration, ce rapport d'inspiration financière conçoive la gestion des risques comme une affaire de spécialistes puisque c'est la tendance dans de nombreux domaines des risques financiers.

Après l'analyse des recommandations, souvent excellentes en tant que telles, relatives à la gouvernance d'entreprise en matière de risque, nous nous tournons vers la réalité. L'ampleur de la crise ouverte aux États Unis par les faillites retentissantes d'entreprise de premier plan comme Enron et WorldCom a fait réfléchir. Comment en est-on arrivé à autant de désinvolture des dirigeants par rapport aux autres parties prenantes : actionnaires, créanciers, salariés, consommateurs californiens d'électricité, comment ont-ils tous ont été instrumentalisés et escroqués ? C'est l'objet du chapitre 14 dont la réponse, au-delà de l'avidité des hommes, met en avant une immense défaillance organisationnelle de '*corporate america*'.

S'agissant de la première, l'avidité imprègne les élites américaines au delà de ce que l'on avait sans doute généralement imaginé. C'est ainsi, par exemple, que « *en 1973, le PDG moyen d'une 'major' gagnait environ 45 fois le salaire des employés...en 1991, le ratio était de 140. Maintenant, il est de 500* » (John Cassidy).

Pour ce qui est de l'organisation, les mécanismes pervers qui ont soutenu la mise en place de cette culture de la cupidité ('*greed*') incluent :

- des incitations perverses des stock options, mais aussi du système global dans lequel opèrent les dirigeants et qui s'imposent à eux ;
- des pratiques 'créatives' voire des tromperies au niveau des comptabilités, mais aussi des règles insuffisantes et l'incitation forte à présenter une image positive ;
- une cupidité naturelle, mais aussi un système qui amène progressivement des personnes à l'éthique 'normale' à glisser vers des pratiques finalement désastreuses.

Ce chapitre donne un grand nombre d'exemples convaincants de la dérive ayant mené d'une culture entrepreneuriale respectant la production et les partenaires, à une culture financière de prédation qui risque de perdurer (voir l'affaire Metaleurop révélée en janvier 2003). Les solutions, elles, ne sont ni nombreuses ni très convaincantes, mais le MEDD pourrait légitimement s'investir dans ces problématiques de gouvernement d'entreprise.

Cette description de la gouvernance d'entreprise au États Unis fait apparaître une orientation fortement financière, axée sur le profit quels qu'en soient les moyens, et tournée vers les seuls actionnaires. Les objectifs financiers globaux, décidés en haut, en partie à Wall Street et dans les bureaux des gestionnaires de fonds de pensions, se traduisent sur le terrain, dans les bureaux et dans les ateliers, par des 'programmes de rigueur', des 'cures d'amaigrissement', des 'licenciements mondialisés'. Une telle culture n'est guère propice au développement de la culture de sûreté.

En effet, la question se pose, face à l'emprise de ce modèle, de savoir s'il est possible d'être efficace autrement ou si l'adoption de la gestion purement financière est inéluctable. Si c'était le cas, on devrait être inquiet en matière de risques, car ce n'est pas à base de suppressions et de pressions répétées sur les moyens disponibles que l'on peut parvenir à améliorer la sûreté au quotidien dans les installations à risques. C'est au contraire à une action de construction que l'on doit s'attacher : construire une connaissance, une intelligence et un sens des risques. Or, précisément, l'exemple de Toyota (chapitre 15) montre qu'il est possible de gérer en reconnaissant la valeur du système de production, en cherchant à améliorer ce système, cet organisme, cet ensemble fin de relations, en reconnaissant qu'il s'agit d'une construction plus organique que mécanique, où l'on ne peut pas impunément changer les éléments, réduire les ressources et pousser les performances à la limite.

La plus grande variété de modèles produits chez Toyota n'y est pas un frein à l'efficacité . L'attention portée au système de production y améliore **à la fois** la gamme de produits et l'efficacité et la productivité ; c'est une façon de sortir par le haut des dilemmes économiques. Il ne s'agit ni d'innovation produit ni d'innovation 'process' au sens strict, mais plutôt d'innovation d'organisation et de culture, d'une attention aux « *détails de la façon dont chaque travailleur, à chaque poste contribue à satisfaire la commande de chaque consommateur* » (Johnson et Bröms). Une bonne gestion des risques technologiques et une bonne gestion de crise doivent également se baser sur l'attention portée au système de production, sur l'innovation d'organisation et de culture, et une attention aux détails de la façon dont chaque travailleur fonctionne. C'est l'ambition du Management Basé sur les Moyens (MBM) que le chapitre 16 expose et compare au management basé sur les résultats (financiers). De nombreux exemples des dangers de ce dernier sont donnés.

Ce sont des approches constructives, semblables aux approches qualité, qui devraient permettre de bâtir la culture de sûreté et l'intelligence du risque. La stratégie MBM vise à instiller en chacun un engagement profond à maîtriser une approche ordonnée du travail. On trouve des idées très similaires dans les textes relatifs à la culture de sûreté des opérateurs du nucléaire (chapitre 1). La qualité est intégrée au travail que chacun effectue.

Une remarque, enfin, sur la gouvernance : la grande taille des groupes mondialisés ne favorise pas nécessairement une attention systémique à la sûreté de chacun des établissements, car chacun ne pèse individuellement que peu au regard du résultat global (chapitre 17).

IV - Gérer les risques, cultiver la sûreté

Pour bien comprendre le paysage des risques, il faut avoir une idée de comment les décisions sont prises, d'où l'intérêt d'une typologie des situations de décision des divers acteurs en matière de risque (chapitre 18). La gestion des risques implique tout un réseau d'acteurs de niveaux hiérarchiques différents et plus ou moins proches du danger. Des contraintes et des limites différentes s'imposent à chacun. Ces contraintes ne favorisent pas une prise de décision idéale, notamment aux niveaux supérieurs de la hiérarchie et à proximité immédiate du risque. Cette situation pourrait être améliorée par une relation plus étroite de ces acteurs avec les spécialistes de l'analyse du risque. Plus généralement, le *risk management* requiert la définition des rôles, des responsabilités et des interactions entre acteurs.

On perçoit les enjeux d'une meilleure intelligence du risque : il est indispensable de 'créer du lien' entre les divers acteurs, on ne peut pas se contenter de développer des panoplies d'instruments à l'usage des analystes et que les autres acteurs ne comprendront guère et n'utiliseront pas.

Pour gérer les risques et cultiver la sûreté, qu'apporte le domaine, connu et reconnu, de la qualité ? Le chapitre 19 compare sûreté et qualité à partir de leurs meilleurs représentants. En termes de sûreté, les bons élèves³ possèdent cinq caractéristiques : (1) l'autorité est déléguée de façon souple ; (2) il existe une organisation spécifique en cas de crise ; (3) les apports des opérateurs sont reconnus ; (4) la transparence est favorisée, on recherche ouvertement les erreurs ; (5) le changement organisationnel est jugé à l'aune de la sûreté. Dans le domaine du management de la qualité, on retrouve des principes semblables aux quatre premiers traits. En revanche, la priorité qu'exprime 'le changement organisationnel est jugé à l'aune de la sûreté' ne se retrouve pas nécessairement dans le domaine de la qualité.

Cette priorité donnée à la sûreté, caractéristique des entreprises à hauts risques et pourvues d'une bonne culture de sûreté, n'est évidemment pas une priorité absolue, même si elle est parfois affichée comme telle. La sûreté absolue, ce serait de ne rien entreprendre de dangereux ! Son statut est probablement complexe, une part relevant de gestion multicritère, une autre de communication.

D'un point de vue économique, « la sûreté n'a pas de prix, mais elle a un coût ! » Quand on observe les comportements d'industries à risques telles que le nucléaire ou l'aviation, le budget alloué à la sûreté n'est pas infini. Ainsi, le discours sur la priorité de la sûreté est perçu avec scepticisme par l'économiste. Un niveau de sécurité *acceptable* est, certes, une condition *nécessaire* de fonctionnement des usines à risques, mais nous envisageons plus généralement, en termes de théorie économique, la prise en compte de la sûreté (chapitre 20). La notion d'avantage conjoint, en terme de sûreté comme en terme de production, se dégage contredisant la notion d'opposition de la production et de la sûreté. La perception des risques par les décideurs apparaît cruciale. Nous comparons avec le domaine voisin de la qualité : si

³ Ce sont, par exemple, les HRO, *High Reliability Organizations*, étudiées aux États Unis, à l'université de Berkeley

le coût de la non qualité est répercuté assez directement par le marché, il n'en est pas de même du coût de la non sûreté. Non seulement le coût de la sûreté n'est pas automatiquement relié à des avantages économiques, mais en outre, la pression du marché va plutôt à l'encontre des objectifs de sûreté.

Ce type d'analyse suggère que la sûreté devrait être conçue dans un esprit d'amélioration tenace, persévérante et jamais achevée des méthodes de production avec la conscience qu'elle a de nombreux effets positifs sur ladite production et sa qualité. D'ailleurs, les ingénieurs qualité qui améliorent les 'process' pour garantir une excellente fiabilité des produits, contribuent ainsi à améliorer la sûreté.

Comment œuvrer dans ce sens au niveau des autorités ?

L'intelligence du risque dans le domaine de l'aviation civile (chapitre 9) permet de mesurer combien la gestion indirecte des risques par l'autorité de régulation est susceptible de faire progresser la culture de sûreté. Peut-on étendre ce type de régulation au domaine des établissements à risques ? Certains soutiennent que l'obligation de tenir un système de gestion de la sûreté (SGS) existe déjà en France pour les entreprises présentant des risques significatifs. Nous montrons (chapitre 21) : (1) que le champ des entreprises à risques est loin d'être couvert ; (2) que les SGS existants ne sont pas nécessairement satisfaisants en raison de la difficulté à les auditer et à prendre des mesures contraignantes le cas échéant.

Plus généralement, le style d'action de l'administration a bien progressé depuis le commandement régalien descendant de Paris. Il est aujourd'hui fondé sur une culture de dialogue entre l'administration et l'industrie et sur l'établissement de plans d'action nationaux concertés. Nous montrons sur un exemple (chapitre 22) qu'une étape supplémentaire pourrait être envisagée, inspirée par le souci de développer la culture du risque et orientée vers la responsabilisation des acteurs.

De tels changements d'attitude, de stratégie, ne sont peut-être pas aussi difficiles à intégrer que le suggèrent certains observateurs, même si, à l'instar d'un exemple documenté dans le cas de l'administration suisse (chapitre 23), les résistances sont parfois profondes dans les administrations.

Nous terminons avec un point capital : les inspections sont-elles efficaces ? (chapitre 24). Les contre-exemples ne manquent pas ! Certes toutes les inspections ne sont pas totalement inefficaces. Si, néanmoins, les inspections ne fournissent qu'une garantie assez médiocre contre les désastres, ne vaut-il pas mieux s'appuyer sur des stratégies de responsabilisation et de développement de la culture du risque et de la sûreté ?

I - CULTURE DU RISQUE ET CULTURE DE SÛRETÉ : DE QUOI PARLE-T-ON ?

Pourquoi les techniques du risque et de la sûreté, pourtant parfois simples et peu onéreuses, sont-elles souvent ignorées ou mal appliquées ? Les notions de culture du risque et culture de sûreté éclairent des facteurs situés en amont des techniques. Elles permettent d'examiner les façons d'aborder le risque, en général et avant toute approche technique. Ces façons d'aborder le risque peuvent influencer de façon cruciale sur l'adoption, ou non, de certaines techniques et sur l'application judicieuse, ou non, d'autres techniques.

Cette première partie est construite autour des définitions de la culture du risque et de la culture de sûreté. Elle aide à préciser l'origine de ces définitions et les débats qui les entourent. En outre, elle propose des exemples réels assez nombreux, car il ne s'agit pas de définir pour le plaisir des mots. Les définitions servent, en effet, à fixer une orientation du regard vers la réalité du risque. Elles aident à répondre à l'interrogation ci-dessus.

L'idée de culture de sûreté vient du terrain, plus spécialement du nucléaire, après l'accident de Tchernobyl. C'est pourquoi la première analyse de cette notion, par le nucléaire, est présentée en ouverture, au chapitre 1. En résumé, cette première analyse indique que pour assurer une bonne culture de sûreté dans l'organisation, les niveaux supérieurs de la hiérarchie doivent définir une politique de sûreté, assurer l'organisation de la sûreté (préciser les responsabilités, mettre en place les bonnes incitations), affecter les ressources nécessaires et faire pratiquer le contrôle et l'audit. Les niveaux opérationnels, quant à eux, doivent développer un professionnalisme de la sûreté qui combine attitude interrogative, démarche rigoureuse et prudente et pratique de la recherche et de la circulation de l'information.

Cette notion de culture de sûreté est ensuite illustrée par le cas des laboratoires des universités américaines (chapitre 2), qui suscite la question : « Faut-il agir par la procédure (ou la réglementation) ou bien en améliorant la culture de sûreté ? La réglementation prescrit ce qu'il ne faut pas faire, alors qu'une bonne culture de sûreté fait adhérer à ce qu'il faut faire et incite à rechercher cette excellence. Elle est fondamentalement responsabilisante. Au contraire, la réglementation s'articule autour des dangers connus plutôt que des pratiques sûres et impose des obligations plutôt que de développer une culture de sûreté.

Les groupes acceptent rarement avec enthousiasme une culture imposée de l'extérieur. Se crée donc un hiatus entre les obligations réglementaires et la culture du groupe. Ce phénomène est bien connu au sein même des entreprises où l'on sait que les procédures décidées '*en haut*' sont souvent inapplicables et conduisent au développement d'une culture parallèle au sein des groupes concernés '*sur le terrain*'.

Les notions de culture du risque et de culture de sûreté sont ensuite discutées avec quelque détail (chapitre 3). Cette discussion souligne leur intérêt pour sortir des limites de la sûreté technique, limites qui ne sont que partiellement repoussées quand celle-ci est combinée aux

analyses de l'erreur humaine. Nous avons retenu trois critiques principales adressées aux notions de culture du risque et de culture de sûreté. La culture de sûreté correspondrait à une culture unique ; cette critique ne nous paraît recevable que pour des utilisations impropres de ces notions destinées à faire porter aux opérateurs l'essentiel de la responsabilité des risques. La notion de culture de sûreté s'appuie sur des concepts flous ; cette critique ne nous paraît pas décisive quand on songe que des notions comme la confiance des consommateurs donnent lieu à des indicateurs chiffrés entourés de beaucoup d'attention. Enfin, la notion de culture de sûreté n'est pas opératoire ; nous pensons que cette critique est infondée — sinon nous n'y aurions pas consacré cet ouvrage ! Nous donnons dès ce chapitre deux exemples concrets d'actions qui réfèrent presque explicitement à ces notions, mais le chapitre suivant ainsi qu'une bonne partie de ce travail montre qu'elle est sous-jacente dans tout le domaine des risques sauf peut-être dans les aspects strictement techniques — et cela resterait à prouver...

Le chapitre 4 montre l'importance des concepts discutés ci-dessus et comment ils peuvent donner lieu à des actions de management. L'organisation peut évaluer sa culture de risque par sondage, en recueillant l'opinion des collaborateurs sur la culture et l'environnement en matière de risque, et se donner ainsi un miroir, notamment sur quatre points principaux : les valeurs de l'organisation, sa mission et ses objectifs (leadership) ; la capacité à responsabiliser, à mesurer l'efficacité et à récompenser la performance ; le partage des connaissances et de l'information ; la promotion et le développement des compétences ; l'évaluation et la mesure des risques ; la capacité à prendre en compte les processus et des mesures de contrôle des risques.

Cette mesure reste probablement souvent grossière, et peut-être plus facilement praticable en Amérique que dans le contexte français. Néanmoins, elle permet de discerner les disparités de culture du risque entre services et de comparer le sentiment de maîtrise de la direction à la perception des employés.

Nous proposons ensuite (chapitre 5) une définition de la culture du risque, à savoir :

La culture du risque est la façon de penser, de ressentir et d'aborder le risque dans l'organisation concernée. C'est la fondation mentale sur laquelle se bâtit le risk management. Elle est donc essentielle.

et une définition de la culture de sûreté :

La culture de sûreté est la partie de la culture du risque qui se rapporte à la technologie utilisée par l'organisation considérée, spécialement à ses usages risqués pour les employés, les riverains, l'environnement.

Ces notions pourraient être repérées par les réponses aux questions suivantes : quels sont nos risques ? Quelle est l'importance relative de nos risques (d'un point de vue subjectif) ? Quelle quantité de risque sommes-nous prêts à prendre ? Comment traitons-nous les risques que nous acceptons de prendre ?

Une organisation dotée d'une forte culture du risque s'engage à *connaître et traiter* ses risques. Leur exploration systématique fait progresser la culture du risque. Il est généralement reconnu qu'une bonne culture du risque se fonde sur une certaine homogénéité des sous-cultures. Au delà de la gestion des risques elle-même, renforcer la culture du risque profite à la culture de l'entreprise en général.

Enfin nous terminons par un exemple de défaut de culture du risque : la rupture d'une digue à Aramon dans le Gard, lors des inondations de septembre 2002 (chapitre 6). C'est l'ignorance du risque qui prédomine avant le désastre, l'incompréhension après. Ainsi, la

culture du risque est une exigence d'intelligence et de connaissance. Ces aspects sont abordés dans la partie II.

1. NAISSANCE DU CONCEPT DE CULTURE DE SÛRETÉ

Le terme de culture de sûreté est d'utilisation assez courante sans que l'on sache toujours clairement ce qu'il recouvre. Ce chapitre en résume la première tentative de définition rigoureuse, due au monde nucléaire. Le texte complet, *CULTURE DE SÛRETÉ, Rapport du Groupe consultatif international pour la sûreté nucléaire, Agence internationale de l'énergie atomique, Vienne, 1991*, figure en annexe 1. Nous passons en revue :

- l'historique ayant conduit à cette notion
- la définition
- ce qu'elle implique pour la structuration et les missions des niveaux supérieurs
- ce qu'elle exige, en outre, dans les comportements des dirigeants
- le bon comportement des individus
- enfin, la tentative de rendre la notion repérable sinon mesurable.

En résumé, les niveaux supérieurs de la hiérarchie doivent définir une politique de sûreté, assurer l'organisation de la sûreté (préciser les responsabilités, mettre en place les bonnes incitations), affecter les ressources nécessaires et faire pratiquer le contrôle et l'audit. Les niveaux opérationnels doivent développer un professionnalisme de la sûreté qui combine attitude interrogative, démarche rigoureuse et prudente, pratique de la recherche et de la circulation de l'information.

Les spécialistes du monde nucléaire considèrent cette première définition comme fondatrice, mais néanmoins inapplicable. Il semble, en effet, que la nécessité pour l'Agence Internationale de l'Énergie Atomique de poser, avec une certaine autorité, une définition crédible ait fait passer au second plan un examen critique poussé des idées.

Historique

Comme dit le directeur de l'Agence Internationale de l'Énergie Atomique (AIEA) : « *Les questions d'ingénierie ont bénéficié pendant de nombreuses années d'une attention soutenue de la part de la communauté nucléaire. Cependant, c'est seulement pendant les années 1990 approximativement que les problèmes d'organisation et de culture ont été reconnus comme essentiels à la sûreté des opérations*⁴. »

La note *Évolutions des concepts de la sûreté nucléaire* (D1-01-103) identifie schématiquement trois périodes :

- jusqu'à l'accident de Three Mile Island (1979), la démarche technologique de sûreté domine largement la pensée majoritaire en matière de sûreté nucléaire ;
- après l'accident de Three Mile Island, les aspects humains deviennent légitimes. On réalise, en particulier, que les opérateurs doivent pouvoir identifier l'état du système (l'interface homme-machine doit transmettre efficacement l'information). L'intérêt pour l'organisation de la sûreté se manifeste par la mise en place de systèmes de retour d'expérience performants dans les pays utilisant des installations nucléaires et au niveau international ;
- après l'accident de Tchernobyl (1986), la communauté nucléaire comprend que c'est l'ensemble de l'organisation nucléaire, le système complet (y compris les régulateurs, les experts, les concepteurs) qui détermine l'attitude des opérateurs et donc la sûreté des opérations.

Pendant quelques années la notion de culture de sûreté circule ensuite sans définition claire du concept. C'est en 1991 que l'AIEA publie *Culture de sûreté* (INSAG-4) et définit précisément le concept dans le cadre de l'industrie nucléaire. Dans l'optique de généralisation qui est la nôtre, nous évitons ici de faire spécifiquement mention du secteur nucléaire.

Définition

L'INSAG-4 donne la première définition de la culture de sûreté :

La culture de sûreté est l'ensemble des caractéristiques et des attitudes qui, dans les organismes et chez les individus, font que les questions relatives à la sûreté bénéficient, en priorité, de l'attention qu'elles méritent en raison de leur importance.

Cette définition fait ressortir que la culture de sûreté est :

- une question d'attitude (les individus) autant que de structure (les organismes) ; les bonnes pratiques sont essentielles, mais elles ne suffisent pas si elles ne sont appliquées que de manière formelle ;
- exige que toutes les questions de sûreté soient perçues et traitées.

⁴ Préface à l'INSAG-13, *Management of Operational Safety in Nuclear Power Plants*, AIEA 1999. INSAG est le sigle anglais du Groupe consultatif international pour la sûreté nucléaire. Les publications de ce groupe sont désignées INSAG – suivi d'un numéro d'ordre.

Des éléments repérables.

Même si les éléments constitutifs de la culture de sûreté ne sont pas mesurables au sens rigoureux que l'ingénieur donne à ce terme, ils sont néanmoins repérables. Définir des moyens d'évaluer la culture de sûreté est capital, car : « *Tous ceux qui s'occupent de questions touchant à la sûreté affirmeront [qu'une bonne culture de sûreté]... 'c'est ce que nous faisons déjà'.* » Autant il sera aisé, rétrospectivement, après l'accident grave, de trouver des éléments défailants dans la culture de sûreté, autant une mission d'évaluation *ex ante* risque d'avoir de grandes difficultés à se faire entendre voire à évaluer la situation⁵.

D'autres éléments relatifs aux attitudes ont été ajoutés à cette définition, tels que *une habitude de penser en termes de sûreté*, ou encore *l'engagement et le sens de la responsabilité de tous*. De telles attitudes ne peuvent évidemment qu'être encouragées, mais pour une généralisation hors du domaine nucléaire, il semble utile, pour commencer, de conserver l'équilibre de la définition ci-dessus entre le rôle des attitudes et des structures. En effet, l'industrie nucléaire possède des structures assez performantes en matière de sûreté parce que la conscience du risque y est grande, mais il n'en est sûrement pas de même dans tous les secteurs et pour tous les risques.

Le résumé ci-après, tout comme le texte complet reproduit en annexe 1, est à l'indicatif du présent, se plaçant résolument dans la situation d'une culture de sûreté parfaite.

Les niveaux supérieurs de la hiérarchie

La manière dont agissent les individus dépend des positions et décisions prises aux niveaux qui leurs sont supérieurs.

Politique de sûreté

Les niveaux supérieurs affichent leur politique de sûreté. Celle-ci fait connaître et comprendre, largement et de façon transparente, leurs responsabilités et leur engagement à rechercher l'excellence en matière de sûreté. Elle exprime clairement que la sûreté est une priorité absolue et prend le pas, au besoin, sur les impératifs de production ou les calendriers de réalisation de projets.

La politique de sûreté des niveaux supérieurs donne des orientations claires aux organismes et aux individus qui dépendent d'eux.

Les niveaux supérieurs commencent avec le pouvoir législatif ; puis incluent les organismes réglementaires et de support ; puis la direction des organismes de production. À ces niveaux, la politique de sûreté fait l'objet d'une déclaration écrite qui peut être empreinte d'une certaine solennité. Elle a but interne, mais est largement diffusée.

Organisation, responsabilités, incitations

Les niveaux supérieurs établissent clairement le système des responsabilités des niveaux inférieurs. L'exercice des responsabilités est facilité par des lignes hiérarchiques uniques (ni omission ni chevauchement) et bien définies (documentées et sans ambiguïté). Les lignes de

⁵ Voir chapitre 24

communication sont aussi directes que possible. Les responsabilités des entités de même niveau (collègues et partenaires de travail) doivent être transparentes à chaque niveau.

La responsabilité formelle des unités de production incombe à l'organisme exploitant et, par délégation, au chef d'établissement. Les organismes de production s'assurent que leurs partenaires sont fiables.

Les responsabilités en matière de sûreté sont intégrées dans la hiérarchie. Elles ont autant d'importance que les autres fonctions principales. En particulier, des services internes indépendants surveillent les activités ayant trait à la sûreté, examinent les pratiques et rendent compte à ce niveau élevé.

Les incitations ne sont pas uniquement basées sur la performance de production, mais aussi sur la performance de sûreté. En dernière analyse, c'est le comportement des individus, influencé par des motivations et des attitudes tant personnelles que collectives, qui fait qu'une pratique est satisfaisante. Les niveaux supérieurs s'efforcent de récompenser et de faire récompenser la performance de sûreté. Ils veillent à ce que les systèmes de récompense n'encouragent pas la production si la sûreté s'en trouve compromise.

Ressources

Des ressources adéquates sont consacrées à la sûreté :

- personnel nombreux et qualifié ;
- les tâches peuvent être effectuées sans hâte ou pression excessives ;
- les professionnels compétents en matière de sûreté peuvent être promus à des postes clefs ;
- la formation est une priorité et dispose des budgets nécessaires ;
- le personnel dispose des moyens matériels nécessaires à sa mission ;
- l'environnement de travail favorise la bonne exécution des tâches.

Contrôle et audit

Les pratiques relatives à la sûreté sont régulièrement auditées : politique du personnel, retour d'expérience, ingénierie, procédures d'exploitation. L'audit est positif, il ne devient jamais une recherche de culpabilités.

Exigences imposées aux dirigeants

Les dirigeants mettent en pratique ce qui précède au niveau supérieur qui est le leur.

En outre, ils doivent y mettre la manière. C'est ainsi que les dirigeants témoignent de leur engagement envers la sûreté ce qui a une vertu d'entraînement sur tout le personnel.

C'est aux dirigeants qu'il appartient d'instaurer un environnement de travail et des pratiques conformes aux objectifs de sûreté.

Réactions des individus

La réaction de tous ceux qui recherchent l'excellence en matière de sûreté implique : une attitude interrogative, une démarche rigoureuse et prudente, la communication. Le résultat est une véritable culture de sûreté chez les individus. Elle rend fier de s'acquitter des tâches importantes avec professionnalisme.

Attitude interrogative

Le texte dresse la liste de onze questions que les individus doivent se poser avant d'agir. Par exemple : « Qu'est-ce qui peut mal tourner ? », « Quelles pourraient être les conséquences d'une défaillance ou d'une erreur ? ». Cette attitude, principalement pensée en référence aux opérateurs, concerne, en réalité, tous les individus.

Démarche rigoureuse et prudente

Comprendre, être prêt à parer à toute éventualité, prendre le temps de réfléchir, etc. Mais aussi pratiquer des valeurs telles que l'ordre, la ponctualité, le soin.

Communication

Reconnaître l'importance d'une bonne information : obtenir l'information nécessaire, informer les autres, rendre compte, proposer des initiatives.

Application

[Le document décline ensuite la mise en pratique des principes ci-dessus.]

L'organisme réglementaire : un engagement sans faille envers la sûreté, mais dans une atmosphère positive de confiance, d'ouverture et de réalisme.

En particulier, s'agissant de l'organisme réglementaire, le texte préconise :

- des rapports fondés sur la confiance tout en conservant le caractère formel et indépendant qui convient ;
- une attitude ouverte, les sujets controversés sont traités franchement ;
- les normes prévoient un niveau de sécurité approprié tout en admettant l'existence d'un risque résiduel inévitable ;
- la sûreté relève clairement de la responsabilité de l'exploitant ; la réglementation ne doit donc pas être astreignante au point d'imposer des contraintes excessives ;
- une démarche généralement conservatrice mais qui n'étouffe pas l'innovation.

[Le lecteur ne peut manquer de remarquer combien la réalité décrite est difficile à saisir de façon rigoureuse, combien elle semble basée sur un art fait de compromis raisonnable et de finesse politique.]

[Un paragraphe spécial, consacré à la contrainte économique, précise : « des considérations purement économiques pourraient être préjudiciables à la sûreté ». L'organisme réglementaire doit en tenir compte.]

Les établissements de production

[Au niveau des établissements de production, trois points principaux sont détaillés : l'environnement de travail, les attitudes individuelles, l'expérience en matière de sûreté. Les principes indiqués plus haut sont précisés. L'importance des échanges portant sur la sûreté est soulignée comme suit.]

Ils mettent en évidence les attitudes des dirigeants et influent sur celles du personnel. En particulier, les dirigeants saisissent les occasions qui se présentent de montrer qu'ils sont prêts à faire passer, au besoin, les exigences de sûreté avant les impératifs de production. Leur présence donne l'occasion de souligner directement l'importance qui s'attache à la sûreté.

La performance de sûreté

[Elle est le reflet de la culture de sûreté. Dans le cas du nucléaire qui apparaît très en avance sur nombre d'autres secteurs :]

Les indicateurs de performance d'une centrale communément admis (disponibilité de la centrale, nombre d'arrêts non programmés, radio-exposition) donnent une mesure de l'attention portée à la sûreté. Ils sont complétés par des indicateurs de sûreté spécifiques comme le nombre et la gravité des événements importants, le nombre d'ordres de travaux en souffrance et la durée de toute indisponibilité des systèmes de sûreté. L'importance de ces indicateurs est expliquée au personnel.

Tous les événements importants qui se sont produits sur le site sont analysés en étroite collaboration avec les personnes concernées afin d'aider tous les membres du personnel à évaluer leur points forts et leurs points faibles.

Ces données d'expérience sont examinées périodiquement pour vérifier que les leçons en ont été tirées et que les mesures correctives nécessaires ont été identifiées et mises en œuvre en temps opportun. L'exhaustivité des examens et la vigueur des mesures correctives constituent des indicateurs importants de la culture de sûreté.

Des questions pour soutenir l'évaluation de la culture de sûreté

L'annexe du document a une orientation pratique indéniable. La liste de 143 questions qui y figure est divisée en 18 thèmes divers :

- engagement du gouvernement à l'égard de la sûreté
- performance des organismes réglementaires
- politique de sûreté de l'exploitant
- pratiques de sûreté à l'échelon de l'organisme
- définition des responsabilités
- formation

- sélection des dirigeants
- la performance en matière de sûreté
- mise en valeur de la sûreté
- charge de travail
- relation entre dirigeants de site et autorités réglementaires
- attitude des dirigeants
- attitude des individus
- pratiques locales
- supervision sur le terrain par le personnel dirigeant
- contribution de la recherche aux analyses de sûreté
- codes pour les aspects de la conception relatifs à la sûreté
- processus d'examen de la conception.

Les questions sur les attitudes sont de loin les plus nombreuses (39 questions au total), suivies par celles portant sur la 'performance des organismes réglementaires' puis sur la 'formation'.

L'ensemble de ce qui précède révèle l'ampleur de la notion de culture de sûreté et la difficulté d'assurer sa qualité puisque l'on voit apparaître : l'art du régulateur, le charisme des dirigeants, des indicateurs de disponibilité, la sûreté au sens des accidents du travail, la volonté d'examen et de correction des événements importants.

La batterie de questions permet d'introduire un analyste aux divers aspects de la culture de sûreté d'un secteur. Elles peuvent l'aider considérablement dans l'art des recommandations possibles en la matière. L'effort doit être d'autant plus salué qu'il s'agit de l'ouverture d'une nouvelle voie. L'ampleur des défis à relever reste, néanmoins, très grande.

2. L'EXEMPLE DES LABORATOIRES DES UNIVERSITÉS AMÉRICAINES

Nous reproduisons ci-après un extrait d'un article de Ralph Stuart *Developing a Safety Culture in Academia* (1992). Il illustre fort bien la notion de culture de sûreté et sa nécessité.

[...]

Lab Safety Culture Taboos and Rituals

Lab cultures tend to be relatively homogenous between campuses, because there is a lot of interaction and communication among laboratories. Their members receive similar education and often move from one lab to another between campuses during the course of their careers as graduate students, lab techs and/or faculty researchers. Their results and methods are easily available in the scientific literature.

I can identify three pieces of lab risk culture which have developed significantly over the last five years (de 1987 à 1992). Lab people (although not without exception) are beginning to accept that mouth-pipetting (utilisation des pipettes en aspirant directement avec la bouche) is not a good idea. They are also beginning to understand that eating and drinking in laboratories is probably a poor practice and should be avoided. I have also noticed increased interest from lab workers in the proper disposal of chemical wastes.

I can also think of hazards which the lab risk culture ignores. For example, climate-controlled rooms, which are usually sealed with no ventilation provided, are commonly occupied by lab workers for hours at a time. At the same time, volatile chemicals, such as liquid nitrogen, dry ice or solvents are commonly stored and allowed to vent in these rooms. This is a high hazard situation, but most lab people have little awareness of this. Another area in which lab safety culture has not developed is fume hoods. In general, lab people have little knowledge about the proper use of fume hoods.

Is a Safety Culture Possible in Academia?

Academia is well known for being a distinct sub-culture. In fact, academia itself is made up of many different sub-cultures, often aligned among various academic fields. Is it possible to develop a safety culture in academia? In order to answer this question, it is necessary to consider the cultures that we are operating in.

U.S. Culture and Risk-Taking

In considering the American risk culture, it is clear that Americans accept and enjoy risks in their personal lives. Drinking, smoking and bungee-jumping (saut à l'élastique) all owe part of their strength in our culture because they carry elements of risk. However, Americans tend not to enjoy risks at work, particularly if they are unexpected. There is a much lower acceptance of any risks that the employer is seen as imposing on the worker on the job.

This dichotomy is particularly important in academic setting. Many people in the academic community see their activities there as a personal vocation

as much as a job. On the other hand, there are many people who work on university campuses who simply see their activity there as "just a job". So within an academic community, there will be many different attitudes toward the same risk.

The Academic Culture and Safety

The basic mission of an academic institution also presents obstacles to the development of a safety culture. Mistakes are considered to be part of the learning process, and therefore room for mistakes must be allowed. The focus of the research process is on the unknown, and serendipity (accidents, good or bad, *le hasard, pour le meilleur ou pour le pire*) is often a part of the process. It is often the job of the safety office to try to anticipate and limit the consequences of these mistakes and accidents.

Another obstacle to developing a safety culture in academia is social inertia. While academia has its share of bureaucratic inertia, there is also the special problem in laboratories of The Sacred Protocol. Changing lab practices for any reason violates the most important research taboo of avoiding change in any known variables. This is the primary reason for the continued use of chromic acid cleaning solution despite the environmental safety and health hazard it presents.

The academic culture does present some advantages when building a safety culture. In a social environment focused on learning, change can occur quickly in the population. In a decentralized environment, you can have a strong safety culture in one part of the institution independently of other parts.

Examples of Safety Culture in Academia

There are many different risk cultures already established in academia. Art departments, chemistry departments, agricultural schools, medical schools all differ in their approach to a similar level of risk. We need to consider these various approaches as we deal with the people in these areas and the risks they face.

To return to the title question of this section, Is a Safety Culture Possible in Academia?, the answer is that we don't have any choice but to work at developing a safety culture. Without a safety culture in place, a central safety office will be limited in its effect on the actual working conditions on campus. There are several reasons for this, including: 1) the prevailing risk cultures allocate few resources for centralized safety services, (consider the resources OSHA⁶ has available, compared to the size of the job it has to do); 2) the decentralized administrative structure of academia makes enforcement of institutional policies difficult and expensive; and 3) high turnover in academia makes central training and reinforcement of safety procedures ineffective.

[...]

Ralph Stuart

LAST UPDATE: 9/24/92

Article complet sur : http://hazard.com/library/safety_culture

⁶ Occupational Safety and Health Administration

Il n'y a donc pas de choix possible, selon l'auteur : il faut développer la culture de sûreté quelles que soient les difficultés.

Définition de la culture de sûreté

On comprend bien, sur cet exemple de l'université américaine et de ses laboratoires, à quoi correspond la culture de sûreté. Les termes employés sont,

en positif :

accepter... que telle pratique n'est pas très bonne,
comprendre... que telle autre pratique doit être évitée,
s'intéresser... à une meilleure façon de faire ;

en négatif :

ignorer... tel type de danger,
une faible conscience (awareness)... que telle situation est dangereuse,
peu de connaissance du bon usage... de tel appareil.

Il ne s'agit donc pas directement des comportements, mais plutôt des attitudes et des représentations que le groupe concerné entretient vis-à-vis de comportements à risques.

Nécessité de la culture de sûreté

Agir par la procédure (ou la réglementation) ou bien en améliorant la culture de sûreté ? À cette question l'auteur répond que la réglementation prescrit ce qu'il ne faut pas faire, alors qu'une bonne culture de sûreté fait adhérer à ce qu'il faut faire et incite à rechercher ce qu'il faut faire du point de vue de la sûreté. Elle est fondamentalement responsabilisante. Au contraire, la réglementation :

- s'articule autour des dangers connus plutôt que des pratiques sûres ;
- impose des obligations plutôt que de développer une culture de sûreté.

Les groupes acceptent rarement avec enthousiasme une culture imposée de l'extérieur. Se crée donc un hiatus entre les obligations réglementaires et la culture du groupe. Ce phénomène est bien connu au sein même des entreprises où l'on sait que les procédures décidées '*en haut*' sont souvent inapplicables et conduisent au développement d'une culture parallèle au sein des opérateurs concernés (par exemple, dans la maintenance des centrales nucléaires ; voir M. Bourrier, *Le nucléaire à l'épreuve de l'organisation*).

3. DISCUSSION DE LA NOTION DE CULTURE DE SÛRETÉ

1. La définition britannique⁷

« La catastrophe de Tchernobyl a projeté le concept de culture de sûreté sur les devants de la scène nucléaire. Proposé à l'origine par le Comité Consultatif de Sûreté Nucléaire de l'Agence Internationale de l'Energie Atomique, ce concept a depuis diffusé vers les autres industries à risques.

« La culture de sûreté est l'ensemble des caractéristiques et des attitudes qui, dans les organismes et chez les individus, font que les questions relatives à la sûreté des centrales nucléaires bénéficient, en priorité, de l'attention qu'elles méritent en raison de leur importance » (INSAG, 1991:1, voir chapitre 1).

Cette définition de la culture de sûreté en termes d'attitudes et de valeurs s'inscrit dans une perspective culturaliste. Cependant les questions de sécurité systémiques dépendent plus souvent de comportements que de valeurs ou d'attitudes. Cette proposition de l'INSAG a maintes fois été critiquée pour cela et il lui a souvent été préféré la définition du Comité Consultatif Britannique sur la sécurité des installations nucléaires (*British Advisory Committee on the Safety of Nuclear Installations – ACSNI*) :

« La culture de sûreté est le produit des valeurs, attitudes, perceptions et comportements individuels et collectifs qui déterminent la forme et le contenu des actions de prévention en santé et sécurité d'une organisation, ainsi que la façon dont ses membres s'impliquent dans ces actions » (ACSNI Study Group on Human Factors, 1993, *Organising for Safety, Health and Safety Commission*, London).

Le comité ACSNI met également en avant dans sa définition les phénomènes d'appropriation collective et le partage des aspects intellectuels et comportementaux de la sécurité.

« La culture de la sûreté est la conscience partagée entre acteurs d'un système qu'il est indispensable de promouvoir la sécurité du système dans sa globalité. Elle va de pair avec l'adoption de comportements appropriés ».

[...]

2. Intérêt de la notion de culture de sûreté⁴

De manière générale, la notion de culture de sûreté a considérablement stimulé l'évolution des recherches et des pratiques dans les systèmes à risques. Dans l'industrie nucléaire, ce concept a soulevé un très large intérêt. A titre d'exemple, les comités consultatifs

⁷ Les sections 1 et 2 ci-dessous sont dues à Fahlbruch & Wilpert (chapitre 4 de *Organiser la fiabilité* sous la direction de M. Bourrier (L'Harmattan, 2001), pp. 120-123). On a supprimé de nombreuses références du texte original (elles sont plus appropriées dans un texte de nature universitaire) et rajouté des sous-titres.

gouvernementaux suisse, allemand et britannique ont chacun publié un *mémoire* sur la culture de sûreté (les britanniques en 1993 ; les allemands et les suisses en 1997). Le concept de culture de sûreté est aussi un outil efficace pour promouvoir les recherches théoriques et empiriques sur la sécurité en attirant l'attention sur des problèmes plus larges de gestion, d'organisation ou de relations inter-organisationnelles qui débordent le cadre d'analyse des approches classiques, centrées sur la question de l'erreur humaine. Dans sa récente réédition, un ouvrage précurseur (à l'époque de sa première parution, en 1978) des théories actuelles de la sécurité, décrit cette nouvelle perspective en ces termes :

« Si l'on veut s'appuyer sur la notion de culture de sûreté pour repenser la conception des institutions, il est indispensable d'aller au-delà d'une étude des attitudes individuelles en matière de sécurité et d'analyser les modes collectifs de cognition, les structures et ressources administratives qui rendent possibles – bien plus qu'elles n'entravent – le développement d'une intelligence organisationnelle, et surtout, un esprit d'inventivité en matière de sécurité. On peut considérer que ces éléments font partie d'un processus d'apprentissage en action qui ne s'achève jamais » (Turner & Pidgeon, *Man-Made Disasters*, 2nd édition, 1997: 188).

La culture de sûreté est analysée au travers de questionnaires, d'entretiens, d'analyses documentaires et d'observations ou même de méthodes d'analyse d'événements.

Les approches en termes de culture de sûreté proposent la mise en place de systèmes d'apprentissage organisationnel, qui puissent prendre appui sur les analyses d'événements ou d'incidents (*Near-Accidents*). On peut citer à titre d'exemple les bases de données d'événements comme *Synergi*. Par ailleurs des formations à l'intention des cadres ainsi que des études *benchmarking* sont proposées, toujours pour favoriser le développement d'une culture de sûreté.

En conclusion, on peut dire que les approches de sécurité systémique présentent plusieurs avantages : elles visent un apprentissage par des retours d'expérience à tous les niveaux de l'organisation et elles mettent en œuvre des méthodes d'analyse d'événements qui placent l'accent sur les facteurs organisationnels. »

3. Quelques critiques fréquentes

3.1 La culture de sûreté correspondrait à une culture unique. On reproche parfois à la notion de culture de sûreté de vouloir aligner les attitudes de tous les opérateurs sur un même modèle, le modèle supposé de la bonne culture de sûreté (voir M. Bourrier et H. Laroche, pp. 20-23, *Risques et Défaillance, approche interdisciplinaire*, CNRS-MSH, 2001). Cette critique semble correspondre à une interprétation excessivement étroite. Pourquoi ne pas concevoir, dans des pays différents, des cultures de sûreté différentes mais également efficaces ? Un ingénieur de la base de Kourou nous confiait :

- « On voit des différences considérables : les italiens essayeront tout ce qui n'est pas interdit, alors que les américains sont morts de trouille, protégés dans des scaphandres. Mais avec eux, attention aux procès... »
- « Et les français ? »
- « Les français ? Ça va... »

Magnifique aveu d'une préférence pour sa propre culture (ce qui est parfaitement légitime !), alors que dans le même temps, cet ingénieur ne voyait pas de différence notable au niveau des résultats ; il décrivait un style. La culture de sûreté n'est pas nécessairement unique.

La notion de culture de sûreté n'est pas non plus incompatible avec l'existence de conflits, par exemple entre agents de conduite et maintenance dans les centrales nucléaires, entre les personnels de maintenance au sol et les navigants des compagnies aériennes.

On ne peut exclure, pour autant, des utilisations impropres de la notion : « ... pour bon nombre d'opérateurs industriels la notion de 'culture de sûreté' a permis de reléguer au second plan toute question concernant l'organisation même des activités... » (*op. cit. p. 23*). Or, la culture de sûreté inclut explicitement, dès sa présentation dans l'INSAG 4, et de façon détaillée, les questions organisationnelles (voir chapitre 1).

3.2 La notion de culture de sûreté s'appuie sur des concepts flous. Certes. Mais, comme souligné à la section 2 ci-dessus, la notion est très utile. Elle permet de dépasser les approches technologiques de la sûreté, ainsi que les approches classiques du 'facteur humain' basées sur l'interface homme-machine et les considérations ergonomiques classiques. Plus encore, elle indique la nécessité d'approches globales.

Dans ces domaines, il reste beaucoup à faire. La notion n'est pas aboutie. Les outils restent largement à développer. Mais que l'on se reporte en arrière : toutes ces critiques auraient pu être formulées à l'encontre de la notion de 'confiance' (des consommateurs, des chefs d'entreprise). Aujourd'hui, pourtant, l'INSEE calcule régulièrement un indice de confiance des chefs d'entreprise français qui anticipe de façon intéressante les mouvements de l'économie. L'indice de confiance des consommateurs américains calculé par le MIT est très attendu et fait souvent réagir les marchés boursiers.

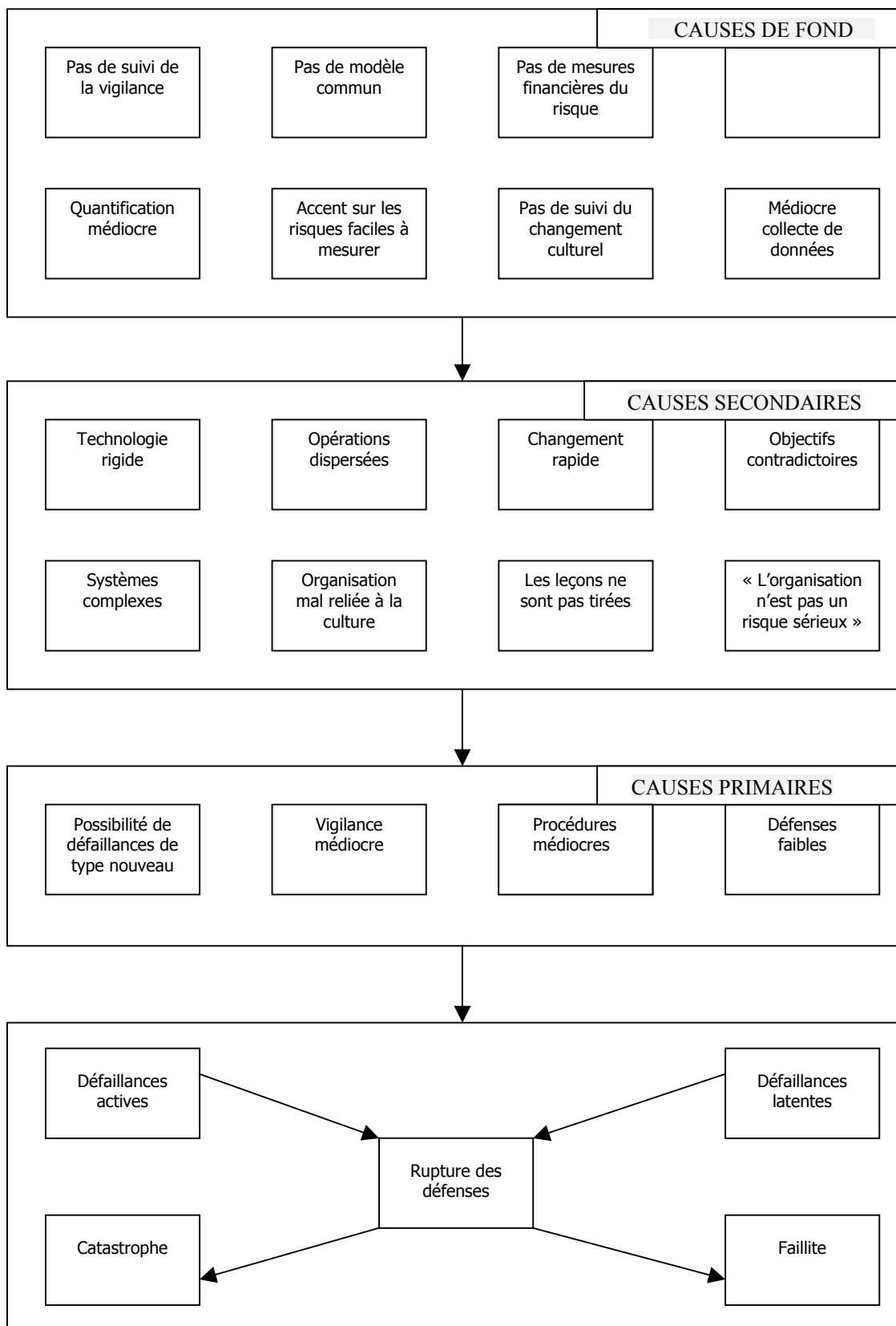
Il n'est pas impossible que la notion de culture de sûreté devienne de plus en plus claire à mesure que des indicateurs en seront développés. Il ne semble pas totalement utopique d'attendre des études sur la culture de sûreté un éclaircissement de la notion d'attitude, de norme, de valeur et de conscience (*awareness*).

3.3 La notion de culture de sûreté n'est pas opératoire. En réalité, on lui reproche à la fois d'être trop pragmatique (version nucléaire) et d'être trop générale (version universitaire). À nouveau, l'avenir rendra probablement la notion nettement plus opératoire. La notion de culture de sûreté a déjà suscité des applications pratiques. À titre d'exemple, l'annexe 2 reproduit des extraits du site Internet de la PME française Dédale active dans ce domaine ; en annexe 3, le projet britannique SCORE qui s'attache à inclure des indicateurs mesurant les attitudes relatives à la sûreté dans des modèles d'évaluation de risques.

De plus, la simple référence à la culture de sûreté évoque une façon différente de prendre les choses et contribue à approfondir la réflexion sur le risque.

4. Culture de sûreté et comportements

Où s'arrête la culture de sûreté : aux questions d'attitudes et de valeurs ? ou doit elle inclure les comportements ? Le texte de l'ACSNI parle de comportements 'qui déterminent la forme et le contenu des actions de prévention et de sécurité'. Mais quelle est la différence entre comportements et actions ? Examinons le schéma suivant (projet SCORE, p. 11).



Ce diagramme explique comment il est possible de distinguer des couches de plus en plus profondes aux causes d'un accident. La notion de culture de sûreté tente de remonter aux causes de fond. Elle se place au niveau des représentations mentales et des attitudes mentales.

De la même façon, lors d'un procès en justice on considère l'acte individuel, mais aussi les intentions. On cherchera à démontrer une succession d'actes mentaux, par exemple, dans le cas d'un crime passionnel : amour passion → jalousie exacerbée → identification d'une rivale fictive → désir d'éliminer la 'rivale' → idée du crime → incapacité de vérifier qu'il s'agit d'une vraie rivale → planification du crime → achat du poison → exécution du crime.

Le tableau ci-dessous présente les éléments du tableau précédent (sans juger de leur pertinence ni de leur ordre d'importance) sous une autre forme. Il nous semble que les comportements découlent des attitudes⁸, non seulement d'une façon directe, par exemple chez un même individu, mais aussi de façon plus indirecte, par exemple certains comportements des opérateurs sont façonnés par certaines attitudes des dirigeants qui déterminent les formes prises par le management. Dans cet esprit, la culture de sûreté comporte les attitude, mais pas seulement. Comme le dit la définition de l'AIEA, elle relève de « l'ensemble des caractéristiques et des attitudes »...

Rôle de la culture de sûreté dans la genèse des risques

Conditions générales	Management	Culture de sûreté
Conditions structurelles	Attitude profonde	Attitude profonde
Technologie rigide	Peu d'attention à la culture de l'entreprise	Médiocre attention au risque générique
Opérations dispersées	'L'organisation ne constitue pas un risque sérieux'	Pas de modèle commun de l'attitude face aux risques
Systèmes complexes		Pas de veille des risques nouveaux ou mal connus
		Peu de science du risque, peu d'intérêt pour une telle science
Autres conditions	Comportements	Comportements
Changement rapide	Organisation mal liée à la culture	Quantification, collecte des données et évaluation financière médiocres
		Accent sur les risques faciles à traiter
		Pas de suivi du changement culturel
		Pas de suivi de la vigilance
Expression concrète	Expression concrète	Expression concrète (risques)
Possibilité de défaillances techniques de type nouveau	Faible cohésion des objectifs	Vigilance médiocre
	Les leçons ne sont pas tirées	Procédures médiocres
Défenses technologiques faibles	Défenses humaines et organisationnelles faibles, défaillances latentes	

⁸ Les termes 'attitude' et 'comportement' ont une signification 'ordinaire', mais l'ensemble du tableau tend à indiquer une étiologie plus générale du risque et met en lumière la place de la culture de sûreté.

4. IMPORTANCE ET MESURE DE LA CULTURE DU RISQUE

Nous reproduisons ci-dessous un article de Carmen Rossiter publié dans *CAmagazine*, une revue de comptabilité. Cet article montre l'importance des concepts discutés ci-dessus et comment ils peuvent donner lieu à des actions de management. L'organisation peut évaluer sa culture de risque par sondage, en recueillant l'opinion des collaborateurs sur la culture et l'environnement en matière de risque, et se donner ainsi un miroir. Quatre points principaux seront examinés dans cette méthode de *PricewaterhouseCoopers* :

- les valeurs de l'organisation, sa mission et ses objectifs (leadership) ;
- la capacité à responsabiliser, à mesurer l'efficacité et à récompenser la performance ;
- le partage des connaissances et de l'information ; la promotion et le développement des compétences ;
- l'évaluation et la mesure des risques ; la capacité à prendre mettre sur pied des processus et des mesures de contrôle des risques.

Cette mesure reste probablement souvent grossière, et peut-être plus facilement praticable en Amérique que dans le contexte français. Néanmoins, elle est en mesure de discerner des disparités de culture du risque dans les services et de permettre de comparer le sentiment de maîtrise de la direction à la perception des employés. Cela répond en partie aux objections soulevées dans le chapitre précédent sur le caractère opérationnel de la notion.

Il suffit de jeter un coup d'œil aux journaux pour trouver des exemples des plus récentes victimes de la non-gestion des risques ou, à l'inverse, d'organisations qui se sont démarquées par l'excellence de leurs résultats et la qualité de leurs pratiques de gestion. Ces exemples illustrent le rôle central que jouent les pratiques de gestion des risques dans la bonne ou la mauvaise réputation d'une entreprise ou d'une organisation auprès du public.

Une gestion des risques efficace constitue la pierre angulaire du succès des entreprises, quels qu'en soient le secteur d'activité ou la taille. Cependant, pour être efficace de nos jours, cette gestion doit tenir compte des deux volets suivants : le volet comportemental, soit la réalité mouvante de la culture de l'entreprise, de son programme et de son environnement; et la réalité plus administrative de la gestion du risque. Une bonne gestion des risques nécessite à la fois une forte culture en matière de risque et un programme solide couvrant l'ensemble de l'entreprise.

Le volet comportemental de la gestion des risques, soit l'environnement et la culture en matière de risque (communément appelée «culture du risque»), est souvent tenu pour acquis, même s'il joue un rôle primordial dans la mise en place d'une structure efficace de gestion des risques. Essentiellement, la culture du risque s'entend de la façon dont les membres de la direction et les autres membres du personnel se situent par rapport aux risques, les sentiments, l'attitude et la perception de chacun en la matière influant sur la façon dont l'organisation est gérée. La culture du risque donne le ton en conscientisant les employés aux risques dans

l'exercice de leurs activités quotidiennes et la poursuite de leurs objectifs au travail.

La culture du risque désigne la capacité de la direction de reconnaître la nécessité des compétences en matière de gestion des risques. Elle englobe l'attitude de l'organisation par rapport au risque et son seuil de tolérance à celui-ci dans ses activités et ses prises de décisions quotidiennes. (L'attitude par rapport au risque est la tendance d'une entité à prendre des risques. Ainsi, il y en a qui sont réfractaires aux risques, d'autres qui ont un comportement neutre, d'autres qui prennent volontiers des risques et d'autres enfin qui recherchent des occasions de prendre des risques. Le seuil de tolérance au risque est le degré de risque maximal que l'entité juge acceptable.) Une organisation empreinte d'une forte culture du risque établit des normes et des protocoles lui permettant de repérer, d'évaluer et de gérer les risques.

Pourquoi mettre l'accent sur la culture du risque? Parce qu'elle est axée sur l'être humain, et que les organisations qui prospèrent sont celles qui savent être à l'écoute de leurs employés et canaliser leur énergie pour l'atteinte d'un but commun. Une culture gagnante est un gage de réussite pour l'organisation qui veut mettre sur pied un programme gagnant de gestion des risques et, par conséquent, atteindre ses objectifs et créer de la valeur.

Les organisations qui reconnaissent l'importance de la culture du risque analysent l'état de leur culture actuelle et vérifient si les membres de tous les secteurs partagent les mêmes valeurs. En examinant de près leur culture du risque et leur environnement en matière de risque, elles parviennent à repérer les lacunes et à identifier les secteurs qui ne sont pas sur la même longueur d'ondes. Elles peuvent ensuite concentrer leurs énergies et leurs ressources sur l'élimination des disparités et la création d'une culture plus homogène et, par le fait même, renforcer leur culture du risque.

Il faut au départ une forte culture du risque pour mettre en place une structure de gestion des risques permettant de gérer les dangers et les opportunités issus d'un environnement mouvant. À l'inverse, une culture du risque faible rend l'organisation plus susceptible de frapper les écueils, ou de les éviter de peu, et de manquer des occasions.

La culture et le comportement étant des caractéristiques qui ne se mesurent pas avec précision, comment peut-on évaluer la force de la culture en matière de risque? L'une des méthodes d'évaluation les plus efficaces et efficientes consiste à effectuer un sondage qui, en recueillant l'opinion de chacun sur la culture et l'environnement en matière de risque, tend un miroir à l'organisation.

Il s'agit fondamentalement d'un sondage de 60 questions accessible sur Internet au moyen d'un mot de passe. Les employés peuvent accéder à ce site 24 heures sur 24 pendant deux ou trois semaines, dans l'anonymat. Les questions peuvent prendre la forme d'énoncés standard envers lesquels les répondants sont appelés à exprimer leur accord ou leur désaccord sur une échelle de 1 à 5. De plus, chaque question peut comporter une section réservée aux commentaires.

Les employés réagissent généralement bien à ce type de sondage, car il permet de garder l'anonymat. De plus, nombreux sont ceux qui fournissent des explications et des commentaires dans la section réservée à cette fin. Cette section non structurée leur donne l'occasion de préciser leur pensée et facilite l'analyse des résultats.

Ce genre de sondage livre un message clair à la direction étant donné qu'il transmet l'opinion de chaque employé sur la culture du risque de l'organisation ainsi que les moyens de la renforcer. Par conséquent, peu de place est laissée à l'interprétation.

Les questions sont conçues pour sonder les quatre principaux attributs d'une culture du risque solidement enracinée : leadership et stratégie; responsabilisation et renforcement; ressources humaines et communications; gestion des risques et infrastructure. L'attribut leadership et stratégie a trait aux valeurs qui sont véhiculées dans l'ensemble de l'organisation ainsi qu'à la mission de l'entreprise et à ses objectifs. L'attribut responsabilisation et renforcement porte sur la capacité de responsabiliser chacun des employés, et de mesurer et de récompenser le rendement. L'attribut ressources humaines et communications dénote, lui, la capacité de partager des connaissances et de l'information ainsi que de promouvoir et de développer les compétences des employés. Finalement, l'attribut gestion des risques et infrastructure afférente a trait à la capacité d'évaluer et de mesurer les risques et de prendre les mesures nécessaires pour mettre sur pied des processus et des mesures de contrôle.

Chacun de ces attributs se subdivise en sous-attributs, qui se subdivisent en indicateurs clés évalués à l'aide de questions particulières. Le fait de catégoriser ainsi les questions facilite l'analyse des résultats et leur comparaison subséquente avec le profil que des organisations bien gérées devraient présenter en matière de culture du risque.

Étant donné que les résultats varient d'une organisation à l'autre, le sondage peut avoir des effets divers. Il peut confirmer la haute direction dans son opinion ou la forcer à se remettre en question et à réagir. À tout le moins, il fait ressortir les forces et les faiblesses de la culture du risque ainsi que les secteurs à surveiller.

Les résultats de ces sondages peuvent varier considérablement, allant de la médiocrité à l'excellence selon l'organisation et la culture du risque qui y est véhiculée. De même, le taux de participation peut être aussi bas que 30 % ou aussi élevé que 85 %. Il est intéressant de noter qu'il existe une corrélation entre le niveau des résultats globaux et le taux de participation, ce qui indique que le personnel des organisations dotées d'une forte culture du risque est plus intéressé à participer aux sondages, à exprimer son opinion et à suggérer des améliorations.

Les résultats du sondage peuvent être comparés aux résultats similaires obtenus par des organisations phares afin de faire ressortir les points forts, les points faibles et les points à améliorer.

Les organisations qui ont le profil idéal se démarquent sur le plan du leadership et de la stratégie, car elles reconnaissent que la culture

d'entreprise prend naissance dans le ton et dans l'orientation donnés par les hauts dirigeants. L'exemple venant du sommet de la hiérarchie indique les attentes réelles en matière de comportement. Les dirigeants et les employés doivent se conformer à ces attentes en tout temps, même dans les situations difficiles. Tous devraient avoir une idée précise de l'orientation qu'ils doivent prendre et comprendre le rôle qu'ils doivent jouer dans la poursuite des objectifs de l'organisation. L'organisation devrait également établir des lignes directrices pour régir ses principaux risques et activités.

Un mauvais score à ce sujet dénote de graves lacunes dans les orientations données par les hauts dirigeants ou, pire encore, un manque de conviction de leur part dans la mise en pratique des valeurs.

Le score devrait également être élevé au chapitre de la responsabilisation et du renforcement, montrant une bonne compréhension des objectifs individuels et un sens marqué des responsabilités, renforcé par des politiques de ressources humaines. Toutefois, dans certaines organisations, bien que les tâches et les responsabilités quotidiennes soient définies, aucun objectif individuel n'est fixé pour guider l'employé dans ses réalisations et l'atteinte des résultats. Il s'agit d'une grave lacune : les employés doivent savoir quelle direction emprunter et ce qu'on attend d'eux pour pouvoir atteindre un résultat particulier. De même, ils ont besoin de savoir qu'ils poursuivent des objectifs qui s'intègrent bien à ceux de l'organisation et qui visent l'atteinte d'objectifs communs.

Au chapitre des ressources humaines et des communications, le score varie en fonction de l'infrastructure de l'entité et de sa capacité d'adaptation aux changements. Dans bon nombre d'organisations, les résultats du sondage dénotent une infrastructure d'exploitation déficiente sur le plan des ressources humaines, des procédés ou de la technologie, ou montrent que l'infrastructure principale est en place, mais qu'elle n'est pas efficace ou qu'elle ne peut répondre en temps opportun aux nouveaux besoins de l'entreprise. De plus, les procédures d'information et de communication sont souvent perçues comme un soutien d'une efficience et d'une efficacité douteuses.

Les résultats au chapitre de la gestion des risques et de l'infrastructure afférente indiquent habituellement qu'il y a place à l'amélioration, particulièrement dans les organisations qui n'ont pas encore opté pour une gestion globale des risques. Les résultats indiquent la plupart du temps que les gestionnaires sont disposés à échanger sur la gestion des risques, mais qu'aucun cadre, processus ou outil structuré n'a été mis en place pour le repérage, l'évaluation et la gestion des risques et la communication d'informations à leur endroit. En effet, les risques sont, dans la majorité des cas, gérés dans le cadre d'un projet particulier mis sur pied en vue de réagir à une crise ou à une menace. Les organisations éclairées adoptent une approche plus proactive vis-à-vis des risques non seulement en cherchant à éviter les dangers, mais également à profiter des opportunités qui les accompagnent.

Il est intéressant de constater que, bien que la plupart des organisations se disent «en contrôle», les répondants expriment souvent des doutes quant à l'efficience et à la fiabilité des modes de fonctionnement de leur

entreprise pour faire face au niveau de changement et de complexité du monde des affaires de demain. Essentiellement, les répondants se sentent «en contrôle» aujourd'hui, mais ne sont pas certains de le demeurer.

En plus de situer l'organisation par rapport à la meilleure pratique, le sondage permet de vérifier si la culture du risque est uniforme. La comparaison des résultats obtenus dans différents secteurs de l'organisation est à ce titre extrêmement éclairante. Les sondages sont généralement conçus en fonction de deux ou trois niveaux de stratification qui correspondent aux regroupements les plus pertinents comme la division, l'échelon hiérarchique ou l'emplacement géographique. La comparaison des résultats de ces différents segments permet à la direction d'apprécier les variations dans la culture du risque et de repérer les secteurs problématiques.

Avec la vogue des fusions et des acquisitions, il n'est pas surprenant que des disparités culturelles existent dans bon nombre d'entreprises. Tout comme les questions de culture peuvent entraver la conclusion d'une entente, elles peuvent avoir un effet désastreux sur la capacité d'un groupe de gérer globalement ses risques de façon efficace.

Effectuer un sondage n'est pas difficile en soi. Le véritable défi réside toutefois dans le partage des résultats avec les répondants et, surtout, dans la prise de mesures appropriées. L'organisation qui relèvera ce défi profitera au maximum des efforts consacrés à sa culture du risque et à son environnement.

Carmen Rossiter est directrice au sein du Groupe des solutions pour la gestion globale des risques du cabinet PricewaterhouseCoopers à Toronto.

Cette chronique est dirigée par Peter Jackson, CA, consultant de Toronto en performance organisationnelle et gouvernement d'entreprise.



avril 2001 — ÉDITION IMPRIMÉE

5. CULTURE DU RISQUE ET CULTURE DE SÛRETÉ

ESSAI DE DÉFINITION, POSITION DES NOTIONS

Après avoir exposé et discuté quelques définitions de la culture de sûreté dans les quatre chapitres précédents, il nous a semblé indispensable d'en donner nous-même une définition. Non pas pour ajouter à une liste qui serait peut-être longue si elle devait être exhaustive, mais pour fixer les idées. Nous remontons à la notion de culture du risque pour bien situer celle de culture de sûreté.

Définition de la culture du risque dans une organisation donnée

La notion de culture du risque a été particulièrement développée dans le secteur financier. En dehors de ce secteur, elle est peut-être plus commune aux risk managers qu'aux nombreux responsables de la sûreté qui seraient, pour leur part, plus familiers de la notion de culture de sûreté. La définition ci-dessous s'inspire des positions exprimées dans le monde financier, par exemple dans le chapitre précédent :

La culture du risque est la façon de penser, de ressentir et d'aborder le risque dans l'organisation concernée. C'est la fondation mentale sur laquelle se bâtit le risk management. Elle est donc essentielle.

Ainsi, quand nous envisageons la culture du risque, nous ne nous intéressons pas à la gestion de risque elle-même, à la technique du risque, mais au choix réalisés en amont de la technique et qui déterminent très largement les conditions de l'exercice de celle-ci.

La façon de penser, de ressentir et d'aborder le risque dans l'organisation, c'est la juxtaposition des vues, des sentiments et des façons de vivre le risque de l'ensemble des membres de l'organisation. De cette complexité, on ne retient, par nécessité, que les éléments principaux : les principaux points communs et les principaux clivages. Autrement dit, analyser la culture du risque c'est préciser ce qu'il y a de commun dans les façons de penser, de ressentir et d'aborder le risque de différents sous-groupes relativement homogènes à cet égard, ainsi que le jeu de ces différentes sous-cultures de risque dans les interactions des différents sous-groupes au cours de leurs activités.

À nouveau, la culture du risque n'est pas la pratique ou la technique du risque. Elle en est la fondation mentale. Elle se situe en amont des pratiques et des techniques. Elle est plus délicate à concevoir et à repérer, mais elle joue un rôle crucial.

Il est clair que la culture du risque des dirigeants joue un rôle considérable. Elle modèle la culture du risque de l'ensemble des membres de l'organisation. Elle peut promouvoir une politique proactive de gestion de tous les risques et améliorer globalement toute la culture du risque des employés. Le choix de privilégier certains risques, volontairement ou par ignorance de risques inconnus, aura des effets spécifiques dans la culture du risque et dans les pratiques opérationnelles (cas de la mine de Moura en Australie, voir note D1-02-005, *La prévention des catastrophes n'est pas impossible*). Enfin, une culture du risque inexistante chez les dirigeants ne pourra que peser négativement sur la mission des responsables chargés de gérer les divers types de risque.

Repérage de la culture du risque

La culture du risque pourrait être repérée, au sein d'une organisation, par la réponse aux questions suivantes que pourraient se poser les membres de l'organisation :

- Quels sont nos risques ?
- Quelle est l'importance relative de nos risques (d'un point de vue subjectif) ?
- Quelle quantité de risque sommes-nous prêts à prendre ?
- Comment traitons-nous les risques que nous acceptons de prendre ?

1. *Quels sont nos risques ?* L'identification des risques serait ici très large. Au delà d'une liste fixée et brève (cas classique de nombreuses entreprises), au delà de réponses oui/non à une vaste liste d'événements possibles jugés risqués ou pas (qui pourrait être issue d'une prestation de cartographie des risques par un grand cabinet de *consulting*), elle attribuerait un coefficient plus général, compris entre 0 et 1, à tous les événements imaginables (et inimaginables !) : 0 pour les événements jugés non risqués, 1 pour les événements certainement risqués, et un coefficient entre 0 et 1 pour les autres, en fonction de la vraisemblance qu'ils représentent, en effet, un risque.

Il pourrait y avoir une question antérieure : penser, ressentir et aborder nos risques est-il légitime et nécessaire ? La réponse dépendrait des risques et serait plus complexe que oui ou non (0 et 1). Elle conduirait donc, à nouveau, à un coefficient du type de celui que l'on vient de mentionner.

Une autre interrogation concerne le 'nous' de 'nos' risques. En cas de réalisation du risque considéré, serons-nous considérés comme responsables (civilement et/ou pénalement) ? Ou bien, du point de vue de notre éthique, devons-nous prendre responsabilité pour tel risque donné ? Ici encore, un coefficient compris entre 0 et 1 pourrait définir si les risques sont 'nôtres' ou de notre responsabilité.

Au total, il nous semble que ces réponses pourraient être résumées en un seul coefficient. La première question de la culture du risque recouvrirait donc à la fois la conscience des risques et leur légitimité en tant qu'éléments à prendre en compte.

2. *Quelle est l'importance relative de nos risques (d'un point de vue subjectif) ?* Il ne s'agit pas d'évaluer objectivement les dommages associés aux risques (cela relèverait de la technique du risque), mais de donner un poids subjectif à ces dommages. Par exemple, il est de notoriété publique que l'énergie nucléaire a causé des dommages faibles en France depuis vingt ans (zéro mort violente connue, présomption de cancers pour certains ouvriers), alors que sur la même période les accidents de la route ont causé plus de 150 000 morts et de très nombreux blessés graves. Pourtant, l'émoi causé par la violence routière a longtemps été relativement faible par rapport à la violence de l'agitation qui entoure le nucléaire. Les poids subjectifs de ces deux types de dommages sont donc *très* différents. Autrement dit, tous les morts ne se valent pas : les morts du

nucléaire sont beaucoup plus chers. Dans le même ordre d'idées, « le mort coûte plus cher en gros » : les journaux et les tribunaux font « payer plus cher » les accidents isolés groupant beaucoup de morts, par exemple les accidents d'avions, que les accidents diffus tuant régulièrement.

Ce poids subjectif pourrait être plus variable dans le temps, pour une organisation donnée, que le coefficient de la question précédente. Il serait donc utile de distinguer ces deux pondérations.

3. *Quelle quantité de risque sommes nous prêts à prendre ?* Il ne s'agit pas de savoir si les risques pris sont correctement payés (cette question relève de la technique du risque et non de la culture du risque), mais si l'organisation souhaite prendre des risques (qui seraient, a priori, correctement payés) ou au contraire limiter fortement ses risques. Autrement dit, sommes nous averses au risque, neutres face au risque, ou au contraire sommes-nous risquophiles, recherchons nous un style 'sportif' ? (Sachant que dans le style sportif, l'évaluation des risques est, en général, à la fois plus cruciale et plus difficile. C'est donc un style généralement plus exigeant : le coût de la vitesse, en quelque sorte.)
4. *Comment traitons-nous les risques que nous acceptons de prendre ?* À nouveau, il ne s'agit pas de la question technique, mais du choix de style de gestion de risque. Par exemple, « notre métier n'est pas le risque, nous nous en remettons aux assurances », ou bien « nous utiliserons massivement la technologie », ou encore « seule la vigilance du personnel nous protégera contre la diversité des risques ».

Ces quelques idées sur le repérage de la culture du risque développent le quatrième point du sondage évoqué au chapitre précédent, en insistant sur l'aspect culture par rapport à l'aspect techniques de traitement des risques. Les trois premiers points de ce sondage (valeurs, organisation, communication et formation) pourraient être conservés à titre de repérage de la culture globale de l'entreprise, car, bien évidemment, celle-ci est le terrain dans lequel se développe la culture du risque.

Un consultant spécialisé en 'facteur humain' nous confiait :

Alors que nous discutons, dans une entreprise, notre proposition de services visant à réduire les risques en améliorant les aspects liés aux facteurs humains, un spécialiste de la direction financière nous a demandé :

— « Pourquoi ceci nous concerne-t-il ? Pourquoi ne pas nous assurer, tout simplement ? »

Qu'est-ce que je peux lui répondre ?

Dans cette situation, le spécialiste du facteur humain, avec sa culture professionnelle, sa connaissance intime des questions de risque, se sent totalement démuné en face d'une culture du risque à ce point différente de la sienne qu'elle ignore pratiquement tout des enjeux du risque sur le terrain, particulièrement l'importance cruciale du facteur humain.

Force de la culture du risque

Une organisation dotée d'une forte culture du risque s'engage à *connaître et traiter* ses risques, par exemple en établissant des normes et procédures destinées à identifier, évaluer et gérer les risques. L'exploration systématique des quatre questions ci-dessus (et plus généralement de toute question liée au risque) fait progresser la culture du risque. En revanche, la réponse à ces questions est souvent peu explicite quand la culture de risque est faible.

Il est généralement reconnu qu'une bonne culture du risque se fonde sur une certaine homogénéité des sous-cultures. Au moins deux raisons vont dans ce sens : la force de l'organisation est celle de son maillon le plus faible ; une culture du risque homogène permet de calibrer les mesures de traitement du risque, par exemple d'adapter les procédures, de créer un langage commun, etc. Ce qui ne veut pas dire qu'il ne peut pas y avoir une part de l'organisation beaucoup plus sensible aux risques : une inspection interne draconienne ou d'un service d'audit intraitable ou d'un régulateur très pointilleux.

Intérêt d'une amélioration de la culture du risque

Au delà de la gestion des risques elle-même — le fait d'éviter des pertes et de garantir la continuité de l'organisation —, renforcer la culture du risque est profitable à l'organisation. Pourquoi ? Parce que les organisations qui réussissent sont celles qui parviennent à séduire les cœurs, captiver les esprits et diriger l'énergie de leur employés à la réalisation d'un but commun. La culture du risque est un élément de cette culture plus large. L'aborder systématiquement par des questionnaires, des séminaires, des formations ou de toute autre façon contribue à améliorer de façon légitime la culture de l'organisation en général, l'intelligence du risque en particulier.

De plus, une bonne culture du risque améliore généralement la qualité, élément reconnu du succès d'une entreprise (voir chapitre 19).

La culture de sûreté

Alors que la culture du risque concerne l'ensemble de l'organisation et l'ensemble de ses activités, le terme de culture de sûreté semble plutôt réservé au domaine HSE : Hygiène, Sécurité (ou sûreté, en tous cas *safety* en anglais⁹), Environnement. La sûreté n'est concernée qu'indirectement par le risque de malversation (criminalité en col blanc), le risque de change, le risque Internet, etc. La discipline HSE est une partie de la gestion globale des risques. Le responsable HSE n'est pas, en général, le risk manager, encore moins le responsable des risques financiers.

⁹ En anglais, ce terme réfère d'abord au risque d'accidents du travail ; il va donc naturellement de pair avec '*hygiene*'. Il désigne aussi, plus généralement, le risque technologique. En français, le terme sûreté réfère au risque technologique dans le secteur nucléaire, mais au risque 'sécuritaire' dans l'aviation ; alors que le terme sécurité désigne dans le nucléaire l'aspect protection policière des installations, il désigne le risque technologique dans l'aviation...

Un critère de distinction envisageable : les victimes potentielles d'une faible culture de sûreté seraient les employés (particulièrement les opérateurs exposés au risque), les riverains et l'environnement. Alors que les actionnaires sont directement exposés à un défaut de culture du risque, ils ne sont qu'indirectement affectés par un défaut de culture de sûreté. Par ailleurs, quand la victime potentielle est un client qui subit des dommages en raison d'un produit défectueux, on parlera plutôt de défaut de la qualité que de défaut de la culture de sûreté.

Nous proposons donc la définition suivante :

La culture de sûreté est la partie de la culture du risque qui se rapporte à la technologie utilisée par l'organisation considérée, spécialement à ses usages risqués pour les employés, les riverains, l'environnement.

On distinguera au moins la culture de sûreté des dirigeants et celle des personnels directement exposés. En effet, la sûreté présente le plus souvent un aspect technique difficile d'accès qui marque fortement le vécu des personnels. Il s'agit de technicité pure, mais aussi de normes, de règlements et de procédures. Il est maîtrisé par certains responsables, mais demeure assez étranger à la direction. Ce vécu de l'usine, de la centrale nucléaire, du porte-avions, de l'hôpital, etc., représente l'essentiel de la culture du risque de ces personnels. Pour eux, grosso modo :

culture du risque = culture de sûreté.

En revanche, la culture de sûreté des dirigeants ne représente qu'une faible part de leur culture du risque ; ils doivent traiter de nombreux autres risques, dans des styles de culture et d'action très différents (voir chapitre 12).

Si cette vue est correcte, il ne faut pas s'étonner de la différence de style entre dirigeants et responsables directs en matière de sûreté. On ne saurait donc aborder de la même façon les questions de sûreté chez ces deux types d'interlocuteurs.

6. EXEMPLE DE DÉFAUT DE CULTURE DU RISQUE

INONDATION À ARAMON (GARD) LE 10 SEPTEMBRE 2002

L'article ci-dessous décrit la rupture de la digue sur le Gardon à Aramon. L'impréparation de tous les acteurs est éclatante (y compris les services départementaux qui ne sont pas mentionnés).



«Ca ne devait pas arriver»

Derrière ses deux digues, Aramon, près d'Avignon, se sentait en sécurité. Lundi soir, la crue y a fait au moins 4 morts.

Par Michel HENRY
mercredi 11 septembre 2002

Aramon (Gard) envoyé spécial

Aramon, 14 kilomètres au sud d'Avignon, on ne s'attendait à rien, lundi soir. Malgré les pluies diluviennes du week-end, malgré les inondations partout alentour. Geneviève la coiffeuse raconte qu'elle s'installait devant la télé pour voir un feuilleton au nom de fleuve, *Garonne*. Elle ne pensait pas au Gardon, en folie, descendant des Cévennes. Une amie lui a téléphoné de Paris, inquiète. Geneviève l'a rassurée : pas de risque, à Aramon, avec les deux digues, l'une sur le Rhône, l'autre pour protéger du Gardon. Et puis sa mère, qui habite la commune, l'a appelée : «Geneviève ! L'eau ressort par les égouts !»

Sonne le glas. Dans ces cas-là, on dit que «le Rhône n'en veut plus» et comme ça arrive souvent, on ne s'inquiète pas. Geneviève a quand même téléphoné au maire : «Dis, Jeannot, tu pompes ? Si je pompe ?, a-t-il répondu. Mais ma pauvre Geneviève, y a pire que ça : l'eau est passée au-dessus de la digue !» Vers 20 h 30 ou 21 heures, la mairie a fait sonner la cloche, pour prévenir. Trop tard. Une dame soupire : «Le glas ? Je ne l'ai pas entendu. Je regardais les inondations à la télé.» Quelques minutes plus tard, l'eau rentrait

chez elle. Chez Geneviève, les flots n'ont rien demandé : «J'ai une barre à la porte, l'eau m'a cassé la porte. Je suis partie au galop. Comme ça. Sans rien.»

Lentement, sans grand débit, l'eau est montée jusqu'à trois mètres par endroit. Le Rhône en crue empêchait le Gardon en crue de se déverser, le Gardon s'est retourné vers le village et «il nous est tombé dessus», raconte un exploitant agricole. *J'ai monté tout mon matériel sur des palettes à 2,50 mètres. Mais l'eau est montée à 3,50 mètres. De mon hangar, on ne voit plus que le toit. Une dame a voulu aller chez ses parents, chercher des affaires. Emportée. Elle a appelé "au secours, au secours", et puis plus rien. Ça montait sans bruit, comme si ça sortait du sol. La plus longue nuit de notre vie.»* Les voitures, vides, glissaient sur les flots, s'engouffraient dans les ruelles, avec le courant. «Une voiture est venue exploser la vitrine de la boulangerie, raconte un employé municipal. Ça sentait le gas-oil, l'essence. Effrayant. On entendait les gens crier dans les petites rues. Tout le monde gueulait. Mais impossible d'y aller, avec la barque. Trop de courant. J'ai dit à mon collègue : "Si on y va, ça fait deux de plus sur la liste."»

Colère. Les hélicos ont tourné toute la nuit pour récupérer les gens sur les toits. Ceux qui ont encore les pieds au sec les hébergent. Au matin, tous les lotissements sont dans l'eau jusqu'au premier étage. Deux tiers des 3 800 habitants sont touchés par l'inondation. Abattement ou colère, la petite ville se scinde en deux. Il y a ceux qui accablent le maire : «A la mairie, ils n'y ont pas cru, et après, ils ont été dépassés», se plaint un homme. «Jeannot [le maire] disait "c'est pas possible que la digue pète". Elle a pété», râle un autre. Il y a ceux qui le soutiennent : «C'est la faute à personne, dit une dame en rose. Il fallait qu'on l'ait, c'est tout. C'est la fatalité.»

Il flotte une sale odeur de mazout. Devant le traiteur, qui s'appelait Le Paradis, un homme pleure. A côté, un gamin joue au foot dans 50 cm d'eau. Un autre réclame à son père «une boîte pour sauver [ses] escargots». Une dame hèle son voisin : «Et les chevaux ? J'ai pas pu les sauver. Ils étaient enfermés dans le box.» Derrière la voie ferrée, la gendarmerie est sous trois mètres d'eau. Comme la maternelle, à côté. Les gens circulent en barque. Au centre-ville, sur un mur, une plaque à trois

mètres de haut indique : «Rhône 31 mai 1856.» Mais la référence, ici, c'est 1935. «Ah moi, j'ai vécu 1935, raconte un vieux. Et 1958 : un gros Rhône, mais les digues n'avaient pas cédé comme maintenant.»

Larmes. Accablé, se restaurant d'une banane au collège qui sert de PC, le maire, Jean Mahieu, reconnaît : «On n'a pas pu prévenir la population. Du coup, tout le monde n'est pas parti. Et ceux qui ne sont pas partis figurent forcément parmi les victimes.» Il est 13 heures hier, l'eau baisse et le maire, 54 ans, pleure. «Officiellement, on a cinq victimes déjà, sanglote-t-il. Et des disparus.» (1) La tête dans les mains, le maire explique : «A 16 heures, lundi, on a eu un bulletin de décrue à Remoulins [en amont]. Ça ne laissait pas présager d'une énorme vague quatre heures plus tard. On pensait à une crue normale. Mais c'est passé par-dessus, et la digue a cédé, une brèche de 25 mètres. Peut-être la digue n'est pas suffisante. Peut-être est-elle mal entretenue depuis trente ans. Mais on pensait que ça n'arriverait pas.»

(1) Selon la préfecture, il y avait hier soir 4 morts et 4 disparus.

© Libération

La comparaison avec les recommandations de la Commission Internationale pour la Protection du Rhin (chapitre 10) n'est guère flatteuse. Elle a le mérite d'indiquer clairement les priorités en termes de politiques de gestion du risque inondation.

Nous reproduisons ci-après des extraits du rapport de cette commission (avec le caractère d'origine, entre guillemets, essentiellement dans la colonne de droite). En regard, certains extraits de l'article figurent (avec leur caractère d'origine). Il en ressort un état d'impréparation et d'ignorance du danger qu'une bonne culture du risque ne pourrait laisser subsister. Nous soulignons avec quelques commentaires en italique.

Inconscience du risque

« **Connaître l'aléa** et ses paramètres essentiels tels que la probabilité, la nature et l'intensité de l'impact est une condition préalable à la prévention des dommages. »

« Ces connaissances doivent être transmises à tous les acteurs avec la crédibilité requise. »

« **Conscience de l'aléa.** Prendre conscience de l'aléa signifie l'avoir reconnu, le savoir latent, ne pas l'oublier ni le refouler, et le prendre dûment en considération dans ses actions. »

« Les crues doivent être considérées comme faisant partie de notre environnement. Le particulier doit se savoir le premier concerné. S'il n'a pas encore vécu d'inondation, il doit être informé. »

« Cette conscience du risque doit être maintenue éveillée par l'information et la formation. Le niveau des dommages potentiels détermine la priorité et l'étendue des mesures. »

À Aramon, 14 kilomètres au sud d'Avignon, on ne s'attendait à rien, lundi soir. Malgré les pluies diluviennes du week-end, malgré les inondations partout alentour.

Pourtant, les orages cévenols sont parfaitement connus. La mémoire en est présente :

Au centre-ville, sur un mur, une plaque à trois mètres de haut indique : «*Rhône 31 mai 1856.*» Mais la référence, ici, c'est 1935. «*Ah moi, j'ai vécu 1935, raconte un vieux. Et 1958 : un gros Rhône, mais les digues n'avaient pas cédé comme maintenant.*»

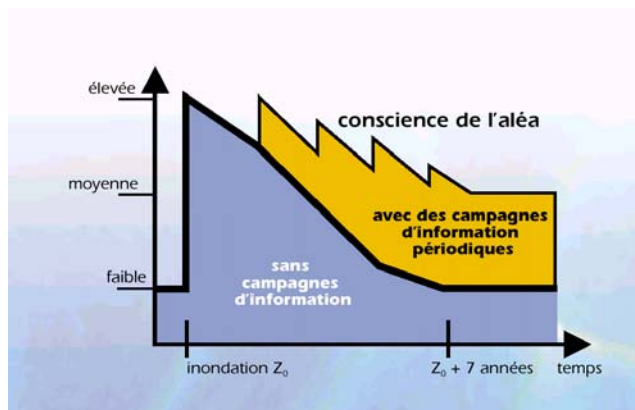
Malheureusement, cette connaissance n'est pas reconnue comme un élément fondamental de la culture du risque. Elle n'a aucune effet sur la vigilance :

Jeannot [le maire] disait "c'est pas possible que la digue pète". Elle a pété.

Il ne semble pas que les autorités concernées aient signalé la possibilité de rupture de digue ou la nécessité de surveillance. C'est l'ignorance qui règne.

« Peut-être la digue n'est pas suffisante. Peut-être est-elle mal entretenue depuis trente ans. »

La nécessité d'entretenir la conscience du risque



« La conscience de l'aléa est très forte chez les personnes touchées juste après une crue. Lorsqu'il n'y a pas de crue, la conscience du danger latent diminue. On peut maintenir à un niveau élevé la conscience de l'aléa par le biais de manifestations d'information périodique

Impréparation à la crise

« Protection des personnes. Les pertes en vies humaines sont souvent imputables à un mauvais comportement. Des refuges sûrs doivent être accessibles rapidement. La prise de conscience de l'aléa et la connaissance de l'accès aux refuges sont indispensables. »

Une dame soupire : «Le glas ? Je ne l'ai pas entendu. Je regardais les inondations à la télé.»

Ampleur de l'inconscience !

J'ai monté tout mon matériel sur des palettes à 2,50 mètres. Mais l'eau est montée à 3,50 mètres.

Impuissance.

«On n'a pas pu prévenir la population. Du coup, tout le monde n'est pas parti.» (En fait, tout le monde a été pris de court). «Officiellement, on a cinq victimes déjà, sanglote-t-il. Et des disparus.»

«A 16 heures, lundi, on a eu un bulletin de décrue à Remoulins [en amont]. Ça ne laissait pas présager d'une énorme vague quatre heures plus

Faible niveau de gestion de crise

Tant que la gestion volontariste de la culture du risque ne sera pas acquise, on peut s'attendre à d'autres épisodes de ce type. La rupture de digue fait partie des scénarios bien connus de crise en cas d'inondation. L'alerte avait été donnée par Météo France. Comme dans l'Aude en 1999, on n'a pas su y réagir dans les services. Aucune vigilance particulière n'est recherchée chez la population.

Avec ce type de 'culture', on peut s'attendre à une mobilisation dans les semaines suivant l'événement, puis à un repli face aux difficultés. Ensuite, on fera tout pour oublier. Ainsi, le Préfet du Gard pouvait-il déclarer :

« Je n'ai pas le sentiment que la réaction a été minable, mais l'événement échappait à tout ce qu'on avait l'habitude de vivre. » Ou encore :

« L'événement climatique qui a touché le Gard est le plus fort qu'ait connu la France (sic !) avec des précipitations d'une violence inconnue. »

tard. On pensait à une crue normale.

II - INTELLIGENCE DU RISQUE

La partie précédente a éclairé les notions de culture du risque et de culture de sûreté et montré qu'une bonne culture du risque implique une exigence d'intelligence et de connaissance des risques. C'est cet aspect qu'aborde maintenant cette deuxième partie, en commençant assez naturellement par le secteur nucléaire, un secteur généralement en avance dans ce domaine — pour d'excellentes raisons, évidemment.

Les concepts de la sûreté nucléaire (chapitre 7) comportent notamment : la défense en profondeur, une attitude de prudence et de pessimisme dans l'étude des accidents possibles, un retour d'expérience systématique, des études probabilistes de sûreté. Dans l'ensemble, on constate que les concepts ont nettement évolué depuis les premières études de sûreté. Le domaine de la sûreté n'a acquis sa légitimité et sa maturité actuelle que de façon progressive. Pour réduire la complexité des tâches, on avait commencé par se donner un champ d'investigation et des hypothèses trop restreints. En particulier, les études, conduites par des ingénieurs, ont eu tendance à privilégier les aspects les plus 'nobles' d'un point de vue d'ingénieur en négligeant parfois certains aspects qui auraient été jugés essentiels par un risk manager. La prise en compte des facteurs humains s'est développée de façon progressive dans les études probabilistes de sûreté.

D'une façon générale, la sûreté est largement inscrite dans la connaissance et l'intelligence des risques — au niveau global de 'la' connaissance, mais aussi dans l'intelligence spécifique des risques dans tel établissement, telle équipe ou chez telle personne. Dans cette optique, une gestion de la sûreté qui se donne pour objectif de satisfaire à minima les normes en vigueur ne développe pas la culture de sûreté. Si elle a pour résultat de faire diminuer l'intérêt porté aux questions de sûreté, de limiter la connaissance et les échanges d'information à ce sujet, on peut considérer qu'elle est dangereuse. Cette vision est esquissée au chapitre 8.

Le chapitre 9 développe cette analyse dans le cas de l'aviation civile. Dans ce secteur, la responsabilisation des compagnies est un maître mot du contrôle. Evidemment, les accidents y sont excessivement coûteux et, d'une façon générale, les compagnies sont motivées à développer la sécurité de leurs opérations. Cette responsabilisation amène à superviser le système de gestion de la compagnie et non les opérations elles-mêmes. Les systèmes d'information jouent un rôle capital et, dans de nombreuses compagnies, l'on procède maintenant à l'analyse systématique des 'boîtes noires'. La gestion de l'inspection et de la formation joue un rôle important. Aux côtés des opérateurs (les compagnies aériennes), les constructeurs d'aéronefs sont tenus de suivre leurs produits pendant toute la durée de vie de ces derniers.

L'intelligence du risque se décline évidemment dans une multitude de secteurs, avec des spécificités parfois très marquées, le cas de l'aviation restant probablement représentatif et utile pour de nombreux autres secteurs. Il serait passionnant de couvrir une grande partie de ces efforts, mais cela dépasserait le cadre de cet ouvrage. On a voulu signaler, néanmoins, un travail assez remarquable dans le domaine du risque inondation, un domaine important en raison du poids économique des dommages et du fait qu'il relève non pas d'entreprises privées comme les compagnies d'aviation, mais d'un ensemble d'acteurs publics. Ce rapport de la Commission Internationale pour la Protection du Rhin incarne un véritable effort d'intelligence et de diffusion de la culture du risque dans ce domaine. On ne peut qu'en recommander la lecture complète, le chapitre 10 se contentant ici d'y introduire le lecteur.

7. L'ÉVOLUTION DES CONCEPTS DE LA SÛRETÉ

À PARTIR DE L'EXPÉRIENCE DU NUCLÉAIRE

La sûreté nucléaire, ce domaine d'excellence de la sûreté, a dégagé et systématisé une approche de la sûreté dont de nombreuses leçons sont transférables à d'autres domaines à risques¹⁰. Les méthodes de la sûreté nucléaire se sont enrichies progressivement. Dans un domaine où il faut quelques dix années pour passer des résultats théoriques à l'application pratique sur les installations, les progrès proviennent de réflexions et d'études systématiques, ou bien de révisions sous la pression des événements. Mais « les événements graves n'ont jamais fait découvrir d'aspects de sûreté inaccessibles à l'analyse « à froid ». Ils ont fait engager des réflexions que rien n'empêchait sinon une trop grande confiance en soi » (J. Libmann).

La défense en profondeur

Le concept de barrières a rapidement cédé la place à celui de **défense en profondeur**. Chaque niveau de cette défense est comme une barrière largement étanche, mais pas totalement ; les incidents qui ne sont pas éliminés à un niveau doivent être presque tous stoppés au niveau suivant. Ce sont :

1. **prévention** des anomalies et des défaillances par un niveau de **qualité** très exigeant ; cette démarche implique au préalable de définir clairement le fonctionnement normal et ce contre quoi on veut se prémunir ;
2. **surveillance**, protection, maintien dans le domaine de fonctionnement normal par toutes sortes de systèmes de régulation, de protection automatique (arrêt d'urgence), de surveillance périodique (vérification des soudures, recherche des fissures), d'aide au diagnostic ;
3. **maîtrise des accidents**, c'est-à-dire des incidents dont on postule qu'il ne seraient pas contenus aux niveaux précédents et seraient à traiter à ce troisième niveau de défense, pour en limiter les effets ;
4. **confinement** des conséquences des accidents graves non maîtrisés au niveau précédent : les dommages à l'installation sont importants, on s'efforce de limiter les rejets en dehors de l'installation ;
5. **limitation des conséquences de rejets** pour la population ; au niveau précédent, le responsable est encore l'exploitant (EDF) ; ici, le Préfet prend le relais.

¹⁰ Nous basons ce résumé très bref sur les ouvrages de J. Libmann : *Approche et analyse de la sûreté des réacteurs à eau sous pression* (CEA, 1987) ; *Éléments de sûreté nucléaire* (IPSN, 1996) ; avec cette seconde édition, l'ouvrage passe de 200 à 575 pages

La place progressive prise par la sûreté

Historiquement, le développement de la production d'énergie nucléaire a commencé par aborder la faisabilité technique, l'industrialisation des prototypes, la rentabilité des filières, les liens avec des objectifs militaires. Dans cette phase, la démarche de sûreté est au départ une préoccupation de second ordre : l'objectif principal est de concevoir une centrale nucléaire qui fonctionne bien, à un coût raisonnable (objectif 1) et, ensuite, il faut limiter les conséquences de défauts, « d'anomalies » (objectif 2). Cette démarche conduit à étudier une série d'accidents postulés afin de dimensionner les équipements productifs (qualité, niveau 1 de la défense en profondeur) et les systèmes de régulation (niveau 2), puis les équipements de sûreté (niveaux 2 et 3, essentiellement) et le confinement (niveau 4). Aujourd'hui, la technologie de la sûreté s'efforce d'être mieux intégrée dès la conception.

L'émergence progressive de la fonction de sûreté.

En France, dans les années 1970, au sein du CEA, les études de sûreté sont menées par quelques ingénieurs parallèlement à la conception de divers types de filières. Progressivement, entre 1970 et 1980, ce petit groupe d'ingénieurs chargé des questions de sûreté à Fontenay-aux-Roses devient un département et gagne son indépendance.

La situation était la même en URSS. Quand les finlandais achètent des réacteurs VVER, ces derniers, tout comme les RBMK (type Tchernobyl), ne sont pas accompagnés d'études de sûreté. En raison de l'insistance de leurs clients finlandais, les ingénieurs soviétiques vont développer des réacteurs à la sûreté est nettement améliorée.

Les précurseurs en matière de formalisation de la sûreté sont les américains : c'est d'abord chez eux que l'on rencontre des ingénieurs spécialistes de la sûreté et des rapports de sûreté stricto sensu. Cette formalisation se concrétise en quelques principes : la redondance, le confinement, les scénarios, les classes d'accidents.

La connaissance insuffisante des évolutions accidentelles

Dans l'étude des accidents, une attitude prudente est systématique. Les phénomènes physiques en cause dans une centrale nucléaire en fonctionnement normal sont parfaitement connus en théorie. Mais il faut bien comprendre qu'en pratique, en dehors de ce champ, les réactions détaillées ne sont qu'imparfaitement connues : par exemple, de nombreuses études sont nécessaires pour connaître le fonctionnement précis des crayons de combustible au fil de leur combustion. Dans ces conditions, les évolutions rares et extrêmes que l'on peut imaginer au cours d'accidents sont nécessairement affectées d'incertitudes diverses et les surprises sont plutôt la règle que l'exception. Par exemple, c'est l'accident de Three Mile Island qui a fait découvrir la possibilité de formation d'une bulle d'hydrogène dans le haut du réacteur et donc la possibilité d'explosions très violentes capables de mettre à mal l'enceinte de confinement. Cette bulle, dont on ne pouvait connaître l'importance, a terrorisé les responsables concernés.

La mise en œuvre d'une prudence systématique

Dans ces conditions, **la prudence et le pessimisme doivent, en effet, être systématiques.** Ils se déclinent, entre autres, comme suit :

- la notion d'accident enveloppe (le pire présumé au sein d'une famille d'incidents) ;
- le critère de défaillance unique (envisager la possible défaillance de chaque équipement de sûreté quand il est sollicité au cours d'une séquence incidentelle) ;

- les défaillances de mode commun (une même cause rend indisponible plusieurs matériels dont la fiabilité est censée être indépendante) ;
- les cumuls pénalisants (accident de dimensionnement les plus graves + perte d'alimentation électrique + séisme) ;
- les marges de sûreté (le séisme majoré de sécurité, etc.).

L'exhaustivité impossible... et pourtant nécessaire

Dans la plupart des cas, la démarche technologique de sûreté n'a pas péché par manque de pessimisme. En revanche, elle a souvent été loin de l'exhaustivité :

- prise en compte trop progressive des éléments essentiels au fonctionnement des systèmes de sauvegarde, comme, par exemple, l'air comprimé ;
- focalisation sur les situations de conduite aux dépens des opérations de maintenance ;
- prise en compte trop fruste des incendies dans les premières études, le spécialiste de la protection incendie étant un spécialiste étranger aux analystes de sûreté ;
- et surtout, prise en compte insuffisante des facteurs humains, surtout avant Three Mile Island, mais même aujourd'hui.

Sans doute l'exhaustivité est-elle inaccessible, mais la liste ci-dessus donne quelques indications assez suggestives sur la façon dont elle s'est progressivement améliorée, et donc, pour l'avenir et pour d'autres domaines, sur la façon d'accélérer le processus et éviter certains modes de pensée inefficaces.

Le retour d'expérience

L'importance des éléments négligés a été révélée par un retour d'expérience systématique effectué par EDF et l'IPSN et complété par les échanges internationaux.

EDF s'est doté d'un système de retour d'expérience destiné, au moins, à améliorer la fiabilité de ses matériels. De son côté, l'IRSN (nouvelle appellation de l'IPSN) alimente et exploite depuis 1973 son fichier d'incidents. C'est pourtant l'accident de Three Mile Island qui a donné toute son ampleur au retour d'expérience. Cet incident avait été précédé de plusieurs incidents précurseurs, mais ils n'avaient pas eu de conséquences et on en restait à l'équation :

pas de conséquence = pas d'importance.

La chasse aux événements précurseurs est devenue, dans son principe, une préoccupation importante de tous les exploitants et de tous les organismes de sûreté nucléaire dans le monde. Les incidents intéressant la sûreté sont au nombre de 30 à 50 par tranche et par an ; les incidents significatifs de 10 par tranche et par an après la période de démarrage. Les incidents font l'objet d'un examen par l'ingénieur chargé du site au sein de l'IPSN et sont portés à la connaissance de tous ingénieurs assurant de telles fonctions, un avantage de la standardisation du parc français. Ceux-ci se réunissent plusieurs fois par mois pour discuter de ces incidents ainsi que des incidents étrangers.

La méthodologie d'étude des incidents significatifs comporte :

- une connaissance approfondie de tous les aspects du déroulement de l'incident ;

- qu’aurait-il pu se passer de plus grave : “*what if?*” ;
- recherche des causes profondes ;
- élargissement à d’autres situations et analyse des conséquences possibles ; c’est la généralisation qui est d’autant plus difficile que les incidents sont moins graves.

Le retour d'expérience est suivi d'études statistiques. Cette forme de connaissance bénéficie de la standardisation du parc français. **Cette étude a révélé l'importance des périodes d'arrêt des réacteurs**, durant lesquelles la puissance résiduelle du réacteur doit être évacuée.

Exemple de résultat de l'analyse statistique

En trois ans, sur près d'un millier d'incidents significatifs, on a noté 13 déclenchements ou refus de démarrage d'une turbopompe sollicitée après arrêt d'urgence. Une recherche dans le fichier des événements a révélé un total de 40 déclenchements au démarrage en 100 années réacteurs. L'étude a alors été poursuivie avec les services centraux d'EDF pour connaître le nombre d'ordres de démarrage correspondant. Elle a conduit à un taux de refus de démarrage à la première sollicitation de 2.10^{-2} , valeur équivalente à celle observée sur les tranches américaines, et non 3.10^{-3} , valeur prise en compte en France jusqu'alors dans les évaluations probabilistes. Elle a permis également de retrouver les causes de ces défaillances et d'étudier les mesures correctives appropriées.

Les Études Probabilistes de Sûreté (EPS)

A partir de 1982, démarrent les études probabilistes de sûreté (EPS), un effort important est engagé pour développer une vue sinon exhaustive, du moins globale et très large. Ces études permettent de mettre en évidence les systèmes et fonctions les plus sensibles, les périodes les plus délicates, les facteurs les plus significatifs et les priorités les plus urgentes.

Elles ne résolvent pourtant pas la question de l'exhaustivité. En effet, les accidents graves qui se sont produits, se trouvent hors champ. En effet, on dit que l'accident de Three Mile Island aurait une probabilité de l'ordre de 10^{-10} (alors que les EPS s'arrêtent à 10^{-6} ou 10^{-7}) et l'accident de Tchernobyl une probabilité tellement faible qu'elle est incalculable.

Les EPS confirment le rôle prépondérant du facteur humain et le caractère critique des périodes de maintenance (arrêts de tranche programmés). Les aspects organisationnels sont plus négligés en France que dans d'autres pays où l'on a mieux compris semble-t-il leur poids prépondérant dans les défis à venir : vieillissement et prolongation de la vie des centrales dans un contexte défavorable au nucléaire.

La première étude globale de sûreté a été effectuée aux États Unis en 1975 : c'est la fameuse étude Rasmussen. C'est en 1982 que l'IPSN a décidé d'effectuer l'évaluation probabiliste globale de la sûreté d'une tranche nucléaire de 900 MWe, EDF s'engageant à réaliser une étude équivalente sur les 1300MWe en 1985. Ces études interviennent donc après les décisions de lancer les programmes nucléaires, aussi bien aux États Unis qu'en France.

L'intérêt de ces études ne se limite pas à déterminer une valeur absolue de risque de fusion du cœur. Elles éclairent les composantes du risque, leurs poids relatif et les priorités de sûreté. Elles permettent aussi de classer par ordre de priorité les modifications jugées souhaitables du point de vue de la sûreté. Elles permettent enfin de définir des états de repli du système quand certains matériels de sûreté sont indisponibles. Les incertitudes de la méthode portent sur :

- l'exhaustivité des voies de défaillance ; de gros efforts portent sur cet aspect qui reste pourtant une difficulté fondamentale ;
- les données de fiabilité des composants ; EDF dispose d'un système de recueil de données de fiabilité qui permet, en principe, malgré les difficultés inhérentes à ce genre de système, une incertitude de l'ordre d'un facteur 2 ou 3 sur les données de fiabilité ; l'encadré précédent révèle pourtant le cas d'un facteur 7 dans un sens défavorable à la sûreté ; en outre, par construction, les événements très rares ne bénéficient guère de ce genre de système ;
- les données de fiabilité humaine ;
- l'incertitude des probabilités finales calculées ; les calculs nécessaires à l'évaluation de cette incertitude sont très complexes ; ils sont prévus lors de la deuxième phase des études.

Prise en compte des facteurs humains. Les facteurs humains jouent un rôle très important lors des situations accidentelles :

- en positif, réparation et remise en service de systèmes, mise en œuvre de procédures adaptées ou de stratégies palliatives ;
- en négatif, intervention inadéquate telle que confusion, omission, action inopportune.

La prise en compte des facteurs humains est donc essentielle dans la réalisation d'une EPS. Il s'agit, cependant, d'un domaine particulièrement difficile, non aisément quantifiable. Les interventions humaines prises en compte peuvent être classées en deux catégories :

- les erreurs pré-accidentelles, qui peuvent contribuer à l'indisponibilité des systèmes ou provoquer des initiateurs ;
- les interventions en situation accidentelle (diagnostic, exécution de procédures, actions hors procédures) pouvant influencer le déroulement des séquences.

Résultats globaux et incertitudes. La probabilité totale de fusion du cœur est de :

5.10^{-5} par année.réacteur pour les 900 MWe

1.10^{-5} par année.réacteur pour les 1300 MWe qui sont plus récents

Si l'on exclut les séquences accidentelles dans les états hors puissance, et si on limite la durée des séquences à 24 heures, la probabilité de fusion du cœur des 900 MWe n'est plus que de 2.10^{-5} par année.réacteur. Néanmoins, cette étude ne tient compte ni des incendies et inondations internes, ni des agressions externes, qui ont, dans certaines autres études, une contribution significative. Certaines séquences envisageables quand le réacteur est à l'arrêt et partiellement vidangé, n'ont pas non plus été traitées dans l'étude car on a supposé que les problèmes identifiés pouvaient être résolus rapidement, les séquences correspondantes n'ayant plus, alors, de contribution significatives.

Dans le cas des 1300 MWe, EDF a accompagné son étude d'un traitement mathématique des incertitudes reconnues sur les données utilisées. Il en ressort que l'intervalle de confiance à 90% autour de la valeur de 1.10^{-5} est :

2.10^{-6} 2.10^{-5} .

Ce calcul ne rend évidemment pas compte des limites du champ de l'étude elle-même. Le calcul effectué pour l'étude 900 donne des résultats similaires.

Les comparaisons avec les études étrangères sont très délicates, car les hypothèses peuvent différer, les matériels ne sont pas les mêmes, les organisations humaines sont parfois très différentes. Un tableau comparatif sur un champ comparable donne des valeurs globales allant de 1.10^{-6} à 6.10^{-5} .

Importance des facteurs humains. Dans l'étude 900, les situations à l'arrêt contribuent pour 32% à la probabilité totale de fusion du cœur. Cette valeur est élevée, car il n'y a pas d'automatisme disponible pour faire face à une telle situation accidentelle et que des interventions humaines sont alors nécessaires. Le risque par heure d'arrêt est, de ce fait, nettement supérieur à celui correspondant aux périodes de fonctionnement. Cependant, l'incertitude est importante, tant sur les probabilités d'erreurs humaines que sur les fréquences des initiateurs.

Les facteurs humains jouent un rôle très important. En effet, les séquences contenant au moins une erreur humaine contribuent pour près de 70% à la probabilité calculée de fusion du cœur. De plus, les facteurs humains interviennent aussi dans la probabilité de défaillance des systèmes et dans les fréquences des initiateurs. Cependant, dans la plupart des cas, on considère que l'homme peut récupérer des situations dégradées ; les séquences conduisant à la fusion du cœur passent alors par l'échec de la récupération par les opérateurs. Sans prise en compte des facteurs humains, la probabilité de fusion du cœur serait plus élevée et on ne peut conclure de façon simple que 70% du risque est dû à des erreurs humaines.

Les facteurs humains ont un poids particulièrement important dans les séquences pour lesquelles une action est nécessaire dans un délai court.

Ajoutons que cette notion de délai court ou lent provient des études, par opposition à des données d'expérience. Le scénario de Three Mile Island s'est déroulé plus vite que prévu et Les études d'accidents ne cessent de revenir sur les hypothèses qui fondent ces délais.

Résultats spécifiques. Les défaillances de mode commun ont une contribution dominante aux probabilités de défaillance des systèmes de sûreté, ce qui était prévisible puisque ces systèmes sont redondants.

Certains équipements non redondants, comme la prise d'eau, ont également une contribution significative.

Les résultats peuvent être analysés par groupe de séquences, pour identifier des groupes dominants. Un découpage trop fin des séquences doit être évité au risque de réduire les probabilités envisagées et de les considérer comme négligeables. On peut étudier des équipements ou des fonctions en les considérant absolument fiables (facteur de diminution potentielle du risque) ou au contraire totalement indisponibles (facteur d'augmentation potentielle du risque). L'EPS permet de ranger les états en fonction du risque et les initiateurs en fonction de leur gravité (probabilité conditionnelle de fusion à partir de cet initiateur).

Les études probabilistes de sûreté peuvent parfois conduire à des attitudes contraires à l'un des principes de la culture de sûreté : « il ne faut pas se contenter des résultats acquis ». Atteindre un objectif pré-défini peut, par exemple, avoir un aspect démobilisateur. Un objectif chiffré de fiabilité d'une fonction complexe peut se révéler inférieur à ce que les techniques de l'ingénieur permettent d'obtenir sans difficultés particulières. Ce serait regrettable.

Ceci peut se produire aussi bien dans le cadre de réexamen de sûreté que lors de la définition de bases de conception de futures installations.

8. LA NOTION D'INTELLIGENCE DU RISQUE

Le chapitre précédent vient de montrer le développement des concepts de la sûreté dans le cas du nucléaire, l'évolution des façons de penser, la légitimité acquise progressivement par la discipline. On peut concevoir la sûreté en termes de connaissance et d'intelligence du risque (*safety awareness*)¹¹. Deux types de connaissances entrent en jeu :

1. connaître les risques et les moyens de les maîtriser (assurance fonctionnelle),
2. savoir comment assurer la mise en œuvre de cette maîtrise, en pratique et de façon permanente (assurance qualité).

Développer cette 'intelligence' est fondamental et les deux points ci-dessus représentent des objectifs de base de la sûreté. Certes, une connaissance du système et de ses risques existe toujours. L'important est qu'elle soit (1) adéquate et (2) mobilisée lors des activités, notamment les plus critiques, ce qui reprend les deux points ci-dessus.

Des procédures de travail sont donc adéquates si elles assurent que les décisions sont prises intelligemment, avec lucidité, sur la base de bonnes connaissances. Par exemple, l'autorité de sûreté nucléaire suédoise s'éloigne de plus en plus de la vérification détaillée de la conformité aux normes et aux règles, pour s'orienter vers l'observation des *processus* et *méthodes* de travail du point de vue de la sûreté.

L'intelligence du risque devrait être commune, correspondre au partage par tous d'une connaissance commune. En pratique, néanmoins, beaucoup d'experts sont très spécialisés et ne connaissent pas tous les aspects du dossier de sûreté. Les méthodes de travail devraient donc assurer une intelligence commune de toutes les situations possibles et de leur potentiel de risque. L'étude probabiliste de sûreté (EPS), généralement disponible dans les centrales nucléaires, fournit un excellent support de l'intelligence des facteurs importants pour la sûreté (voir chapitre 7).

Intelligence du risque et culture de sûreté

Concevoir la sûreté en termes de connaissance et d'intelligence est clairement en ligne avec une réflexion en termes de culture de sûreté. Nous avons en effet opposé culture du risque et techniques particulières de gestion du risque, culture de sûreté et techniques diverses d'amélioration de la sûreté. De même, l'intelligence du risque se place en amont du savoir particulier que confère telle technique spécifique, elle est capable de la juger, d'en comprendre les tenants et les aboutissants, de la comparer à d'autres techniques voisines ou concurrentes. En outre, l'intelligence du risque fournit une compréhension de l'ensemble constitué par les diverses techniques.

¹¹ Ce qui suit est notamment basé sur un article de Hammar et Andersson, deux consultants suédois dans le domaine des déchets nucléaires : *Awareness – A key to safety management and risk communication*.

Par exemple, revoir à intervalles réguliers la conception de la sûreté (design et méthodes de travail ; opérations, surveillance et maintenance) est une voie typique de l'amélioration de la culture de sûreté. Cela correspond précisément à un effort pour accroître l'intelligence du risque. Inversement, rechercher la conformité sans autre forme de réflexion est faire preuve de peu d'intelligence du risque, mais c'est aussi le signe d'un défaut de culture de sûreté.

Une bonne culture de sûreté se distingue par un engagement constant à *améliorer* la sûreté. Un tel objectif n'est pas toujours logique si la sûreté est uniquement conçue en termes de dispositions visibles et chiffrables. Considérer, au contraire, que la sûreté est une question de connaissance et d'intelligence est tout à fait logique dans ce contexte puisque cette intelligence peut toujours être améliorée. Par exemple, les personnes chargées de la maintenance connaissent généralement assez mal les conséquences de leur travail sur la sûreté des opérations. Il est clair qu'il y a un gain de sûreté à améliorer cette connaissance, même si la qualité de la maintenance est parfaitement adéquate à l'instant présent¹².

Dans une organisation donnée, à un moment donné, le concept de sûreté ainsi que les pratiques de sûreté en vigueur peuvent refléter une connaissance ancienne. Celle-ci peut avoir largement disparu depuis lors, par exemple en raison de remplacements des personnels. Il y a de nombreux exemples de vieilles centrales nucléaires où des connaissances critiques pour la sûreté ont été restaurées par la reconstruction complète du concept de sûreté.

Les objectifs de sûreté

Les objectifs classiques de sûreté peuvent être jugés à l'aune de l'intelligence du risque. Par exemple, '*éviter complètement les accidents graves*' ne fournira probablement guère d'indications ni de possibilité d'apprentissage — on ne s'attend guère à ce que des accidents graves se produisent. Il serait plus utile de '*éviter les incidents qui révéleraient de graves lacunes dans le système de défense en profondeur*'. Cela devrait, en effet, attirer l'attention sur le *sens* de l'information issue du retour d'expérience.

Les objectifs probabilistes liés aux EPS sont particulièrement utiles : couplés au retour d'expérience, ils permettent de valider le modèle probabiliste de la centrale, fournissant ainsi une compréhension approfondie des éléments clé pour la sûreté.

Les indicateurs de sûreté

Tout comme les objectifs, les indicateurs de sûreté sont utiles dans la mesure où leur suivi contribue à la connaissance et à l'intelligence des facteurs et des conditions pertinents pour la sûreté. Or, les indicateurs généralement employés pour suivre les opérations des centrales nucléaires sont largement des indicateurs généraux de qualité, par exemple : énergie disponible, erreurs répétées, erreurs humaines, réactivité aux conclusions des audits, etc. — indicateurs qui n'ont pas de signification directe en termes de sûreté¹³.

D'autres indicateurs seraient plus utiles : le taux d'événements initiateurs de séquences accidentelles et la fiabilité des systèmes de sûreté (et de leurs composants) mesurée à partir du retour d'expérience. En utilisant le modèle probabiliste de la centrale, de tels indicateurs

¹² Un autre exemple frappant, en dehors du nucléaire, est la fausse appréciation du risque d'échec de la navette Challenger par le management. Ils estimaient ce risque à un sur 10 000, voire un sur 100 000 alors que les ingénieurs savaient qu'il était de l'ordre de un sur 100 (Voir C. Morel, *Les décisions absurdes*, Gallimard, 2002).

¹³ Ils sont, néanmoins, complétés par des indicateurs plus spécifiques du risque tels que : efficacité du confinement, rejets radioactifs normaux, doses de radiation subies par les personnels, etc.

peuvent donner des mesures probabilistes de sûreté. Celle-ci confèrent une cohérence d'ensemble à la connaissance et à l'intelligence de la sûreté.

Le fait de découvrir des éléments imprévus peut constituer un indicateur qualitatif : découverte de déficiences en dehors des inspections et des opérations de surveillance régulière ; de lacunes dans le système de défense en profondeur ; de phénomènes non pris en compte dans le concept de sûreté.

Communiquer avec le public

Pour établir la confiance du public et promouvoir des discussions constructives, on devrait viser à donner à ce public les moyens de former son propre jugement. Lui soumettre des informations trop techniques et qui ne peuvent être reçues que superficiellement n'accomplira pas grand chose. Il vaut mieux communiquer sur *les principales idées et façons de penser* la sûreté. Les aspects techniques importants peuvent être abordés, mais pour *illustrer* les idées et les modes de pensée plutôt que pour aligner des arguments.

Par exemple, dans les centrales suédoises après l'accident de Three Mile Island (1979), on insistait beaucoup, dans la communication, sur l'existence de filtres de ventilation. Ces filtres jouent, en effet, un rôle de sûreté important, mais une telle insistance peut faire croire que l'on s'appuie lourdement sur cette protection qui ne constitue que la barrière ultime. Il vaudrait mieux décrire la sûreté en termes de défense en profondeur, un principe fondamental facile à faire comprendre, qui met l'accent sur les premières lignes de défense, notamment le système qualité (pour éviter les incidents) et les systèmes de sûreté (pour récupérer les incidents qui se produiront malgré tout et éviter qu'ils n'aboutissent à des accidents).

Pour illustrer, prenons à nouveau les EPS. Des EPS améliorées aboutissent quelques fois à des fréquences d'accidents *plus élevées*, par exemple lorsque des interdépendances imprévues sont mises en évidence. Il est certainement fort délicat de l'expliquer au public... De plus, de telles explications ne traiteraient pas la question fondamentale, à savoir : peut-on faire confiance à la sûreté de la centrale ? Il est impossible d'éviter tout impact négatif d'une telle information sur la confiance du public, mais la confiance sera plus facilement retrouvée en traitant en priorité les aspects d'intelligence. L'EPS doit alors être présentée comme un moyen puissant d'engendrer cette intelligence de tous les facteurs à contrôler pour assurer la sûreté d'installations aussi complexes que les centrales nucléaires. Comme une intelligence complète ne peut jamais être garantie, les EPS sont, en effet, constamment sujettes à de nouveaux développements. Le progrès continu de la connaissance fait découvrir des faiblesses jusqu'alors ignorées, ce qui permet d'y remédier.

9. INTELLIGENCE DU RISQUE DANS L'AVIATION CIVILE

Les facteurs de la sécurité dans le secteur de l'activité de l'aviation civile sont ¹⁴ :

- Le facteur technique : des règles strictes de certification des aéronefs, ainsi qu'une standardisation des procédures.
- Le facteur humain : celui-ci désignait, au départ, le solde de la technique, l'homme, tout bêtement. Si la technique n'avait pas failli, les pilotes étaient coupables et étaient mis à pied — s'ils n'étaient pas morts. Le facteur humain, ainsi défini, représenterait 80 % des causes d'accident aujourd'hui. Mais on sait maintenant que l'erreur est inévitable même chez les meilleurs¹⁵. Il faut élaborer des systèmes qui tolèrent ce type d'erreur.
- Le facteur organisationnel : il permet de passer au delà de l'étiquette 'erreur humaine'. On remonte alors vers « *les tables d'acajou des échelons supérieurs* » (Lagarhus). Les décisions prises à ces niveaux peuvent créer des dangers qui demeurent latents pendant des années, des défaillances latentes qui finissent par se combiner avec des défaillances actives et mettre en défaut le système de défense en profondeur. À présent, les préoccupations de sûreté dans l'aviation se concentrent largement sur l'organisation et le management. La gestion moderne de la qualité (voir chapitre 19) est utilisée pour améliorer les contrôles.

Toute compagnie aérienne qui veut survivre et se développer doit intégrer les considérations de sûreté à tous les niveaux de l'organisation. Sa base doit se trouver dans le management de la compagnie, au plus haut sommet, là où la sûreté et la qualité sont définies sous formes de politiques de l'entreprise. « *Pas seulement dans le langage oratoire commun aux grandes entreprises, fait de mots et de belles phrases. Non, il faut une politique de sûreté et de qualité acceptée au sein de l'ensemble de la compagnie et qui intervient dans toutes les décisions prises par la Direction.* »

Puis, cette politique doit être communiquée au sein de toute la compagnie, être comprise et 'honorée' partout. Pour cela, il est nécessaire que cette politique soit acceptée et honorée au niveau de la Direction, qu'elle soit visible dans toutes ses décisions et priorités.

¹⁴ Ce chapitre est basé sur *The crucial role of Safety culture*, article du pilote suédois Otto Lagarhus, PDG de la firme de consultants LAC, disponible sur www.lac.no/Safetyculture.htm et se réfère au cas scandinave, même si l'application des idées exposées déborde à la fois la Scandinavie et le secteur de l'aviation.

¹⁵ « Le proverbe latin, 'l'erreur est humaine', définit encore [aujourd'hui] une caractéristique universelle de nos existences. Les organisations peuvent tendre vers le 'zéro erreur', mais c'est un but hors d'atteinte. Tant que des êtres humains opéreront dans des environnements complexes, il y aura des erreurs. Et en cas de stress, de surcharge de travail, de sous-charge de travail ou d'ennui, la probabilité d'erreur augmente. Le mieux que les organisations puissent espérer, c'est de gérer efficacement ces erreurs, dans le but d'en faire diminuer la probabilité et d'en minimiser les conséquences. » (Helmreich, *Error Management as Organisational Strategy*, in Proceedings of the IATA Human Factors Seminar, Bangkok, 1998)

On pourra aussi se reporter à *Risques, erreurs et défaillances, approche interdisciplinaire*, séminaire sous la direction de René Amalberti, Catherine Fuchs et Claude Gilbert, CNRS, MSH, 2001

L'autorité de contrôle et la compagnie

Il existe un principe fondamental dans l'aviation scandinave : la compagnie est responsable, elle suit et corrige ses propres opérations. L'autorité ne s'en désintéresse pas, au contraire, mais sa mission consiste à :

- Déterminer un ensemble de règles communes à toutes les compagnies ;
- Mettre en œuvre un contrôle des nouveaux entrants qui vérifie leurs compétences et leur organisation, les personnes clés, les ressources financières et en personnel, l'assurance qualité ;
- Superviser le contrôle fonctionnel de la compagnie.

Ce dernier point est essentiel. Une fois autorisée à opérer, c'est la compagnie elle-même qui détecte et corrige toute incohérence de ses procédures pour éliminer les erreurs potentielles. En parallèle, l'autorité la supervise en continu. Elle possède les manuels, dispose d'un accès direct aux systèmes de reporting et aux ordinateurs et entretient un contact suivi avec les personnes clés de la compagnie. Elle sait très bien ce qui se passe.

Son objectif n'est pas d'identifier les erreurs ni les fautifs ni même de poursuivre la compagnie pour ses erreurs ou omissions. Elle a une perspective beaucoup plus vaste : s'assurer que le contrôle fonctionnel de la compagnie fonctionne. Ce n'est que lorsque la compagnie ne parvient pas à corriger ses défaillances que l'autorité agit — initialement par une remarque, ultimement par le retrait du permis d'opérer.

Ce système — contrôle à l'entrée, contrôle fonctionnel et supervision par l'autorité — épargne à l'autorité une énorme tâche d'inspection et de police. De plus, il indique très clairement que la responsabilité de la sûreté et de la qualité repose sur les compagnies et non pas sur l'autorité.

En d'autres termes, il n'est pas possible de se contenter de faire tourner une compagnie aérienne de façon limite tant que l'autorité n'a rien remarqué. Le contrôle fonctionnel de la compagnie détectera très tôt les problèmes éventuels, les annoncera et les corrigera. L'autorité vérifie en continu que ce contrôle fonctionnel remplit bien les fonctions qui en sont attendues.

Le rôle du constructeur

Le fabricant d'aéronefs est soumis à une sévère procédure de certification au cours de laquelle les tests vont bien plus loin que le fonctionnement normal des appareils. En outre, la procédure certifie également la documentation qui doit préciser les limites d'utilisation, les procédures opérationnelles, les calculs de performance et les programmes de maintenance.

Mais la responsabilité du constructeur ne s'arrête pas là. Il suit les opérations bien après la livraison du dernier appareil fabriqué et, en cas de problème détecté, il doit produire un bulletin de service qui suggère des solutions appropriées. L'autorité suit ce processus en permanence. Pour certains problèmes cruciaux, elle peut rendre certaines modifications obligatoires — dont certaines devront être mises en œuvre en quelques jours, d'autres dans un délai moins court. Sur les avions qu'utilise actuellement SAS [la compagnie aérienne scandinave], cela se produit de nombreuses fois chaque année.

Promouvoir la sécurité au quotidien

SAS a formulé une politique connue de tous dans la compagnie, des priorités impératives :

1. sécurité,
2. ponctualité,
3. service.

En aucun cas la ponctualité ou le service ne peuvent compromettre la sécurité, et le service ne passera jamais avant la ponctualité. L'échelle de priorité est très simple, elle est donc comprise partout et prise en compte dans chaque décision.

Le système d'information (reporting)

Pour quelques accidents, il existe un grand nombre d'incidents sans conséquence sérieuse, mais un jour, une combinaison des causes de ces incidents peut produire une catastrophe. Il est donc très important d'enregistrer tous les incidents un par un, d'en tirer les conclusions. D'où un système d'information complet.

Le moyen d'information le plus évident est le Livre de Bord où l'équipage rapporte tout défaut technique noté pendant le vol. Le personnel de maintenance y enregistre les actions correctives apportées. Les inspections de l'avion y figurent aussi. Toutes les remarques inscrites sur les Livres de Bord sont enregistrées dans un système informatique. Celui-ci est accessible dans toute la compagnie ainsi que dans les bureaux de l'autorité de surveillance.

Dès qu'il se produit en vol un événement quelconque susceptible d'influer sur la sécurité, le capitaine rédige un Rapport d'Événement en Vol. En moyenne, un ou deux tels rapports sont rédigés chaque jour à SAS. Ils sont classés par domaine concerné (technique, opérationnel, etc.) ainsi que sur une échelle de risque allant de 1 à 10. Les rapports correspondant à des risques faibles sont diffusés pour information, alors que d'autres donnent lieu à enquêtes. Pour les incidents mineurs, le département responsable conduit l'enquête et recommande des actions correctives. Pour les enquêtes plus importantes, une équipe spéciale doit opérer selon les principes de l'OACI (Organisation de l'Aviation Civile Internationale).

Outre les rapports d'événement en vol, de nombreux rapports spécifiques sont consacrés à la sécurité : rapports sur le contrôle aérien, sur les collisions avec des oiseaux, ou sur l'environnement de travail... Les personnels navigants ont aussi des procédures de reporting pour les questions de sécurité.

L'objectif des rapports et des enquêtes est d'éliminer les problèmes pour l'avenir. Ils contiennent le plus souvent des recommandations en général acceptées et mises en œuvre. Les rapports d'enquête sont diffusés à l'autorité qui est très attentive à la mise en œuvre des recommandations.

Les questions qui ne concernent pas la sécurité font l'objet d'un 'Rapport de Voyage'. Le capitaine peut y indiquer tout ce qu'il souhaite communiquer à la compagnie : la médiocre qualité de l'hôtel réservé à l'équipage à Chicago, un passager malade à Singapour, etc. Ces rapports en disent long sur la réalité du terrain — simple confort ou de ponctualité — mais révèlent aussi des éléments susceptibles d'affecter la sécurité.

Tous les rapports sont accessibles, et comportent le nom de leur auteur. Il faut donc que chacun se sente libre de faire rapport sans risquer d'être puni par la compagnie ou l'autorité. SAS bénéficie d'une grande fréquence de reporting grâce à la confiance des pilotes. On tend,

néanmoins, au sein de l'autorité, à recourir aux actions en justice envers les individus, une tendance qui pourrait miner la confiance des acteurs. Les compagnies tout autant que l'autorité devraient favoriser un reporting ouvert ainsi que la fréquence de reporting.

D'autres pays et d'autres compagnies ont des cultures de reporting sensiblement différentes. Certains pratiquent un reporting anonyme ou confidentiel à côté du reporting ouvert. De tels systèmes n'ont pas démontré qu'ils offraient la même qualité et le même volume de reporting.

Les compagnies sont souvent rôdées en matière d'enquêtes et de mesures correctives liées aux incidents pris individuellement. En revanche, l'analyse d'ensemble reste à améliorer en vue de repérer des tendances globales et de créer un système d'alerte avancée. Pour cela, il faut augmenter le volume de reporting. À trois rapports par jour, il demeure un vaste gisement d'information au sein des autres 997 vols quotidiens. On peut également penser à l'utilisation conjointe des bases de données. Il en existe beaucoup : la plupart des compagnies aériennes gèrent la leur ; les autorités, les constructeurs, les organisations professionnelles, tous rassemblent de l'information sur les incidents, accidents et autres événements. La coopération entre ces acteurs pourrait être sensiblement améliorée.

Le reporting automatique

Tout avion est équipé d'un enregistreur de vol que l'on utilise en cas d'accident — la fameuse 'boîte noire'. Dans les avions modernes, cette boîte noire a été améliorée et ses capacités étendues bien au delà des exigences réglementaires. Plusieurs centaines de paramètres sont enregistrés pour chaque vol. On analyse systématiquement ces informations, on vérifie si les pilotes ont bien suivi les procédures d'approche, comment ils respectent les altitudes, les vitesses, etc. Au sein de ce vaste matériau, on identifie donc des tendances dans la façon dont les pilotes remplissent leur fonction.

C'est *Big Brother* ? Eh bien, il est clair que les pilotes sont suivis de près. Ils ne peuvent s'écarter beaucoup de la norme sans que cela soit détecté. Mais ils comprennent les bienfaits du système pour la sécurité. De plus, le système a été conçu en coopération avec les syndicats de pilotes en accordant beaucoup d'attention à la confidentialité des données individuelles. Le système est géré par un département dédié, dirigé par un capitaine expérimenté, très intègre et qui jouit de la confiance de ses collègues.

Dans certains cas exceptionnels, le système est à même de détecter des écarts qui n'ont pas fait l'objet d'un rapport et qui méritent néanmoins qu'une action soit engagée à l'encontre d'un pilote donné ou, au moins, qu'une explication soit exigée. Même dans ce genre de cas, la confidentialité est largement assurée.

Le système est très utile pour la sécurité et la compagnie prend soin de le gérer de façon à conserver la confiance des pilotes.

L'inspection

Les inspections constituent un autre moyen de prendre la température des opérations de vol. Un pilote inspecteur, spécialement sélectionné et formé, observe ses collègues dans leur travail quotidien. Sa présence dans le cockpit est connue et annoncée très à l'avance. Après l'inspection, la conduite du vol est analysée avec l'ensemble de l'équipage, les problèmes particuliers sont discutés et l'on aborde les conditions de travail générales. Il n'y a pas de rapport sur les individus, mais les pilotes inspecteurs font régulièrement des rapports sur les tendances et les aspects délicats détectés lors de ces observations.

La formation continue

Deux fois par an, chaque pilote suit une formation continue, une session soigneusement préparée comprenant un examen oral et une discussion ainsi qu'un vol sur simulateur dans lequel un équipage au complet est confronté à un vol à problème : détournement, défaillance d'un moteur, météo difficile ou indisponibilité d'un membre d'équipage... L'objectif de ces formations n'est pas de tester les capacités d'un pilote donné à gérer physiquement l'avion, mais plutôt de vérifier ses capacités à collaborer avec le reste de l'équipage et à utiliser tous les moyens disponibles — en l'air et au sol — pour gérer la situation. De grands efforts sont consacrés à élaborer des situations de formation réalistes et à faire comprendre que les compétences, les relations humaines et la coopération sont les clés en cas de situation difficile.

L'administration

Le travail effectué par l'administration est d'importance capitale pour la sécurité des vols, tant dans la rédaction des procédures que dans la documentation, la gestion des modifications d'appareils et dans de nombreuses autres tâches. Il faut garantir qu'aucune question relative à la sécurité ne soit égarée dans des tas de papiers. Ce domaine doit donc être abordé avec la même approche systématique que celui des opérations de vol.

Généralisation hors de Scandinavie

D'après Jean Paries, directeur de Dédale, une société spécialisée dans le risque et le facteur humain, notamment dans l'aviation civile (voir aussi annexe 2) :

« Ce qui précède correspond au standard moyen européen des compagnies majors. Par différence, les compagnies US sont encore rares à faire de 'l'analyse systématique des vols' (analyse des enregistreurs après chaque vol) pour des raisons de culture juridique. Les petites compagnies ne se sont pas toutes mises à l'assurance qualité.

Le rôle de l'autorité est parfois plus proche d'une surveillance directe des opérations : inspections sur le terrain, audits, pilotes inspecteurs dans les cockpits... Elle peut assumer la délivrance des licences de pilotes. Mais la tendance est bien celle décrite : dire le droit commun, réguler l'entrée, et surveiller la surveillance.

Au plan international, il existe encore une forte hétérogénéité. L'Afrique, la Chine, l'ex URSS, l'Amérique latine sont encore localement loin de ce standard et les taux d'accidents y sont 10 à 20 fois supérieurs. Ce qui tend à stabiliser la moyenne mondiale et donne l'impression qu'on ne progresse plus. En réalité, le progrès de la sécurité continue à un taux faible mais non nul : par exemple, les majors US en sont à 0,3 accident mortel par million de départ, contre environ 1 il y a dix ans.

La sûreté dépend aussi de l'interaction de la compagnie avec son environnement économique (ses fournisseurs, ses passagers, etc.), avec les aéroports encombrés, avec le système ATM de gestion du trafic aérien saturé (Europe) ou déliquescents (Afrique) (sûrement un des défis de l'avenir à moyen terme). Au niveau du vol individuel, on a sans doute atteint l'apogée de la stratégie normalisation-procéduralisation-automatisation. Conserver l'intelligence devient un axe de réflexion important. »

10. INTELLIGENCE DU RISQUE ET INONDATIONS

La Commission Internationale pour la Protection du Rhin a publié en 2002 un ouvrage intitulé *Prévention du risque de dommages liés aux inondations*¹⁶ dont la synthèse figure en annexe 4, ainsi que quelques recommandations techniques destinées à améliorer la culture de sûreté du lecteur dans le domaine des inondations. Ce rapport témoigne de ce que peut réaliser un effort d'intelligence du risque tant pour les professionnels que pour les particuliers (habitations). Voici les 'slogans' mis en exergue au fronton des chapitres, répartis par thèmes. Ils constituent une feuille de route pour une politique de prévention en matière de risque naturel. La nécessité de connaître le risque et d'en conserver la vigilance collective — points forts de l'approche en termes de culture du risque — est éclatante :

La culture du risque concerne l'ensemble des parties.

Seule la volonté des différents acteurs de coopérer permet de limiter les dommages dans l'intérêt commun.

La prévention des dommages nous concerne tous.

Vivre avec les crues.

La connaissance des risques est essentielle

Un aléa reconnu réduit le risque de moitié.

Prendre en compte les forces hydrauliques.

Le comportement préventif doit pouvoir s'ancrer dans des prévisions fiables.

Les personnes sont exposées au risque quand elles sont surprises par la crue, qu'elles croient à tort se trouver en lieu sûr ou qu'elles ne peuvent atteindre à temps un refuge.

Connaître les refuges sûrs – s'entraîner aux secours.

L'humidité et les salissures sont à l'origine de l'endommagement.

Il n'y a pas lieu d'agir là où les dommages potentiels sont inexistantes.

Réduction des dommages bien avant la crue

Espace pour le fleuve – il n'y a pas de dommages là où les dommages potentiels sont inexistantes.

Les projets de construction et d'occupation des sols sont à adapter à l'aléa en présence.

¹⁶ Cet ouvrage est disponible à partir du site de cette commission (www.iksr.org) à l'adresse suivante : http://www.iksr.org/pdf/RZ_iksr_franz.pdf.

Reliée à des usages et un équipement adaptés, la mise en eau de bâtiments constitue une mesure de limitation des dommages.

L'étanchement de bâtiments compte parmi les mesures les plus efficaces quand le bâti est en mesure de supporter la pression de eaux.

La préparation doit démarrer bien avant que ne survienne la crue.

Réduire presque de moitié les dommages avec des moyens simples!

Anticiper la crise

Planifier les mesures de prévision des dommages et s'y entraîner avec le personnel de l'entreprise!

Planifier la prévention des crues extrêmes et s'entraîner à y faire face!

Quelles mesures choisir? Comment agissent-elles?

Les espaces de décharge de secours sont les derniers remparts de la prévention des crues.

Assurer le minimum vital en situation cruciale.

Qui fait quoi?

Améliorer la culture du risque est une tâche de longue haleine

La tâche de persuasion est un outil important!

III - GOUVERNANCE D'ENTREPRISE

Un mouvement se dessine en faveur d'une gouvernance des risques dans les entreprises. En Grande Bretagne, pays le plus avancé dans ce domaine, probablement en raison de l'émoi suscité par la faillite de la banque Barings, le rapport Turnbull (1999) explicite les exigences de base d'une telle gouvernance. Il décline la *nécessaire intelligence* des risques au niveau du Conseil, de la Direction et de l'ensemble des employés et montre qu'elle implique d'intégrer la gestion des risques au sein de l'activité ordinaire, tout en restant lucide sur l'impossibilité d'éliminer totalement le risque (chapitre 11). En particulier, le rapport détaille les caractéristiques d'un système de contrôle interne et propose une intéressante série de questions relatives à l'intelligence du risque, aux contrôles (l'organisation interne), à la communication et au suivi (voir pp. 80). Enfin nous discutons le rapport Turnbull à partir des questions suivantes : une approche purement financière est-elle valable ? une approche de la gouvernance uniquement dirigée vers les actionnaires est-elle équilibrée ? quelle est l'efficacité d'un code de gouvernance, particulièrement après l'affaire Enron et les autres scandales de gouvernance d'entreprise au États Unis ? et enfin, quelle communication peut-on mener autour des risques ?

Le rapport Turnbull a suscité de nombreuses questions sur sa mise en oeuvre. L'institut des comptables britanniques a publié des documents explicatifs qui sont autant de développements pratiques du rapport. Ces documents révèlent, en particulier, la faible place des risques technologiques et environnementaux dans les entreprises en général, c'est-à-dire y compris les entreprises n'opérant pas d'installations à risques (chapitre 12). Le rapport Turnbull suggère que le traitement des risques doit être intégré dans les activités et impliquer l'ensemble du personnel (chapitre 13). Contrairement à d'autres fonctions, il est mauvais de vouloir l'externaliser. La théorie s'appliquant à des activités ordinaires (nettoyage des locaux, maintenance informatique, etc.) n'est pas pertinente en matière de risque. Une remarque de poids, car on aurait pu penser que, se plaçant au niveau des Directions d'entreprise et des Conseils d'administration, ce rapport d'inspiration financière conçoive la gestion des risques comme une affaire de spécialistes comme c'est le cas dans de nombreux domaines des risques financiers.

Après l'analyse des recommandations, souvent excellentes en tant que telles, relatives à la gouvernance d'entreprise en matière de risque, nous nous tournons vers la réalité. L'ampleur de la crise ouverte aux États Unis par les faillites retentissantes d'entreprise de premier plan comme Enron et WorldCom a fait réfléchir. Comment en est-on arrivé à autant de désinvolture des dirigeants par rapport aux autres parties prenantes : actionnaires, créanciers, salariés, consommateurs californiens d'électricité, comment ont-ils tous ont été instrumentalisés et escroqués ? C'est l'objet du chapitre 14 dont la réponse, au-delà de l'avidité des hommes, met en avant une immense défaillance organisationnelle de '*corporate america*'.

S'agissant de la première, l'avidité imprègne les élites américaines au delà de ce que l'on avait sans doute généralement imaginé. C'est ainsi, par exemple, que « en 1973, le PDG

moyen d'une 'major' gagnait environ 45 fois le salaire des employés...en 1991, le ratio était de 140. Maintenant, il est de 500 » (John Cassidy).

Pour ce qui est de l'organisation, les mécanismes pervers qui ont soutenu la mise en place de cette culture de la cupidité ('*greed*') incluent :

- des incitations perverses des stock options, mais aussi du système global dans lequel opèrent les dirigeants et qui s'imposent à eux ;
- des pratiques 'créatives' voire des tromperies au niveau des comptabilités, mais aussi des règles insuffisantes et l'incitation forte à présenter une image positive ;
- une cupidité naturelle, mais aussi un système qui amène progressivement des personnes à l'éthique 'normale' à glisser vers des pratiques finalement désastreuses.

Ce chapitre donne un grand nombre d'exemples convaincants de la dérive ayant mené d'une culture entrepreneuriale respectant la production et les partenaires, à une culture financière de prédation qui risque de perdurer (voir l'affaire Metaleurop révélée en janvier 2003). Les solutions, elles, ne sont ni nombreuses ni très convaincantes, mais le MEDD pourrait légitimement s'investir dans ces problématiques de gouvernement d'entreprise.

Cette description de la gouvernance d'entreprise au États Unis fait apparaître une orientation fortement financière, axée sur le profit quels qu'en soient les moyens, et tournée vers les seuls actionnaires. Les objectifs financiers globaux, décidés en haut, en partie à Wall Street et dans les bureaux des gestionnaires de fonds de pensions, se traduisent sur le terrain, dans les bureaux et dans les ateliers, par des 'programmes de rigueur', des 'cures d'amaigrissement', des 'licenciements mondialisés'. Une telle culture n'est guère propice au développement de la culture de sûreté.

En effet, la question se pose, face à l'emprise de ce modèle, de savoir s'il est possible d'être efficace autrement ou si l'adoption de la gestion purement financière est inéluctable. Si c'était le cas, on devrait être inquiet en matière de risques, car ce n'est pas à base de suppressions et de pressions répétées sur les moyens disponibles que l'on peut parvenir à améliorer la sûreté au quotidien dans les installations à risques. C'est au contraire à une action de construction que l'on doit s'attacher : construire une connaissance, une intelligence et un sens des risques. Or, précisément, l'exemple de Toyota (chapitre 15) montre qu'il est possible de gérer en reconnaissant la valeur du système de production, en cherchant à améliorer ce système, cet organisme, cet ensemble fin de relations, en reconnaissant qu'il s'agit d'une construction plus organique que mécanique, où l'on ne peut pas impunément changer les éléments, réduire les ressources et pousser les performances à la limite.

La plus grande variété de modèles produits chez Toyota n'y est pas un frein à l'efficacité . L'attention portée au système de production y améliore **à la fois** la gamme de produits et l'efficacité et la productivité ; c'est une façon de sortir par le haut des dilemmes économiques. Il ne s'agit ni d'innovation produit ni d'innovation 'process' au sens strict, mais plutôt d'innovation d'organisation et de culture, d'une attention aux « détails de la façon dont chaque travailleur, à chaque poste contribue à satisfaire la commande de chaque consommateur ». Une bonne gestion des risques technologiques et une bonne gestion de crise doivent également se baser sur l'attention portée au système de production, sur l'innovation d'organisation et de culture, et une attention aux détails de la façon dont chaque travailleur fonctionne. C'est l'ambition du Management Basé sur les Moyens (MBM) que le chapitre 16 expose et compare au management basé sur les résultats. De nombreux exemples des dangers de ce dernier sont donnés.

Ce sont des approches constructives, semblables aux approches qualité, qui devraient permettre de bâtir la culture de sûreté et l'intelligence du risque. La stratégie MBM vise à instiller en chacun un engagement profond à maîtriser une approche ordonnée du travail. On trouve des idées très similaires dans les textes relatifs à la culture de sûreté des opérateurs du nucléaire (chapitre 1). La qualité est intégrée au travail que chacun effectue.

Cette partie se termine avec une remarque : la grande taille des groupes mondialisés ne favorise pas nécessairement une attention systémique à la sûreté de chacun des établissements, car chacun ne pèse individuellement que peu au regard du résultat global (chapitre 17).

11. INTELLIGENCE DU RISQUE ET GOUVERNANCE D'ENTREPRISE

Les entreprises ont-elles des obligations en matière de culture du risque ? Formulée aussi brutalement, cette question appelle une réponse négative. Mais un mouvement se dessine vers des codes de bonne conduite en matière de gestion globale des risques. La Grande Bretagne, pays le plus en avance dans ce domaine, dispose d'un code de gouvernance du risque pour les sociétés cotées à la Bourse de Londres. Celui impose un système de contrôle interne et de gestion des risques intégré à l'activité normale et impliquant le Conseil, la Direction et l'ensemble des employés.

Le rapport Turnbull (1999) explicite ces exigences. Il décline la *nécessaire intelligence* des risques au niveau du Conseil, de la Direction et de l'ensemble des employés. Le contrôle interne implique l'intelligence des risques ainsi qu'une communication valable et le respect des règles. Le système est donc composé d'activités de contrôle, de processus d'information et de communication, de processus de suivi permettant de vérifier la permanente efficacité du système de contrôle interne. On retrouve, à côté de l'assurance fonctionnelle, une assurance qualité (comme au chapitre 8), mais aussi une exigence de communication. L'intelligence du risque implique d'intégrer la gestion des risques au sein de l'activité ordinaire, tout en restant lucide sur l'impossibilité d'éliminer totalement le risque.

Le rapport propose une série de questions à se poser relatives à l'intelligence du risque, aux contrôles (à l'organisation interne), à la communication et au suivi.

Après avoir présenté le rapport Turnbull plus en détail — le texte complet figurant en annexe 5 et un article de Carey et Turnbull en annexe 6 —, nous le discutons à partir des questions suivantes : une approche purement financière est-elle valable, une approche de la gouvernance uniquement dirigée vers les actionnaires est-elle équilibrée, quelle est l'efficacité d'un code de gouvernance, particulièrement après l'affaire Enron et les autres scandales de gouvernance d'entreprise au USA, et enfin, quelle communication peut-on mener autour des risques.

I. PRÉSENTATION DU RAPPORT TURNBULL

1. Principes de gouvernance du risque

Au Royaume uni, les sociétés cotées sont soumises à un code de gouvernance et de bonnes pratiques (*'the Combined Code'*). Celui-ci énonce les principes suivants :

D.2 : Le Conseil doit maintenir un système de contrôle interne valable afin de protéger l'investissement des actionnaires et les actifs de la compagnie.

D.2.1 : Les directeurs doivent, au moins annuellement, examiner l'effectivité du système de contrôle interne du groupe et informer les actionnaires qu'ils l'ont fait. Cet examen doit inclure tous les (types de) contrôles (financiers, opérationnels, de conformité et le risk management).

D.2.2 : Les compagnies qui n'ont pas d'audit interne doivent examiner de temps à autre l'intérêt d'établir une telle fonction.

De plus, la Bourse de Londres impose aux sociétés cotées d'expliquer dans leurs rapports annuels comment la société a mis en œuvre ces principes au cours de l'exercice considéré.

Le rapport Turnbull explique ces principes et précise qu'ils correspondent à :

(...) the adoption by a company's board of a risk-based approach to establishing a sound system of internal control and reviewing its effectiveness. This should be incorporated by the company within its normal management and governance processes. It should not be treated as a separate exercise undertaken to meet regulatory requirements.

(...) le Conseil d'administration des sociétés adopte une approche basée sur les risques pour mettre en place un système de contrôle interne valable et pour suivre l'efficacité de ce système. Ce système doit faire partie des processus normaux de management et de gouvernance de la société. Il ne doit pas être traité comme un exercice à part destiné à satisfaire une exigence réglementaire.

Il s'agit donc d'exigences en termes d'intelligence du risque : prendre la responsabilité de connaître ses risques, de les suivre et d'en informer les actionnaires.

L'équivalent n'existe pas en France, même si un décret de février 2002 introduit l'obligation d'une information sociale et environnementale dans le rapport de gestion des sociétés cotées.

Gouvernement d'entreprise et obligations de contrôle des risques

Le rapport du comité Turnbull au Royaume-Uni et le KonTraG en Allemagne, par exemple, fixent certaines règles générales en matière de reporting annuel sur les risques en entreprise. En France, il existe une réglementation spécifique comparable dans le domaine des assurances et de la banque, mais cette initiative n'a pas vraiment d'équivalent dans les autres secteurs : ces derniers ne sont soumis à aucune contrainte légale en matière d'information sur les risques. Aucune contrainte légale n'impose, non plus, la création, ni ne définit la mission, des divers comités qui se sont constitués depuis quelques années, dans une majorité de grands groupes français : comité d'audit ou comité d'audit et des risques, ou encore comité d'éthique, etc. Les deux rapports Viénot de 1995, sur le Conseil d'administration des sociétés cotées, et de 1999, sur le gouvernement d'entreprise, ne contiennent pas non plus de recommandations en matière de contrôle des risques, au sens large, pouvant avoir un impact sur l'atteinte des objectifs de l'entreprise. Le rapport Viénot de 1995 évoque seulement et de manière implicite la responsabilité du Conseil d'administration en termes de risques purement comptables et recommande que cette responsabilité soit portée par un comité des comptes.

Les Echos, 28 septembre 2000

Le résumé ci-dessous du rapport Turnbull insiste sur l'aspect intelligence du risque ; nos commentaires se distinguent par le format suivant : [*commentaire*].

2. Les responsabilités

Le Conseil est responsable du contrôle. Il fixe la politique en la matière et vérifie que le contrôle fonctionne correctement et efficacement. Il considère :

- la nature et l'importance des risques,
- leur acceptabilité par nature et par taille,
- leur vraisemblance,
- les capacités de l'entreprise à en réduire les conséquences,
- le rapport coût/avantages des divers outils de gestion des risques.

La Direction identifie et évalue les risques à l'intention du Conseil. Elle élabore, exploite et effectue le suivi d'un système adéquat de contrôle interne.

Tous les employés ont une responsabilité dans le contrôle interne au titre des objectifs qui leur sont fixés. Collectivement, ils devraient avoir les connaissances, les capacités, les informations et le pouvoir nécessaires pour établir, exploiter et effectuer le suivi du système de contrôle interne. Cela requiert une compréhension de l'entreprise, de ses objectifs, de son métier et de ses marchés et des risques auxquels elle est exposée.

[Le rapport décline donc, dans cette section, la nécessaire intelligence des risques au niveau du Conseil, de la Direction et de l'ensemble des employés.]

3. Les éléments du système

Le système doit :

- répondre aux risques qui affectent la réalisation des objectifs de l'entreprise, (risques stratégiques, opérationnels, financiers, de conformité, etc.). Cela implique de protéger les actifs d'un usage inapproprié, de la perte et de la fraude et d'assurer que les responsabilités juridiques (*liabilities*) sont identifiées et gérées ;
- contribuer à la qualité du reporting interne et externe qui doit fournir un flux d'informations pertinentes, fiables et à jour ;
- contribuer à la conformité avec les lois et règlements applicables mais aussi avec les règles internes de conduite des affaires.

[Le contrôle interne implique donc non seulement l'intelligence des risques, mais aussi une communication valable et le respect des règles.]

Le système sera composé

- d'activités de contrôle,
- de processus d'information et de communication,
- de processus de suivi permettant de vérifier la permanente efficacité du système de contrôle interne.

[On retrouve l'assurance fonctionnelle et l'assurance qualité (voir chapitre 8), mais aussi une exigence de communication.]

Le système de contrôle interne doit : faire partie intégrante du fonctionnement normal de l'entreprise et de sa culture ; évoluer en fonction des changements internes ou externes ; permettre d'informer immédiatement les niveaux appropriés de la hiérarchie de défaillances ou de faiblesses du système lui-même ainsi que de proposer des actions correctives.

Un bon système de contrôle n'élimine jamais complètement la possibilité d'erreurs de jugement dans les décisions, d'erreur humaine, de détournements volontaires, de contournement des contrôles et enfin de survenue d'événements imprévisibles. Il offre donc une assurance raisonnable, mais non absolue, que les activités se dérouleront comme prévu.

[L'intelligence du risque implique d'intégrer leur gestion au sein de l'activité ordinaire, tout en restant lucide sur l'impossibilité d'éliminer totalement le risque.]

4. Évaluer l'efficacité de la gestion des risques

Le rapport propose à cette fin, dans son annexe, une série de questions :

Questions générales

- L'entreprise a-t-elle des objectifs clairs ? Ont-ils été communiqués ? Donnent-ils aux employés une direction claire relative à l'évaluation des risques et au contrôle interne ? Par exemple, existe-t-il des indicateurs et des objectifs chiffrés ?
- Les risques sont-ils évalués en continu ? (risques de marché, de crédit, de liquidité, technologique, juridique, santé et sécurité du personnel, environnement, image, éthique commerciale)
- La Direction et les autres collaborateurs de l'entreprise ont-ils une claire compréhension de quels risques sont acceptables pour le Conseil ?
- Le Conseil a-t-il une stratégie de traitement des risques identifiés ? Existe-t-il une politique de gestion de ces risques ?
- Est-ce que la culture de l'entreprise, ses codes de conduite, ses politiques de ressources humaines, ses systèmes de primes d'efficacité soutiennent la réalisation des objectifs, la gestion des risques et le système de contrôle interne ?

Questions relatives au contrôle *[à l'organisation]*

- La Direction générale montre-t-elle, par ses actions et ses politiques, son nécessaire attachement à de bons niveaux de compétence et d'intégrité, et son engagement à établir un climat de confiance ?
- Les rôles et les responsabilités sont-ils clairement définis de telle sorte que les décisions et actions sont prises par les bonnes personnes ? La coordination est-elle adéquate ?
- L'entreprise communique-t-elle à ses employés ce que l'on attend d'eux et l'étendue de leur liberté d'action ? En termes de risque cela peut concerner la protection HSE, la sécurité des biens tangibles et intangibles, les questions de continuité des opérations.
- Les personnels de la compagnie (ainsi que ceux qui fournissent des services externalisés) ont-ils les connaissances, les capacités et les outils nécessaires à la réalisation des objectifs de l'entreprise et à la gestion efficace des risques qui y sont attachés ? *[Il eut été plus clair de parler directement de ressources de toutes natures comme fait l'INSAG-4 (chapitre 1).]*

- Comment les méthodes et les contrôles sont-ils ajustés pour s'adapter aux risques nouveaux ou changeants ou aux défaillances opérationnelles ?

Questions relatives à l'information

- La Direction et le Conseil reçoivent-ils l'information nécessaire au suivi des objectifs et des risques ?
- Les besoins et les systèmes d'information sont-ils réévalués quand les objectifs et les risques évoluent ou quand des défaillances du système d'information sont identifiées ?
- Les rapports régulièrement produits sont-ils des moyens efficaces pour communiquer la position et les perspectives de l'entreprise de façon équilibrée et compréhensible ?
- Existe-t-il des canaux de communication établis permettant aux individus de faire connaître les entorses aux lois et règlements ou autres conduites impropres qu'ils suspecteraient ?

Questions relatives au suivi

- Existe-t-il des moyens réguliers de suivi du contrôle interne et de la gestion des risques ?
- Ces moyens permettent-ils de suivre la capacité de l'entreprise à ré-évaluer les risques et à ajuster les contrôles ?
- Les procédures de suivi assurent-elles que des actions sont prises quand l'évaluation des risques et le contrôle détectent des changements ?
- Les questions de risque et de contrôle remontent-elles bien vers le Conseil ?
- La Direction dispose-t-elle de moyens spécifiques d'informer le Conseil sur des questions particulièrement importantes relatives au risque et au contrôle ? (par exemple : fraude, activités illégales, activités susceptibles de ternir l'image de l'entreprise ou sa position financière).

II. DISCUSSION

1. Une approche purement financière est contestable

Le rapport Turnbull semble être une réaction à la faillite de la Barings, vénérable institution bancaire britannique dont la chute a fortement marqué les esprits, spécialement outre-Manche. Une origine financière, donc, et dans le corps du texte, une forte influence du secteur financier où, par exemple, il existe des 'contrôles' sous la forme d'instruments financiers de couverture. Peut-on ramener tous les aspects du risque à l'aspect financier ?

Prenons un exemple grossier et choquant, mais qui explique bien la difficulté. Si le Conseil et la Direction de l'entreprise se penchent sur la question des accidents du travail avec l'approche du rapport Turnbull, ils envisagent les accidents du travail du point de vue de leur coût. Ainsi, le fait qu'un ouvrier perde un bras au cours de son travail ne peut pas être un risque majeur, puisqu'il ne remet pas en cause la viabilité de l'entreprise, et n'affecte même pas ses résultats. Dans une justice antique ('œil pour œil, dent pour dent') où un dirigeant devrait donner un bras à chaque fois qu'un ouvrier en perd un, il y a fort à parier que les décisions prises seraient largement différentes. Dans la version actuelle de la réparation, un

bras, c'est X milliers d'euros. Mais si l'on proposait aux dirigeants d'échanger X milliers d'euros (voire deux ou dix fois plus...) contre leur propre bras, il en est peu qui s'y résoudraient...

Cette remarque ne signifie pas que la quantification des risques n'est pas nécessaire. Elle signifie qu'une quantification des risques n'est probablement pas suffisante, car la question ne se limite pas à « Combien vaut ce risque ? », elle doit aussi indiquer qui porte ce risque : « Combien vaut ce risque, pour qui ? » Auquel cas, ce n'est pas en général une quantification, mais plusieurs, qui sont nécessaires. Dans le cas ci-dessus, l'accident ne coûte rien à la compagnie, en France, puisqu'elle souscrit à l'assurance obligatoire des accidents du travail. Le coût pour l'ouvrier qui a perdu son bras reste une question délicate : au minimum, c'est la valeur actuelle nette de sa perte estimée de revenus au cours de sa vie (probablement supérieure à l'indemnité de X milliers d'euros ; une évaluation plus complète inclut évidemment une estimation de la 'perte de bien-être' de son bras dans toutes sortes d'activités non rémunératrices).

2. Une approche de la gouvernance à rééquilibrer

Le rapport Turnbull est clairement orienté vers les actionnaires. Le risque est défini comme déviation par rapport à des objectifs, les objectifs étant ceux des actionnaires. Avec une seule concession, le fait d'y inclure les '*objectifs de l'entreprise*' ce qui évoque la préoccupation de protéger les actifs contre des décisions très à court terme d'actionnaires volatils, de prédateurs d'un jour qui pourraient quitter l'entreprise juste avant qu'elle ne sombre.

Cette approche est doublement simplificatrice : (1) il est peu probable qu'une approche déductive à partir d'objectifs généraux puisse permettre d'envisager l'ensemble des risques, particulièrement les risques les moins prévisibles ; (2) la protection '*de l'investissement des actionnaires et des actifs de la compagnie*' est probablement un objectif trop étroit qui sera vraisemblablement revu dans l'avenir pour inclure les autres parties prenantes, y compris les employés, les riverains, les clients, l'environnement. Par exemple, un changement de périmètre après fusion modifie complètement des objectifs de risque préalablement définis : quand AZF Toulouse appartient à TotalFinaElf, sa disparition ne menace en rien le groupe, mais si l'établissement n'appartenait qu'à lui même ou à un petit groupe chimiste, il n'en serait sûrement pas ainsi.

3. Efficacité d'un code de gouvernance

Le rapport ne soulève guère la question. Dans un style très britannique, il suppose que les diverses compagnies seront motivées par les exigences très générales du *Combined Code* et qu'elles sauront le mettre en pratique en fonction de leur situation particulière. Le rôle du contrôle *externe* n'est pas mentionné. Or le séisme Enron et ses répliques ont bien montré que même le contrôle externe pouvait se révéler très inefficace quand l'ensemble de la structure est sous-tendu par une éthique douteuse. Combien plus encore en l'absence de contrôle externe !

Le système proposé représente une sorte d'idéal fonctionnant dans un monde d'éthique solide et de transparence de l'information. Rien ne garantit que le Conseil soit à même de contrôler la Direction comme les 'affaires' américaines (Enron et autres) le démontrent de façon éclatante. Rien ne garantit que 'les marchés' sauront dénouer le vrai du faux dans la communication de l'entreprise comme l'ont montré l'envolée démesurée des start-up et du virtuel et la prolongation de la bulle boursière des TIC.

Ces questions très délicates ne remettent pas en cause les arguments du rapport Turnbull, mais soulignent ses limites pratiques. Sa mise en œuvre par les entreprises britanniques cotées ne semble pas présenter de difficultés particulières : on trouve plusieurs déclarations de telles sociétés sur l'Internet. Néanmoins, il pourrait demeurer une marge entre ces déclarations et la culture du risque de l'entreprise.

L'administration a décidé de suivre aussi les recommandations du rapport ce qui soulève quelques difficultés, par exemple dans les universités. En effet, les membres du Conseil n'ont pas toujours les compétences nécessaires et, n'étant rémunérés que de façon symbolique, ils endossent une responsabilité juridique relativement lourde sans en retirer de profit. Ainsi, l'adoption brutale du rapport Turnbull pourrait conduire certains membres des Conseils des universités à les désertir dans l'avenir.

4. Quelle communication autour des risques ?

Le rapport déclare qu'une telle communication est nécessaire, mais ne pose pas la question de sa nature. Or, il y a là au moins deux grandes difficultés.

La communication descendante qui affiche l'engagement de la Direction et les objectifs de risque est souvent très irréaliste. Elle se base sur des slogans du type zéro défaut : voici, par exemple, la politique QHSE (Qualité, Hygiène, Sécurité, Environnement) de Schlumberger explicitée sur son site :

- no accidents
- no loss to process
- no harmful emissions
- no health-related incidents
- no lapses in security

À part le dernier objectif, tous les autres sont totalement irréalistes et il est fort peu probable que le management les considère comme réalisables. Il s'agit d'affichage. Et cette pratique n'est pas nécessairement mauvaise ; elle peut avoir sur les personnes concernées un impact positif. En général, la communication descendante est de deux types : (1) informationnelle, technique ou moins technique, sur les questions de sécurité, et (2) motivationnelle, incitant chacun à rester raisonnable et vigilant. De plus, toute une série de dispositions doivent rester confidentielles, notamment celles sur la sécurité au sens militaire et au sens du renseignement (espionnage industriel). La communication sur le risque n'a donc rien d'évident.

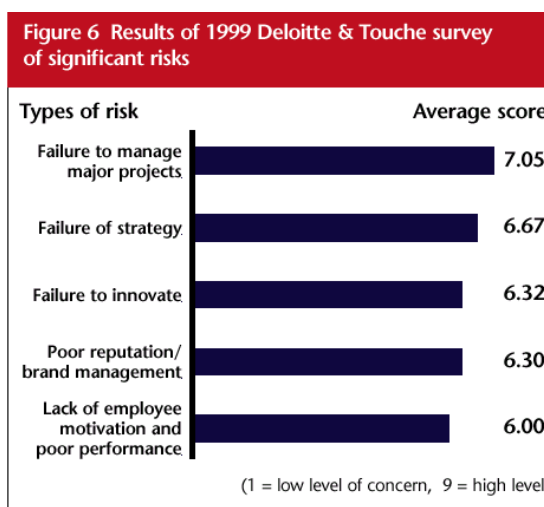
La communication de bas en haut n'est pas plus aisée. Communiquer au Conseil la réalité du risque de terrain est quasi impossible. Il faudrait y vivre. Une inspection sur le terrain, arrivée en hélicoptère, visite en costume, sauf le casque de chantier, petits fours en fin de parcours ne peut aucunement donner le vécu du risque. C'est bien pourquoi, jadis, les jeunes pleins d'avenir passaient des semaines de stage dans les ateliers. Il se dit que Thierry Desmarests, PDG de TotalFinaElf, n'aurait guère été touché par le naufrage de l'Erika, mais que les morts de Toulouse l'ont affecté, provoquant une réorganisation de la gestion du risque dans le groupe. Il est malheureusement bien tard quand la catastrophe étale devant le dirigeant un spectacle affligeant. Un véritable chantier s'ouvre pour répondre à la question : comment représenter les risques de façon appropriée aux divers niveaux de la hiérarchie ?

Malgré les quelques critiques ci-dessus, le rapport Turnbull représente un effort louable vers la prise en compte des risques dans l'entreprise, notamment à ses niveaux les plus élevés. Il restera encore beaucoup à faire quand les recommandations de ce rapport seront entièrement prises en compte.

12. LA SÛRETÉ OCCUPE UNE FAIBLE PLACE AU SEIN DES RISQUES DE L'ENTREPRISE

Le rapport Turnbull évoqué au chapitre précédent a suscité de nombreuses questions des praticiens sur sa mise en oeuvre. C'est pourquoi l'institut des comptables anglais a publié des documents explicatifs qui sont autant de développements pratiques du rapport Turnbull. En particulier, *Implementing Turnbull : A Boardroom meeting*, aborde spécifiquement la gestion des risques en son chapitre 4 (reproduit en annexe 7). On peut y discerner une très faible place des risques technologiques et environnementaux dans les entreprises en général (c'est-à-dire y compris les entreprises n'opérant pas d'installations à risques). C'est ainsi qu'une enquête de Deloitte & Touche indiquait que les risques suivants étaient les plus importants, du point de vue des entreprises :

1. les grands projets,
2. la stratégie,
3. l'incapacité à innover,
4. l'image,
5. la motivation et la 'performance' des employés.



Ni le risque technologique ni le risque environnemental ni le risque produit n'y figurent. Les trois premiers points concernent la capacité de l'entreprise à rester gagnante dans l'avenir. Les deux suivants reflètent l'atmosphère de travail au présent. D'une façon générale, les risques au sens ordinaire du terme ne figurent pas dans ces préoccupations.

De plus, au sein d'une liste de risques (figure 7 de l'annexe) réunie par les auteurs du rapport cité, une seule ligne concerne le risque technologique et le risque environnemental : la ligne '*Physical disasters (including fire and explosion)*'. Sachant que la liste en question comprend... 80 lignes (!), on mesure combien se retrouvent isolés les risques qui relèvent de la sûreté au sens du chapitre 5, c'est-à-dire ceux qui concernent les employés et les riverains, leur santé ou leur survie. La ligne qui les inclut comprend, en priorité, l'incendie et l'explosion qui sont en effet les premiers risques en termes de sinistres recensés par les assurances¹⁷.

Ces indications confirment, au delà de l'intuition qu'on aurait pu en avoir, que la culture de sûreté n'est, en général, qu'une toute petite partie de la culture du risque des dirigeants d'entreprise (voir aussi chapitre 18, prise de décision).

* * *

Sans doute en va-t-il autrement dans les industries à risques, dans les centrales nucléaires, sur les porte-avions, etc. Mais il ne faudrait pas sous-estimer le 'risque' que constituent des dirigeants dépourvus de culture de sûreté. Le cas Enron montre que les dirigeants peuvent représenter le risque majeur pour les retraites des employés (pour le montant perçu après la cessation d'activité, certes, mais aussi pour toute la vie pendant cette période). Il s'agissait là d'un 'risque éthique' et même si les coûts ont été globalement très élevés, il n'y a pas de morts dans l'affaire Enron.

Le cas emblématique en matière de risque technologique reste certainement Bhopal : la maison mère américaine, Union Carbide, avait passé la main à une filiale indienne sans se préoccuper de la culture de sûreté de cette entité. Elle avait cru suffisant que le directeur technique du site ait fait un long séjour dans un établissement américain où il avait reçu une culture de sûreté forte et adéquate. Or la maison indienne était de culture majoritairement financière et son objectif, la mission que lui avait confiée la maison mère, était de réduire les coûts d'un établissement qui perdait de l'argent. Le directeur du site était un gentilhomme bengali, distingué financier proche de la retraite, qui n'avait aucune notion des risques en cause. Le jeune ingénieur de sûreté, de formation américaine, ne faisait pas le poids. Le résultat : 14 000 à 30 000 morts (officiellement 2 500 environ, voir *Il était minuit cinq à Bhopal*, Dominique Lapierre et Javier Moro, Robert Laffont, 2001).

On en conclut qu'il pourrait y avoir place pour une action des pouvoirs publics au niveau de la culture de sûreté des dirigeants — ou plus généralement, au niveau du facteur organisationnel. Par exemple, il pourrait être risqué de scinder EDF et de voir les centrales nucléaires dispersées, vendues à des sociétés aux intérêts majoritairement financiers, avec la perspective d'en voir un jour aux mains de 'coupeurs de coûts', ces managers prestigieux, intrépides, mais irresponsables qui tranchent sans états d'âme dans les coûts ('*cost cutters*') afin d'améliorer la rentabilité à court terme (voir chapitres 14, 15 et 16). Cette action des pouvoirs publics pourrait alors être inspirée par le souci de faire que '*les questions de sûreté bénéficient de l'attention qu'elles méritent*' (définition séminale de la culture de sûreté dans le nucléaire, chapitre 1).

Le rapport Turnbull apporte une première amélioration à la gouvernance du risque, mais pas à la gouvernance de la sûreté.

¹⁷ Le terme '*Physical disasters*' montre bien l'orientation financière du texte. Ce *physical* s'oppose à *financial*. En réalité, les risques incendies et explosion n'ont rien de commun avec des risques physiques comme les tempêtes ou inondations. Ils sont profondément humains.

13. LE RISQUE N'EST PAS UNE AFFAIRE DE SPÉCIALISTES, MAIS L'OBJET DE LA VIGILANCE DE TOUS

On aurait pu penser que le rapport Turnbull (voir chapitre 11), se plaçant au niveau des Directions d'entreprise et des Conseils d'administration, conçoive la gestion des risques comme une affaire de spécialistes. On a souligné l'inspiration financière de ce rapport et l'on sait que dans ce domaine il existe, en effet, de nombreux spécialistes des différents types de risque. Or, il n'en est rien, au contraire, comme l'indiquent les citations ci-dessous extraites du chapitre 5 (reproduit en annexe 8) du document déjà examiné au chapitre précédent (*Implementing Turnbull: A Boardroom meeting*). Non seulement le rapport Turnbull considère indispensables une bonne intelligence générale des risques et une transparence dans la communication, mais il suggère en outre que le traitement de ces risques doit être intégré dans les activités et impliquer l'ensemble du personnel.

Contrairement à d'autres fonctions, il est considéré mauvais de vouloir les externaliser. La théorie économique s'appliquant à des activités ordinaires (nettoyage des locaux, maintenance informatique, etc.) n'est donc pas pertinente en matière de risque.

« Un point important du rapport Turnbull est l'intégration du contrôle dans le fonctionnement normal de l'entreprise à la poursuite de ses objectifs. Plutôt que de développer des systèmes séparés de reporting des risques, il vaut mieux inclure des mécanismes d'alerte au sein des systèmes d'information existants. Des bases de données compliquées dédiées au *risk management* peuvent éloigner du point clé, à savoir que tout le monde, dans l'organisation, soit plus attentif à la réalisation de ses objectifs et à la gestion des risques significatifs pour sa fonction. »

« Modifier les comportements à tous les niveaux de l'entreprise et intégrer de meilleures pratiques à l'activité normale, rend moins nécessaire une multitude de contrôles surajoutés à l'activité productive. »

A major point which Turnbull stresses is that control should be embedded within the business processes by which a company pursues its objectives. Rather than developing separate risk reporting systems, it is best to build early warning mechanisms into existing management information systems. Cumbersome risk management databases can be a distraction from the key point which is that each person in the organisation becomes more focused on meeting the business objectives and in managing significant risks which relate to the tasks which he or she performs.

By changing behaviour at all levels of the company and embedding better business practices within day-to-day activities, there is less need for a multitude of control procedures to be laid on top of the business.

« Un facteur essentiel de succès est que les employés comprennent l'utilité des contrôles et s'approprient ces contrôles. »

Employee understanding of the purpose of controls and a sense of 'ownership' are critical to success.

« Pour inverser la tendance dans une unité à problèmes, il faut généralement disposer d'un engagement affirmé du management et des employés. »

A high level of management and employee involvement in improving risk management and internal control is usually needed in order to turn around a problem unit or department.

« Quand il existe un comité des risques, celui-ci doit éviter d'usurper le rôle du comité exécutif. Il peut encourager et promouvoir une bonne gestion des risques et une bonne intelligence des risques, mais il ne doit pas jouer le rôle de la Direction. »

Where there is a risk committee, it should avoid usurping the role of the executive committee. It can encourage and foster good risk management and awareness, but it should not take over the role of the executive management.

14. GOUVERNANCE ET CULTURE DES ÉLITES : ENSEIGNEMENTS DE LA CRISE DE GOUVERNANCE AUX ÉTATS UNIS

L'avidité imprègne les élites américaines au delà de ce que l'on avait sans doute généralement imaginé¹⁸. C'est ainsi, par exemple, que « en 1973, le PDG moyen d'une 'major' gagnait environ 45 fois le salaire des employés...en 1991, le ratio était de 140. Maintenant, il est de 500 ». Les mécanismes pervers qui ont soutenu la mise en place de cette culture de la cupidité (*greed*) incluent :

- des incitations perverses des stock options sur les dirigeants (incitations que l'on n'avait pas prévues tant les stock options semblaient aligner l'intérêt des dirigeants et celui des actionnaires), mais aussi des incitations perverses du système dans lequel opèrent les dirigeants et qui s'imposent à eux ;
- des pratiques 'créatives' voire des tromperies au niveau de la comptabilité, mais aussi les règles insuffisantes en ce domaine et l'incitation systémique à présenter une image positive ;
- la cupidité des dirigeants, mais aussi un système qui amène progressivement des personnes à l'éthique 'normale' à glisser vers des pratiques finalement désastreuses.

Il est néanmoins trop simpliste de s'en prendre uniquement aux individus, il faudrait réformer l'ensemble du *Greed Cycle*, ce cercle vicieux de l'avidité ou, plus simplement en français, ce 'culte du dollar'. Les solutions, elles, ne sont ni nombreuses ni très convaincantes. Nous concluons en montrant que le MEDD pourrait légitimement s'investir dans les problématiques de gouvernement d'entreprise.

¹⁸ Ce chapitre est basé sur un article de John Cassidy (*The Greed Cycle*, 'The New Yorker', 23 septembre 2002). Cet article est long, 11 pages, mais il se lit d'un trait tant on est stupéfait de l'immensité de l'avidité (*greed*) qu'il révèle avec nombre d'exemples convaincants.

1. Évolution de la culture des dirigeants d'entreprise américains

1.1 Le 19^{ème} siècle : les origines vertueuses de la société par actions

À l'origine de la société par action se trouve le pacte suivant : le dirigeant s'engage à gérer la compagnie dans l'intérêt des actionnaires, dont il fait en général partie, et les actionnaires lui délèguent la responsabilité quotidienne de l'entreprise. Reste à assurer que le dirigeant consacre effectivement suffisamment d'énergie à cette gestion, dispose des compétences nécessaires et qu'il ne détourne pas une partie des revenus qu'il gère par délégation. Aura-t-il, comme disait Adam Smith, « *la vigilance anxieuse* » de celui qui dirige sa propre entreprise ?

Avec le développement de grandes entreprises, par exemple les compagnies de chemin de fer du 19^{ème} siècle, apparut la race des managers, des dirigeants aucunement propriétaires de l'entreprise, ou très peu, mais qui possédaient des compétences précieuses. Ces managers étaient grassement payés en salaires et en retraites et ne s'employaient généralement pas à détrousser les actionnaires et les créanciers. Alfred Marshall pouvait dire, en 1890 : « C'est une preuve solide du merveilleux développement, ces temps-ci, d'un esprit d'honnêteté et de droiture en matière commerciale que les directeurs des grandes entreprises cèdent si peu à la vaste tentation de frauder qui se présente à eux. »

1.2 Le 20^{ème} siècle : comment limiter inefficacité et malversations ?

Hélas, à la fin des années 1920, il était devenu clair que la « *perfidie* » prospérait dans les entreprises. Après le krach de 1929, les enquêteurs du Congrès américain découvrirent des délits d'initié, des manipulations de cours et des abus de biens sociaux sur une grande échelle. Il s'ensuivit une législation de la Bourse et la création de la SEC (Securities and Exchange Commission, équivalent de la COB française).

La confiance revint mais, durant les années 1960-1980, on disait parfois les dirigeants désinvoltes vis-à-vis des intérêts des actionnaires. En général payés en fonction de la taille de l'entreprise, ils étaient poussés « *à construire des empires tentaculaires plutôt que de s'attacher à la profitabilité de l'entreprise.* » Empires logés dans des sièges luxueux, possédant des propriétés d'entreprise et coutumiers de dépenses somptuaires qui se poursuivaient même quand les compagnies étaient en difficulté.

En théorie, les actionnaires peuvent se regrouper et évincer des dirigeants incompetents ou indéliçats, au cas où ils en seraient informés, mais il faut pour cela de l'énergie, du temps et de l'argent. Cela s'est rarement produit. L'inefficacité de certains dirigeants n'était pas non plus contenue par des concurrents qui auraient été plus économes et auraient évité d'installer des « *marbres roses dans les toilettes* ». Il se développa plutôt un mouvement d'idées : les actionnaires devinrent les personnages les plus importants de l'entreprise, avant les dirigeants, les employés ou les clients. Il leur revenait de rémunérer les dirigeants de façon à aligner les intérêts de ces derniers avec ceux des actionnaires.

Il s'agissait d'un saut qualitatif. Auparavant, beaucoup de dirigeants considéraient que leur mission était de veiller au bien-être de leurs employés et de leurs clients. Et tout allait bien tant que la compagnie dégagait un profit raisonnable et payait chaque année un dividende à ses actionnaires. En revanche, à partir du moment où le PDG devient *l'agent* des actionnaires, il ne vit plus que par et pour la valeur actionnariale. Il lui faut maximiser la valeur de l'entreprise *telle que mesurée par la Bourse*.

1.3 Les raids des années 1980

Le mouvement en faveur des intérêts des actionnaires signifiait donc une focalisation sur la valeur boursière. Il n'en fallait pas plus pour attirer des investisseurs riches et offensifs qui utilisèrent cette culture purement financière pour mener des attaques sur les entreprises cotées. Ces raideurs achetaient des entreprises 'sous-évaluées', finançant leurs attaques par l'emprunt, ce qui leur conférait un fort effet de levier. Ayant acquis l'entreprise, ils la géraient ensuite en fonction de leurs seuls intérêts pour faire monter substantiellement le cours de Bourse et pouvoir revendre avec profit. L'intérêt de l'entreprise n'entraînait guère en ligne de compte ; la gestion à court terme se déclinait en réductions, recentrages et autres cures d'amaigrissement.

Près de la moitié des entreprises cotées firent l'objet d'une offre de rachat durant les années 1980. Beaucoup furent contraintes de licencier et de se séparer de leurs divisions les moins performantes pour éloigner les acquéreurs potentiels.

Bien des économistes défendirent ces opérations au nom de l'efficacité : les dirigeants, ployant sous les lourdes charges financières de l'acquisition, seraient contraints, estimait-on, d'améliorer la gestion de l'entreprise. Mais lors de la récession du début des années 1990, nombreuses furent les entreprises qui ne purent survivre à leurs charges. La vague de faillite discrédita ces raids dont beaucoup avaient abouti à ruiner actionnaires et créanciers. La cupidité et la logique financière se révélaient insuffisantes pour améliorer l'efficacité de la gestion des entreprises.

Les dirigeants, quant à eux, conclurent que ceux qui embrassent le credo de la valeur actionnariale deviennent très riches, alors que ceux qui soutiennent leurs employés et leurs consommateurs autant que leurs actionnaires se retrouvent sans emploi.

1.4 Les stock options et l'explosion de l'avidité

Le développement des stock options allait leur donner raison au delà de ce qu'ils imaginaient. Car, le problème de l'intéressement des dirigeants demeurait après la mode des raids. Comme disait en effet, de façon fort exagérée, l'économiste Michael Jensen : « les firmes payent leurs leaders comme des bureaucrates [dont le revenu n'est pas lié au niveau de l'action de la firme] ; est-il étonnant que tant de PDG se conduisent comme des bureaucrates plutôt que comme des entrepreneurs qui maximisent la valeur de la compagnie ? »

En 1980, moins d'un tiers des dirigeants bénéficiait de stock options. L'intéressement passait par les bonus et la participation aux bénéfices. Puis, durant la décennie 1980, les stock options devinrent moins risquées en raison du décollage de la Bourse et furent 'parrainées' par des firmes prestigieuses comme Microsoft et Intel. Elles apportaient enfin la solution miracle permettant d'inciter efficacement les dirigeants à défendre l'intérêt des actionnaires,

En 1994, 7 dirigeants sur 10 recevaient des options ; ces options représentaient environ la moitié de leur rémunération. Dans la seconde moitié des années 90, les 'méga-options' devinrent la norme : des options valant plus de 10 millions de \$. Les PDG n'étaient plus payés comme des bureaucrates, mais comme des rock stars. En 1997, Michael Eisner, PDG de Walt Disney gagnait 570 millions de \$; un an plus tard, Mel Karmazin, Directeur de CBS leva des options d'une valeur de 200 millions de \$.

D'après Paul Volker, ancien président de la réserve fédérale : « La cupidité des dirigeants a explosé au delà de tout ce que l'on aurait pu imaginer dans les années 1990... Les normes

traditionnelles n'existaient plus. Il y avait une véritable culture dans laquelle le seul signe de valeur était combien d'argent on pouvait faire. »

Même dans l'échec. Le Financial Times a examiné les 25 faillites les plus importantes sur les trois années 1999-2001 : les dirigeants de ces entreprises sont partis avec un total de 3,3 milliards de \$. Par exemple, Gary Winnick (Global Crossing, 500 millions de \$), Ken Lay (Enron, 250 millions de \$), Scott Sullivan (World Com, 50 millions de \$), Clark McLeod et Richard Lumpkin (McLeodUSA, environ 100 millions de \$ chacun en stock options levées avant leur chute).

2. De nombreuses incitations perverses

Globalement le système (*'corporate America'*) incite à :

- augmenter la taille des entreprises,
- manipuler les cours de l'action,
- manipuler la rentabilité des stocks options,
- annuler les incitations positives des stocks options,
- oublier la valeur réelle de l'entreprise,
- perdre toute réactivité vis-à-vis des moutons noirs,
- perdre toute lucidité globale,
- ne pas dire la vérité,
- répandre des mensonges optimistes.

2.1 La rémunération des dirigeants à la taille de l'entreprise incite à augmenter la taille

De façon très générale, les dirigeants sont payés en fonction de la taille de l'entreprise. Une plus forte taille permet à l'entreprise de monter les enchères pour se payer les meilleurs dirigeants. Inversement, cette caractéristique « *encourage les leaders à construire des empires tentaculaires plutôt que de s'attacher à la profitabilité de l'entreprise.* »¹⁹

2.2 La rémunération par les stocks options incite à manipuler les cours de l'action

Qui possède des stock options exerçables a une forte incitation à faire monter le niveau de l'action. Les dirigeants peuvent influencer le niveau de l'action par différents moyens à court terme qui n'ont de rapport ni avec la valeur instantanée de l'entreprise ni avec la stabilité des revenus ni avec la création durable de valeur.

Cela commence par une 'culture des bonnes nouvelles', du 'tout va pour le mieux' ; se poursuit avec quelques 'arrangements' avec la réalité ; pour finir en de véritables entreprises de dissimulation et de tromperie à base d'artifices comptables (voir page suivante) et de montages illégaux (affaire Enron).

¹⁹ L'augmentation de la taille de l'entreprise peut être positive quand elle permet des économies d'échelle, mais bien d'autres transformations peuvent se produire et le changement lui-même doit être géré.

Les manipulations comptables

En 1993, Howard Schilit, professeur de comptabilité, dressait la liste des 7 arnaques comptables majeures utilisées par les entreprises :

1. enregistrer des revenus trop tôt, ou de façon optimiste ;
2. enregistrer des revenus fictifs ;
3. gonfler les revenus avec des gains exceptionnels (et laisser croire qu'il s'agit d'une croissance à long terme) ;
4. transférer des coûts vers des années futures ou des périodes antérieures ;
5. ne pas enregistrer des engagements ou les réduire de façon impropre ;
6. transférer des revenus à une période future ;
7. transférer des dépenses futures à la période actuelle en tant que dépense exceptionnelle.

L'entreprise de Howard Schilit produit des alertes comptables depuis 1994 : « *Les problèmes n'ont pas surgi soudainement... ils sont devenus effrayants depuis 1997.* »

Le cas de CUC Cendant

L'entreprise CUC faisait du marketing direct. Ses profits augmentèrent considérablement (elle avait traité ses coûts de marketing comme des coûts de capital ce qui lui permettait de les amortir, arnaque no.4 ; elle avait aussi utilisé des provisions généreuses pour restructuration et qui lui permettaient de gonfler les profits, arnaque no.7). En 1994 et en 1997, Schilit et ses collègues donnèrent des avertissements relatifs à CUC, mais personne ne s'en préoccupa. Le cours de CUC doubla entre septembre 1996 et avril 1998 (18 mois !) alors que CUC fusionnait avec HFS, une grosse entreprise en franchise, et devenait Cendant.

Quand la firme annonça qu'elle avait découvert des irrégularités comptables, une surestimation des revenus de plus de 100 millions de \$, l'action baissa de 50%. En juin 2000, trois employés plaidèrent coupables de fraude. Les dirigeants sont poursuivis pour avoir gonflé les revenus pendant 10 ans.

Cendant est un scandale financier de grande ampleur ayant conduit à 20 milliards de pertes (!) pour les actionnaires. Le cas ne fut guère connu hors des cercles spécialisés.

Le cas de Sunbeam

'Chainsaw' Al Dunlap fut contraint de démissionner de cette entreprise où il avait tranché 'à la tronçonneuse'. En 2001, la SEC (Securities and Exchange Commission) l'accusa de fraude, ainsi que quatre de ses collègues, en particulier d'avoir fait gonfler la valeur de l'action afin de rendre la compagnie plus attractive dans l'optique d'une éventuelle acquisition. Sunbeam se déclara finalement en faillite et ses actionnaires perdirent tout leur investissement.

Le cas de Waste Management

Waste Management est la plus grande entreprise américaine de ramassage de déchets. Le premier avertissement de Schilit fut émis en 1995, mais la valeur de l'action continua à grimper. En juillet 1998, elle fusionna avec une de ses grandes rivales USA Waste Services et l'action atteint un niveau record le printemps suivant. Quelques mois plus tard, la compagnie annonçait qu'elle revoyait sa comptabilité. La SEC lança une enquête et découvrit qu'entre 1992 et 1996 Waste Management avait surestimé ses profits de 1,4 milliards de \$ (!).

Le cas de Lucent

Lucent Technologies était la division équipement de AT&T, 'the bluest of blue chips'. Elle fut introduite sur le marché en 1996 et, en l'espace de trois ans, sa valeur avait été multipliée par 8, elle était devenue l'action la plus détenue des USA. En 1998, Lucent faisait environ un milliard de \$ de revenu net. Les investisseurs anticipaient le même type de croissance pour cette année et Lucent ne faisait rien pour les en dissuader. En réalité ses ventes ralentissaient et ses stocks augmentaient.*

La compagnie inclut dans ses revenus des gains réalisés par son plan de retraite (arnaque no.3), se mit à capitaliser ses dépenses de programmation (arnaque no.4) et créa de nouvelles réserves liées à des acquisitions (arnaque no.7). En février et mars 1999, Schilit émit deux alertes. Comme d'habitude, les investisseurs n'y prêtèrent guère attention. En novembre, l'action valait 80\$.

En janvier 2000, Schilit et ses collègues émirent un troisième avertissement en détaillant les preuves. Une semaine plus tard, Lucent annonçait qu'elle ne participerait pas aux estimations de revenus pour le quatrième trimestre 1999 à Wall Street. L'action chuta lourdement. Deux ans et demie plus tard, elle s'échange en dessous de 2 \$.

* L'expression blue chip désigne des actions de sociétés connues, très honorables, dont les risques sont faibles et dont les perspectives de revenus et de plus values sont donc elles aussi plutôt faibles. En français, ce sont à la fois des actions de 'père de famille' et des 'fleurons de la cote'.

2.3 Le poids considérable des stocks options incite à manipuler leur rentabilité

Sans manipuler l'information qui détermine le cours de l'action, il est possible d'influer sur la valeur initiale des options et sur la rentabilité des actions.

Quelques manipulations liées aux stock options

- les options distribuées *avant* une bonne nouvelle qui fera monter les cours de l'action, mais *après* une mauvaise nouvelle qui a chuté les cours ;
- les prix des options revus à la baisse si l'action baisse : Advanced Micro Devices a ainsi revu six fois à la baisse le prix d'exercice des options de son fondateur, lui permettant de lever des millions de dollars alors que le prix de l'action baissait ! En 2000, Larry Ellison, fondateur d'Oracle, levait 700 millions de \$ d'options à bas prix ;
- les rachats d'actions : les entreprises rachètent leurs propres actions pour ensuite les annuler ce qui, réduisant le nombre d'actions, fait monter le revenu par action.

2.4 L'utilisation perverse des stock options annule leur incitation positive

En effet, si les prix d'exercice des options peuvent être revus à la baisse en cas de baisse de l'action, comme dans les exemples de l'encadré ci-dessus, les dirigeants peuvent s'assurer des revenus très confortables quel que soit le résultat de leur gestion. « *Quand l'action de la firme se comporte bien, les responsables empochent autant que les gagnants du loto. Mais quand les cours chutent, ils ont une nouvelle possibilité de gagner ! Le montage, dans son audace et sa logique est presque magnifique.* » (John Cassidy). En combinant volatilité des cours et possibilité de modifier le prix des options : « *on crée une machine à faire de l'argent, un appareil anti-gravitationnel qui garantit que les hauts dirigeants deviendront richissimes* ». (Graef Cristal, 'expert en rémunération des dirigeants').

2.5 Le diktat des cours fait oublier la valeur réelle de l'entreprise

Plus grave, certains dirigeants (tel le fameux 'chainsaw' Al Dunlap, voir l'article de Time en annexe 9) pratiquent une forme de destruction de l'entreprise : réduction drastique de coûts, y compris licenciement de milliers de travailleurs, au mépris des conséquences à long terme sur la valeur de l'entreprise ; dans le court terme, les coûts sont effectivement réduits et, les profits décollant, les cours de l'action s'envolent.

2.6 Un marché haussier fait perdre toute réactivité vis-à-vis des moutons noirs

Quand un marché haussier fait rage, les investisseurs perdent beaucoup sur des entreprises comme Cendant (voir encadré), mais comme le dit l'article dans un style bien américain, les conseillers disent : « *OK, Joe. La fraude, ça peut se produire. Mais vous avez beaucoup gagné sur les cinq transactions précédentes que je vous ai apportées.* » Les investisseurs grincent des dents et disent : « *Oui, je me suis fait avoir cette fois-ci, mais j'ai effectivement touché beaucoup d'argent sur les cinq autres affaires.* » Il y a des moutons noirs, mais le système reste globalement rentable. Ou, plus précisément, il y a des signaux précurseurs, mais on ne sait pas quand viendra la chute généralisée...

Si l'ensemble des acteurs — conseillers, investisseurs, banquiers, et même certificateurs et agences de notation —, si tous profitent du marché et ne demandent pas de comptes, il ne reste qu'une autorité²⁰ très isolée pour tenter de réagir... En tous cas jusqu'à la généralisation des difficultés, après quoi il sera bien tard.

2.7 Un marché haussier fait perdre toute lucidité globale

Quand un marché haussier fait rage, les incitations à la prudence ont peu de prise sur les investisseurs. C'est ainsi que sur les cinq années 1996-2000, les profits des sociétés américaines mesurés par la comptabilité nationale américaine atteignaient un sommet en 1997 pour baisser ensuite fortement en 1998 (-10%) et ne retrouver les niveaux de 1997 qu'en 2000. En revanche, le revenu moyen par action augmentait régulièrement de 39 \$ à 55 \$. Il est hautement probable que les entreprises utilisèrent nombre de subterfuges plutôt que

²⁰ En France, la COB (Commission des Opérations de Bourse) considère que son rôle n'est pas d'alerter sur des niveaux excessifs de la Bourse.

d'admettre que l'augmentation des salaires et l'intensité de la concurrence érodaient leurs profits.

On mesure le dilemme de l'investisseur lucide : il sait que tout cela se terminera mal, mais il ne sait pas quand. Comme dans le concours de beauté de Keynes²¹, rien ne sert d'avoir raison, il faut 'suivre' et 'le marché a toujours raison'.

2.8 Les réactions excessives et myopes des marchés n'incitent pas à dire la vérité

Quand une entreprise admet que ses profits ne croissent pas aussi vite qu'attendu, l'action est punie et les dirigeants cloués au pilori.

2.9 Les marchés récompensent les mensonges optimistes

En effet, le cours monte ce qui permet aux dirigeants qui détiennent des options de les exercer avec profit, surtout s'ils sentent que les cours peuvent se retourner à la baisse. Ces deux derniers effets pervers sont particulièrement dévastateurs. « *On entraîne les managers en les pénalisant quand ils disent la vérité et en les récompensant quand ils mentent ! Ce type de comportement contraire à l'éthique s'étend ensuite à toutes sortes de domaines* ». (Michael Jensen).

3. Plutôt un problème systémique que les excès d'une mafia de forbans

En résumé, au lieu d'inciter les dirigeants à construire des sociétés capables de produire de la valeur pour des décennies, un ensemble d'incitations perverses les encourage à gérer à court terme, à aligner leur action sur les exigences des analystes financiers, et trop souvent, à devenir des escrocs.

Jensen considère que les dérives décrites ci-dessus, plus les autres (Enron, WorldCom, Global Crossings, etc.), sont le résultat d'un système plus que l'émergence d'une perversité des individus, nouvelle et singulièrement plus virulente que dans le bon vieux temps. Dans un papier avec Joseph Fuller (*Just Say No to Wall Street*, http://www.monitor.com/binary-data/MONITOR_ARTICLES/object/136.pdf) il souligne que « Enron était, sur de nombreux points, une entreprise extraordinaire, pouvant s'enorgueillir de nombreux actifs, de véritables réussites, d'innovations étonnantes et d'un avenir prometteur. » Mais sa valeur de marché était très excessive, presque 70 milliards de \$ en août 2001. Pour la justifier, les analystes de Wall Street exigeaient des revenus toujours plus élevés et les dirigeants s'employaient à les satisfaire. « Si le management d'Enron avait accepté la confrontation avec les analystes, avec courage et conviction, s'il avait résisté à leur pression continuelle en faveur d'une croissance hors norme des profits, l'entreprise aurait évité d'avoir à mener des actions douteuses pour plaire aux analystes et aux marchés ». « Elle aurait très bien pu devenir une entreprise moins sur-évaluée mais stable et rentable ».

²¹ Keynes utilisa l'exemple frappant des concours de beauté dans les journaux britanniques. Des photos de jeunes femmes étaient publiées et il fallait choisir 'les plus belles' ; ceux qui trouvaient la bonne réponse gagnaient ; or la bonne réponse était précisément le choix majoritaire des lecteurs qui répondaient au concours. Par conséquent, le problème n'était pas vraiment de trouver 'les plus belles', mais de prévoir ce que répondraient la majorité des répondants. Il en est de même en Bourse.

Tous ces patrons n'étaient pas nécessairement des champions de la duplicité et de la vénalité. Jensen pense que des hommes honnêtes ont été soumis à des pressions nombreuses, à des forces très puissantes, à un système qui s'est constitué graduellement et qu'il était donc difficile de comprendre parfaitement.

Il est clair que les économistes et les financiers ont participé à la constitution de ce système avec aussi peu de lucidité que ses acteurs directs aujourd'hui confrontés à la justice. C'est le même Jensen qui était l'avocat des raids et des stock options... Rétrospectivement, il apparaît clairement qu'un libéral étroit fait une apologie myope des marchés, négligeant leurs possibles effets pervers, militant sans lucidité pour une intervention minimale des régulateurs. Au contraire, un libéral intelligent comprend que c'est dans des circonstances données et dans des conditions bien précises qu'un marché peut effectivement constituer un puissant outil de coordination des acteurs. Il recommande donc une régulation vigilante qui permette précisément d'assurer ces conditions favorables.

Les intellectuels ne furent pas les seuls coupables. La plupart des acteurs du système faisaient de bonnes affaires : les certificateurs payés par les certifiés, les actionnaires choyés par les dirigeants (les financiers, mais aussi les salariés et les dirigeants), les agences de notation qui préféraient ne pas déplaire et ne pas écouter les lanceurs d'alertes, les créanciers bénéficiant grassement du business des émissions de titres, etc. Et quand tout le monde trouve son compte dans un système, peu nombreux sont ceux qui prennent le risque de le critiquer.

4. Des solutions ?

John Cassidy suggère que beaucoup d'articles de presse ne vont pas plus loin qu'une explication basée sur la rapacité et le mensonge, mais que néanmoins nombre d'acteurs comprennent l'aspect systémique de la crise et encouragent des réformes propres à modifier le système. Il cite essentiellement trois réformes :

1. améliorer les règles comptables,
2. supprimer les stock options,
3. menacer systématiquement de poursuites pénales.

1. Ces solutions ne sont pas dénuées de difficulté. Par exemple, des professionnels américains de la comptabilité pensent qu'il est impossible de créer un système 'étanche' de règles comptables (voir note D1-02-72, *Enron : quelques idées pour améliorer la certification*). Il semblerait tout aussi utile de donner autant de poids à des instituts d'alertes comptables qu'aux agences classiques de notation dont l'efficacité s'est révélée déplorable dans la crise de gouvernance des sociétés américaines, mais aussi lors de la crise des marchés asiatiques, de la Russie, etc.

2. La suppression des stock options est une solution extrême²². Elle ramènerait au premier plan la question du respect des actionnaires par les dirigeants (le problème principal-agent²³). Moins extrême, une réglementation serrée des stock options pourrait être judicieuse :

²² Elle est pourtant, d'après Cassidy, prônée par Paul Volker, ancien patron de la Réserve Fédérale américaine qu'on ne peut guère soupçonner d'être un dangereux gauchiste.

²³ Un pan de la théorie économique qui envisage les rapports entre agents qui ne possèdent pas la même information, typiquement un 'employeur' (les actionnaires) qui emploie un agent aux pouvoirs non négligeables (le PDG).

publication nominale des attributions de stock options, indexation sur un indice pertinent des actions ; attributions non de stock options à court terme (trois ans) mais de plans à long terme de stock options exerçables sur 10 ou 20 ans à raison d'un montant fixé par année ; publication des dates et montants d'options exercées par les dirigeants et surveillance par les autorités, etc.

Néanmoins, le gros défaut des stock options est que la valeur de l'action n'a qu'un rapport assez lointain avec la valeur de l'entreprise. Comme dit Volker : « *Dans un marché haussier, tout le monde est récompensé — les bons, les brutes et les truands —, dans un marché baissier, personne. Pourtant, tous ne sont pas des génies quand le marché grimpe ni des cancrenards quand il plonge.* »

Un autre défaut est que les stock options ne sont pas des dépenses de l'entreprise comme le seraient des salaires ou des primes. Du point de vue de l'entreprise, les options cédées aux dirigeants sont gratuites. Leur montant ne modifie en rien les profits que l'on annonce aux actionnaires. Même l'effet de dilution ne peut être clairement pris en compte puisque les options ne seront pas obligatoirement exercées ou bien le seront à une date inconnue. La transparence est minimale.

3. Le recours à la justice pénale ne doit pas être écarté, mais on n'oubliera pas la difficulté technique de certaines investigations, les possibilités d'erreurs judiciaires, les possibilités de manipulation de l'image d'une personne par le biais d'accusations qui finiront par se révéler infondées, les délais inhérents à la justice...

Plus fondamentalement, l'enjeu semble être :

1. de rééquilibrer la place des actionnaires et autres parties prenantes dans les entreprises, un considérable défi politique qui aboutirait à faire baisser le poids des financiers dans la vie économique ;
2. d'améliorer de façon très significative les méthodes d'évaluation de la valeur des entreprises, un considérable défi intellectuel ;
3. d'imaginer des systèmes d'incitations efficaces et dépourvus d'effets pervers à l'intention des dirigeants d'entreprise.

5. Enseignements pour le MEDD

Sur le premier point, le MEDD est intéressé au titre des accidents technologiques, d'une part, et au titre de la protection de l'environnement, d'autre part. On pourrait soutenir que, de façon générale, dans tous les pays, le Ministère chargé de l'environnement pourrait utilement représenter les parties prenantes liées à ces risques.

Un actionnaire qui optimise son portefeuille n'a actuellement que peu de raisons et de moyens de se préoccuper de risque technologique ou de risque environnemental. Cela n'exclut pas que certains actionnaires, ne se contentant pas uniquement d'optimiser leurs portefeuilles, tentent d'utiliser leur capital pour peser sur les orientations de la société, par exemple par l'intermédiaire de fonds verts ou de fonds 'socialement responsables'. Il peut, en effet, exister des actionnaires citoyens. Mais les pouvoirs publics peuvent-ils en rester à ces considérations optimistes ? Il est probable que les électeurs et 'la société civile' ne le pensent pas.

On peut, par exemple, citer à la rescousse l'avocat Jean-Michel Darrois qui s'exprimait ainsi lors d'une rencontre débat organisée par le barreau de Paris et 'La Tribune' (voir La Tribune du 4 octobre 2002) : « *Il y a une sorte de théocratie actionnariale qui s'est emballée au détriment de l'attention portée aux salariés, clients, fournisseurs, banquiers. Cette prédominance culturelle de l'actionnaire a fait qu'on est allé imposer aux dirigeants des normes s'écartant de la logique économique, comme le retour de 15% sur fonds propres.* » Il pourrait être opportun que le MEDD soutienne un rééquilibrage du gouvernement d'entreprise, par exemple en expliquant la logique de ce rééquilibrage au niveau interministériel.

S'agissant du second point, « améliorer de façon très significative les méthodes d'évaluation de la valeur des entreprises », il pourrait constituer un axe de travail de la D4E. La légitimité de ces travaux s'appuierait sur une orientation politique du type de celle décrite ci-dessus.

Quant au troisième point, « imaginer des systèmes d'incitations efficaces et dépourvus d'effets pervers à l'intention des dirigeants d'entreprise », la transparence doit être recherchée. Dans le domaine de l'efficacité de la gestion privée, on rejoint la nécessité de bonnes méthodes de mesures de la valeur. Pour ce qui concerne les pouvoirs publics, cette transparence peut concerner les systèmes de gestion de la sécurité, la gestion de la qualité environnementale, les plans de couverture du risque par l'assurance classique et autres méthodes apparentées à l'assurance. La participation du public à des comités locaux d'information est une façon de favoriser cette transparence (voir aussi la note D1-01-145, *Charles Perrow : La participation au service de la sûreté*)

15. OBJECTIFS DE SÛRETÉ ET OBJECTIFS DE COÛT

LE SYSTÈME DE PRODUCTION TOYOTA RÉDUIT LES COÛTS ET AMÉLIORE LA QUALITÉ ET LA VARIÉTÉ DES MODÈLES

Assurer la sûreté est une exigeante discipline quotidienne, à l'opposé de la réalisation ponctuelle d'objectifs imposés de l'extérieur, par exemple des objectifs financiers. Or, la gestion par les objectifs financiers est très répandue. Le chapitre précédent donne de nombreux exemples d'objectifs financiers imposés par le marché (directement ou indirectement sous la forme d'obligations intégrées dans l'esprit des managers). Ces objectifs globaux doivent alors être traduits sur le terrain, dans les bureaux et dans les ateliers. D'où les 'programmes de rigueur', les 'cures d'amaigrissement', les 'licenciements mondialisés'.

La question se pose, face à l'emprise de ce modèle, de savoir s'il est possible d'être efficace autrement ou si l'adoption de la gestion financière est inéluctable. Si c'était le cas, on devrait être inquiet en matière de risques, car ce n'est pas à base de suppressions et de pressions répétées sur les moyens disponibles que l'on peut parvenir à améliorer la sûreté au quotidien dans les installations à risques. C'est au contraire à une action de construction que l'on doit s'attacher pour améliorer la gestion des risques : construire une connaissance, une intelligence et un sens des risques. Or, précisément, l'exemple de Toyota montre qu'il est possible de gérer en reconnaissant la valeur du système de production en place, en cherchant à améliorer ce système, cet organisme, cet ensemble fin de relations, en reconnaissant qu'il s'agit d'une construction plus organique que mécanique, où l'on ne peut pas impunément changer les éléments, réduire les ressources, pousser les performances à la limite.

Ce qui suit est issu de l'ouvrage de Johnson et Bröms, *Profit Beyond Measure*, traduit en français sous le titre *La Méthode MBM : le Management Basé sur les Moyens*. Cet ouvrage a été salué par le prix Shingo 2001. Johnson, considéré comme un des meilleurs connaisseurs du système Toyota, grand familier de l'usine Toyota du Kentucky, prétend que la majorité des analystes ne comprennent pas ce système, car ils n'imaginent pas une philosophie différente de l'industrie. Toyota n'est pas un constructeur comme les autres, ainsi que le montrent les coupures de presse réunies en 10. Il assure une grande qualité de fabrication ainsi qu'une grande variété des modèles, à des coûts plus performants que de nombreux autres producteurs et ce depuis de nombreuses années. Il est nettement plus rentable que les 'Big Three' à savoir General Motors, Ford et Chrysler.

Les cinq points forts du système Toyota

1. **Tempo (takt time)** : l'usine fonctionne à un rythme donné variant de 80 secondes par véhicule à 55 secondes par véhicule. Tous les postes de travail sont alignés sur ce rythme qui est comme le battement cardiaque de l'usine (ou le tempo d'un ensemble musical). Ce tempo variable donne une grande souplesse à la machine dans son ensemble : de 337 unités produites en huit heures au rythme de 80 secondes par véhicule, à 490 unités pour un rythme de 55 secondes par véhicule (soit + 45%). Cette souplesse permet d'adapter le rythme de l'usine à la demande. De tels ajustements sont toujours menés de façon progressive.
2. **Standardisation du travail** : ces standards sont déterminés poste par poste, conjointement par les travailleurs et les ingénieurs qui les encadrent. L'encadrement estime que les travailleurs ont des idées raisonnables et sont bien informés. Les échanges sont encouragés. L'établissement des standards est guidé par un ordre de priorité : sécurité du travailleur (et ergonomie) ; qualité client ; productivité ; coûts²⁴. Les standards sont fréquemment modifiés, les travailleurs étant encouragés à faire des remarques et à participer à ce travail d'amélioration en continu.
3. **Alertes au niveau des postes** : il est possible d'interrompre le processus de production soit par des automatismes (montés sur les machines et qui se déclenchent en cas d'anomalies), soit par intervention humaine. Celle-ci est prévue par l'intermédiaire du câble *andon*, un câble qui parcourt toute la chaîne, à portée de main des travailleurs en poste, comme dans les anciens autobus pour demander l'arrêt. Cette caractéristique permet la mise en pratique d'intervention rapides.
4. **Le juste à temps** : pour travailler sans gaspillage et avec souplesse, on ne démarre une production que quand une commande a été reçue. Ce principe est décliné entre les différents postes de l'usine : un poste aval passe commande à un poste amont pour réaliser le travail correspondant à un ordre qu'il a lui-même reçu d'un poste situé en aval ou, en bout de chaîne, reçu du client. Les postes adjacents sur la ligne de production sont donc dans des relations client-fournisseurs dont l'ensemble de la chaîne transmet la commande client, irriguant toute la production par la demande finale. Ce système très naturel se rapproche de nombreux fonctionnements du vivant. Le flux informationnel et le flux physique demeurent intimement liés, par construction.
5. **Répartition équilibrée des diverses fabrications dans le temps** : la succession de différents modèles à produire sur une même chaîne devrait, a priori, surcharger temporairement certains postes, alors que d'autres seraient mis en 'chômage technique'. Toyota choisit d'espacer régulièrement les modèles ; par exemple, s'il faut produire 75% de modèles sans air conditionné et 25% avec air conditionné, ce dernier modèle sera programmé *tous les quatre véhicules* (et non pas en bloc dans le dernier quart de la journée).

²⁴ La priorité est la forme la plus simple de l'analyse multicritère. Il est probable qu'en cas de besoin l'ordre mentionné ici peut être modifié. Ce qui implique chez Toyota une forme d'optimisation multicritère informelle et décentralisée.

Souplesse et réactivité au service de la qualité et de la récupération des erreurs

La standardisation (point fort 2) permet aux travailleurs de détecter plus facilement les anomalies et les erreurs. La possibilité d'alertes (point fort 3) permet d'y remédier rapidement. L'immense majorité des erreurs sont traitées rapidement, elles ne sont pas signalées pour être traitées plus tard par des 'réparateurs' spécialisés. Cette capacité de détecter les anomalies et d'y remédier rapidement améliore la compréhension de l'opérateur. Elle aboutit à une récupération efficace des erreurs et à un apprentissage des aspects imprévus du process.

Avec l'équilibrage des fabrications (point fort 5), le choix stratégique de la souplesse est poussé très loin, il devient partie intégrante du quotidien. L'habitude structurelle de la souplesse au poste de travail aide beaucoup dans le cas de perturbations imprévues et pour le passage à de nouveaux modèles. Elle réduit la monotonie du travail 'à la chaîne' et la pression qu'il fait peser sur les opérateurs. Accomplir toute une série de variations dans la même journée, favorise un meilleur apprentissage, une meilleure expertise et beaucoup de soin apporté à la réalisation de chaque unité produite.

Les *feedbacks* constants font partie du système, par construction, comme chez les organismes vivants. Chez ces derniers, un système immunitaire détecte en permanence les éléments étrangers. Il les traite en continu. Il n'attend pas un 'rapport' qui serait produit par un 'système d'information centralisé' et ne serait disponible que plus tard, avec un décalage dans le temps. De même, le système Toyota détecte naturellement les anomalies et remédie en continu aux inévitables erreurs humaines. Ce processus n'est ni centralisé ni bureaucratique ; il découle de la fine ingénierie des relations entre les divers postes de travail. L'activité produit elle-même l'information, en continu. D'où une grande robustesse du système.

La continuité des processus naturels du vivant nécessite des dispositifs assurant la souplesse de leur fonctionnement. Ainsi, proche des systèmes vivants, la chaîne Toyota est-elle divisée en sections séparées par un tampon de cinq ou six voitures. Ceci permet, lors d'une alerte mineure (de moins de 10 minutes environ), de ne pas interrompre toute la chaîne. L'ensemble de l'usine ne s'arrête que pour des interruptions supérieures à deux heures. La souplesse ainsi réalisée réduit les coûts en permettant aux ouvriers d'interrompre le travail pour corriger les erreurs et traiter les anomalies.

La maîtrise d'une telle forme de production requiert probablement un long apprentissage du groupe humain que constitue l'usine.

Production et information

Le système Toyota instille un sens de l'harmonie et de la perturbation, de l'ordre et du désordre. Il ne nécessite pas de 'système d'information' surajouté : l'information émane naturellement du flux d'activité, en temps réel. Par exemple, l'équilibrage des programmes d'activité (point fort 5) est étendu aussi loin que possible en amont de la chaîne de montage vers les processus de fabrication des pièces nécessaires. L'information que constitue la commande du client doit irriguer la production le plus en amont possible.

Pas de système de coûts standardisés, pas de variance de coûts standards, pas de '*Management Ressource Planning*', pas d'informatique d'atelier. Les résultats ne sont pas des objets indépendants à gérer en manipulant le système d'activité à partir de l'extérieur. Les résultats sont incorporés dans l'activité, dans les détails des opérations de production. Ils ne sont pas des abstractions généralisables imposées d'en haut.

Tout employé comprend le système, les résultats sont immanents dans le travail. Chacun peut répondre de façon autonome. La réactivité et la flexibilité assurent que la variété et la qualité puissent émerger au coût le plus bas.

Au niveau de la comptabilité, les activités de l'usine sont considérées comme une boîte noire. La comptabilité calcule les coûts sans entrer dans la boîte noire, à partir des données globales : intrants matériels, nombre de travailleurs, nombre de véhicules produits, etc. La comptabilité *mesure* l'activité globale de la boîte noire sans jamais *déterminer* son fonctionnement interne : le design des véhicules, le plan de l'usine, le type de machines, etc. Comme dit le contrôleur financier : « Il n'y a jamais eu de système de coûts standards et il n'y en aura sans doute jamais. »

Le contrôle des coûts est assuré par la maîtrise du système de production Toyota : accomplir chaque étape en respectant le tempo d'ensemble ; respecter les procédures standard ; identifier les anomalies et les corriger dès qu'elles surviennent ; ne travailler qu'en réponse à la commande d'un client ; répartir les divers modèles à produire aussi également que possible dans la journée. En se focalisant sur la réalisation d'une activité harmonieuse et ordonnée, les coûts restent naturellement sages.

Le tempo de production respecte les ouvriers. La responsabilité de la sécurité et de la qualité repose sur les eux. Les dirigeants ne mettront jamais en péril la sécurité ou la qualité en ordonnant d'accélérer la chaîne.

La responsabilité des quantités et des coûts des produits revient aux dirigeants. Ils s'en acquittent non pas en manipulant les opérations de production, mais lors de la conception des véhicules, en fixant un objectif de coût, à savoir le coût maximal que la compagnie peut supporter. Un élément clé des calculs est bien évidemment le coût des opérations de production menées à l'intérieur de la boîte noire. Il est estimé à l'aide de tableaux de coûts par type d'opération standard et de temps de fabrication. Par conséquent, les opérations de fabrication sont envisagées dans le détail dès la phase de conception, ce qui fournit des données de coût extrêmement détaillées dès avant le début de la production. Pratiquement aucune de ces données n'émane de la comptabilité classique ou d'un système de contrôle de gestion financier.

Symbiose entre direction et employés

Le management ne consiste donc pas à *éliminer* le gaspillage ou les activités qui ne créent pas de valeur par des programmes de réduction, de lissage ou d'amaigrissement. Rien n'est plus éloigné de l'esprit Toyota. On s'y efforce, au contraire, de maîtriser des pratiques qui *évitent* systématiquement le gaspillage. Si on devait découvrir des symptômes de gaspillage ou d'excès d'investissement, on rechercherait les écarts au système pour y remédier ; on ne s'embarquerait pas dans des plans de licenciement ou d'élimination des ressources. C'est la maîtrise du système et de ses pratiques qui produit les hautes performances de l'entreprise, pas le ciblage répété d'objectifs définis par le résultat financier final.

La stratégie d'amélioration constante de la productivité se concentre sur la réalisation du travail en moins de temps sans déséquilibrer les rythmes établis. Il ne s'agit pas d'augmenter le tempo et de travailler plus vite. Les travailleurs savent que la stratégie d'amélioration continue leur ouvre des possibilités, par exemple de promotion. Ils n'ont pas à craindre que leurs trouvailles les amènent, à terme, à se retrouver licenciés. Au contraire, Toyota crée continuellement de nouveaux emplois en *internalisant* des tâches et en aidant leurs sous-traitants à appliquer le système Toyota, allant jusqu'à former des équipes à *cette seule fin*.

16. LA SÛRETÉ PEUT-ELLE ÊTRE GÉRÉE DE LOIN PAR OBJECTIFS FINANCIERS ?

LE MANAGEMENT BASÉ SUR LES MOYENS OFFRE UNE ALTERNATIVE CONCEPTUELLE AUX MODÈLES DE LA GESTION PUREMENT FINANCIÈRE

Ce chapitre s'attache à exposer le Management Basé sur les Moyens (MBM) et ce que cette notion peut apporter pour éclairer les points de vue sur la gestion de la sûreté. Le MBM est défini dans le livre de Johnson et Bröms, *Profit beyond measure* (The Free Press, 2000), traduit en français sous le titre *La Méthode MBM : le Management Basé sur les Moyens*. Il est opposé au MBR, le Management Basé sur les Résultats, à savoir les résultats comptables globaux. L'exemple phare du MBM fait l'objet du chapitre précédent qui détaille les spécificités du système de production Toyota.

D'après *Profit Beyond Measure*, « la plus grande variété (de modèles produits chez Toyota) n'y est pas un frein à l'efficacité ; en fait, elle y améliore l'efficacité et la productivité ». Ainsi, l'attention portée au système de production est une façon de sortir par le haut des dilemmes économiques. En effet, à système de production donné, la demande pour plus de variété de production et de qualité des produits implique nécessairement des coûts supplémentaires. L'exemple de Toyota montre qu'en soignant le système de production, il est possible d'échapper à ces contraintes. Modifier les systèmes de production, c'est mettre en œuvre l'innovation. Il ne s'agit ici ni d'innovation produit ni d'innovation 'process' au sens strict, mais plutôt d'innovation d'organisation et de culture.

Dans le domaine du risque, les HRO (High Reliability Organisations) mettent en place des systèmes appropriés à la nature très risquée de leur activité perçue comme telle. La confrontation avec le risque y produit de hauts niveaux de qualité (voir chapitre 19, *Gestion des risques et management de la qualité*).

D'après *Profit Beyond Measure*, l'amélioration mentionnée provient « d'économies de proximité » plutôt que d'économies d'échelle, en regroupant dans un même lieu les différentes phases du processus de production, par une attention aux « détails de la façon dont chaque travailleur, à chaque poste contribue à satisfaire la commande de chaque consommateur ». Une bonne gestion des risques technologiques et une bonne gestion de crise doivent également se baser sur « l'attention portée au système de production », sur « l'innovation d'organisation et de culture », et par « une attention aux détails de la façon dont chaque travailleur fonctionne ». Donc, précisément sur des approches du type envisagé par *Profit Beyond Measure*, et appelées MBM — Management Basé sur les Moyens .

Ce sont des approches constructives, semblables aux approches qualité, qui devraient permettre de bâtir la culture de sûreté et l'intelligence du risque. La stratégie MBM (par exemple Toyota) vise à instiller en chacun (y compris les fournisseurs) un engagement profond à maîtriser une approche ordonnée du travail. On trouve des idées très similaires dans les textes relatifs à la culture de sûreté des opérateurs du nucléaire (chapitre 1). La qualité est intégrée au travail que chacun effectue. C'est le contraire d'un système où le coût est

minimisé par le recours à une chaîne ‘de base’ (l’assemblage taylorien caricatural) à laquelle on rajoute un impératif de variété qui impose en cascade : une production par lots importants (pour garder les avantages de coût), des stockages importants (car de nombreux lots importants ne peuvent être écoulés simultanément), un système de management ‘rajouté’, une gestion complexe des pièces et des stocks de pièces. Bref c’est le contraire d’un système mécanique — et pour caricaturer, le contraire d’une usine à gaz...

Ce qui explique que, dans un système MBM, on ne peut pas — et on ne veut pas — en changer un élément de façon isolée dans le but ponctuel d’améliorer les performances à court terme. Le MBM vise à créer un organisme intégré où les ouvriers ont la place d’organes vivants et où la direction ne travaille pas contre les ouvriers, mais contribue plutôt à optimiser leur production.

La gestion du risque appelle une ingénierie détaillée des relations de production, incluant les capacités individuelles de travailleurs à part entière, et se fondant sur la contribution de chacun. Toyota a découvert qu’il est plus profitable d’investir dans le personnel, pour en faire des hommes et des femmes informés, responsables, capables de prendre des décisions, plutôt que d’investir en capital dans de nouvelles machines et autres ressources générales. Son exemple indique que la production peut y trouver bien des avantages au niveau de la qualité et de la motivation des employés.

Historique du Management Basé sur les Résultats (MBR)

DuPont après la Première Guerre Mondiale ou General Motors dans les années 1920 ont cherché à exploiter plus efficacement les multiples brevets ou marques qu'elles détenaient. Elles ont créé à cette fin des départements spécialisés sur un marché ou un produit unique, indépendants sauf qu'ils ne pouvaient ni lever de capital ni choisir leur direction. Ces deux prérogatives demeuraient l'apanage du groupe.

La direction centrale pratiquait un 'management basé sur les résultats' (MBR) : elle utilisait les données comptables — littéralement le bilan et le compte d'exploitation — pour piloter les chefs de département. Les parties de l'entreprise devenaient des centres de profit ou des centres d'investissement dont les dirigeants étaient jugés par d'autres dirigeants (pas encore par les marchés financiers). On pouvait prendre les décisions en ignorant les produits, les techniques ou les clients de l'entreprise ; il suffisait de comprendre les subtilités du reporting financier. Pas étonnant que, dans les années 1970, les dirigeants aient majoritairement été d'anciens comptables ou auditeurs plutôt d'anciens ingénieurs, designers ou commerciaux.

Les dirigeants qui 'obtenaient des résultats' financiers étaient très demandés. Ils passaient fréquemment d'une entreprise à une autre, d'un secteur à un autre, d'un marché à un autre. Pour 'faire bonne figure financière', les chefs de département faisaient appel à des universitaires professeurs de comptabilité qui leur montraient comment piloter l'entreprise par objectifs financiers. Une synergie se développa entre le management comptable enseigné dans les universités et les pratiques des contrôleurs en entreprise, donnant au management comptable une vie propre et modelant la façon dont les dirigeants pilotaient leurs entreprises.

À partir des années 1970, les managers ont de moins en moins l'expérience de l'atelier, de la vie des diverses divisions de l'entreprise. Dans l'industrie, mais aussi dans les administrations, les universités et les entreprises du monde entier, les dirigeants gèrent indirectement, depuis leurs bureaux, par l'intermédiaire d'indicateurs et de modèles abstraits. Au lieu de s'attacher à la façon dont *l'activité elle-même* est organisée et à l'impact de cette organisation sur les résultats, les managers de formation financière se sont focalisés sur les résultats financiers en supposant que *la production suivrait*. Ils ont considéré les personnes et les divisions de l'entreprise comme des pièces de mécano à utiliser, ou non, pour atteindre des objectifs financiers abstraits. C'est le management basé sur les résultats (MBR).

L'historique récent et les conséquences de cette culture ont été développés au chapitre 14 *Gouvernance et culture des élites : enseignements de la crise aux USA*.

Le MBR est simplificateur

Aujourd'hui, la plupart des managers croient donc que la meilleure façon d'atteindre un objectif financier global au niveau de l'entreprise est d'attribuer à chacune des unités des objectifs quantitatifs locaux dont la somme correspond à l'objectif global. Le tout est considéré comme égal à la somme des parties.

Dans cette simplification, les relations entre les parties, la fine ingénierie de la production, tendent à être négligées. Le quantitatif tend à prendre le pas sur le qualitatif, la focalisation sur le chiffre simple (additionnable) constitue une simplification drastique de la réalité et propage des vues simplistes. La complexité du réel étant ignorée, ses potentiels ne peuvent pas être exploités. Il en résulte de graves pertes de capacité ainsi que de vastes gaspillages, par exemple 'l'usine parallèle' que constitue le système de gestion informatisée des données.

Les dirigeants d'entreprise ne considèrent la production que comme moyen apte à réaliser des buts financiers. La vue financière de la production en ignore les subtilités, le montage, la fine ingénierie, et la considère comme la juxtaposition de parties sommables. Elle est ainsi à l'opposé d'une vision qui considère l'établissement de production comme un organisme. De ce point de vue, la pensée qui sous-tend le management actuel ressemble, selon *Profit beyond measure*, « à l'étude de cadavres », alors qu'il faudrait s'intéresser au système vivant. Comme en médecine : « ne jamais traiter des résultats d'examen, traiter les patients eux-mêmes ».

Le management basé sur les moyens (MBM), considère au contraire les établissements de production comme des organismes vivants. Il consiste à soigner ces organismes, en particulier en améliorant de façon continue les relations entre les parties, de façon à répondre toujours mieux à la demande des clients. L'exemple type du MBM est le système Toyota analysé dans le chapitre précédent.

Comparaison du MBR et du MBM

D'un point de vue philosophique, le MBR considère que les moyens sont distincts des fins, qu'ils sont comme des passages éphémères et contingents permettant d'atteindre des buts plus importants et plus permanents. Au contraire, le MBM (management basé sur les moyens) considère que les moyens ne sont pas subordonnés à des fins plus ou moins lointaines, mais sont eux aussi des fins à part entière, des fins évoluant vers un autre état final.

Pour le MBR, les systèmes de production n'étant que des moyens pour assurer des buts financiers, ils peuvent être reconfigurés à volonté, comme dans un mécano à éléments distincts et combinables. Pour le MBM, les moyens que représentent les systèmes de production sont des entités organiques. Les lois qui les gouvernent sont plus proches des lois de la physiologie que de celles de la mécanique. Les relations entre les parties sont essentielles et tout n'est pas interchangeable, comme dans un organisme où l'on ne peut pas remplacer un pied par une main sans conséquences majeures. Chaque partie doit s'intégrer de façon *organique* à l'ensemble.

Dans une vision mécanique du système de production, les pièces diverses qui le constituent doivent être commandées par un système 'plus évolué' que des éléments inertes, un système à base de feedbacks, d'informations et de contrôles. Le MBR suscite donc une 'usine à données' afin de guider et contrôler les opérations. En revanche, dans une vision organique, les relations entre les organes constituent une grande part du contrôle, de la stabilité et de la pérennité du système. Ainsi, pour le MBM, le travail de chacun, dans les unités de production, devrait être lié à l'ensemble et à la justification de fond de l'entreprise : la rencontre entre besoins du client et compétences de l'entreprise. Les activités de production sont largement gérées 'par elles-mêmes' ; une grande partie de 'l'usine à données' du MBR est donc inutile. Il demeure une comptabilité traditionnelle, mais le poste de contrôleur financier est voué à disparaître. Le MBM ne repose donc pas fondamentalement sur des données financières.

En termes de gestion du risque, la conception d'un système technologique complexe 'de base' auquel on ajoute ensuite une série de dispositifs de sûreté de nature technologique qui impose une gestion 'après coup' de la maintenance et des opérateurs est une conception de type mécanique et additive. Le modèle MBM propose un style qui, bien que fondé sur une amélioration de la productivité et de la durabilité, pourrait inspirer la gestion des risques. Les exemples phares que sont Toyota et Scania pourraient constituer une référence solide et reconnue dans le domaine industriel. À l'opposé, le style de gestion abstraite, financière et lointaine dont l'apogée industrielle se situe dans les années 1990 pourrait se révéler dangereux pour les systèmes de gestion des risques.

Pour le MBR, le profit est le but et le sens même de l'entreprise ; il doit être poursuivi à tout prix. Pour le MBM, le profit est certes indispensable à la survie de l'entreprise, comme la respiration à l'être vivant, mais il ne constitue pas sa *raison d'être*.

Pour le MBR, la mesure est l'outil indispensable pour comprendre quelle mécanique mettre en place et comment maximiser les profits et la valeur actionnariale. Pour le MBM, la mesure ne peut *expliquer* l'entreprise, car celle-ci est le lieu géométrique des relations qui lient les membres du personnel, les clients, les populations et l'environnement. La mesure peut parfois contribuer à développer ces relations mais non les expliquer ou les fonder. En ce sens, le MBM vise un 'profit sans mesure'.

En résumé, le MBR considère que la production n'est rien d'autre qu'un moyen d'arriver à des résultats financiers. La production est en fait un mécano, aucun élément ni aucune fonction n'y mérite d'importance particulière, les pièces y sont interchangeables, les relations entre ces pièces 'n'existent pas'. Surimposé à cette production mécanique de masse, un système de contrôle veille à minimiser les coûts sur la base d'une analyse financière détaillée des actes élémentaires de production. Le système global est peu souple et peu réactif. Le profit et sa mesure constituent le sens et l'explication de l'ensemble. Le contrôle est noble, proche du but financier, la production est corvéable.

Au contraire, le MBM considère que la production a une existence propre, respectable, indépendante des résultats financiers. Le système de production est un organisme où chaque élément joue son rôle spécifique et où les relations entre éléments constituent fondamentalement le système. Par un MBM, cet organisme est constamment amélioré, les relations sont repensées, adaptées, soignées, entretenues. Il devient alors souple et réactif. Il est alors naturellement efficace et génère un profit sain, durable et stabilisé. La production est une valeur dont le résultat financier est le signe ou le sous-produit.

Les conséquences de ces différences sont considérables. Au niveau de la pensée, le MBR se limite aux additions (et aux soustractions !) et « travaille sur des cadavres ». Le MBM traite de systèmes vivants et suit l'adage de la médecine : « ne jamais traiter des résultats d'examens, traiter les patients eux-mêmes ». Sa manière de gérer n'est pas d'imposer des plans et des méthodes de contrôle qui s'efforcent de donner forme aux résultats ; elle est de découvrir et de soigner les relations souhaitables pour que les résultats en découlent. Comme un bon jardinier sait qu'il lui suffit de soigner sa terre, la nature s'occupant du reste.

Les dangers du MBR

1. Ce sont d'abord les dangers d'un gestion 'de loin' qui ne connaît pas bien les problèmes.

Les hôpitaux

Lors d'une émission à France Inter sur les problèmes dans les hôpitaux français, de nombreux intervenants ont souligné des conditions de travail déplorables (manque de lits disponibles) et des pénuries de personnel (manques criants d'infirmières). Ces difficultés concernent plus particulièrement les grandes structures hospitalières des grandes villes.

Les médecins privés ont déclaré que ces difficultés proviennent du style de management « par des gens qui ne connaissent pas le terrain », des personnes diplômées de grandes écoles « qui ne se déplacent jamais sur le terrain et ne connaissent pas les problèmes ». Ils « gèrent des chiffres ; les 60 000 lits 'en trop' en région parisienne que l'on traîne

depuis des années sans que l'origine ou la démonstration de ce chiffre ait jamais été précisée ».

À travers d'autres témoignages et à travers le ton des interventions, il apparaissait que la gestion administrative des hôpitaux démoralise nombre d'employés, non seulement les infirmières dont les conditions de travail et de carrière ne sont pas enviables, mais encore les médecins, particulièrement les 'urgentistes', qui passent beaucoup de temps à régler des problèmes administratifs dans une atmosphère de souffrance des patients.

Si ce tableau est exact, il donne un exemple vivant des piètres résultats de la gestion abstraite et financière...

Le juge

Un soir, nous pénétrâmes dans un squat, à travers les gravats et sans prévenir. Panique générale à bord, sauve qui peut ! L'un des squatters, dans sa fuite, laissa tomber un paquet de Marlboro dans lequel je découvris trente grammes de poudre blanche. Le corps du délit dans la poche, j'allai voir le procureur le soir même.

« Monsieur le procureur, lui dis-je, il se passe des choses absolument inadmissibles en plein Paris. L'héroïne circule librement, en toute impunité. Nous ne pouvons pas laisser faire. J'ai le sentiment que nous ne jouons pas notre rôle. D'ailleurs, regardez ... » Et de lui tendre le fameux paquet de cigarettes. Sa réponse fut aussi fulgurante que sidérante, mais tellement judiciaire : « Monsieur, avez-vous saisi cet objet régulièrement ? » Je restai un instant sans voix. Pourtant, j'aurai dû m'y attendre, car derrière ce formalisme tatillon se dissimulait un réflexe bien humain que pourrait fort bien résumer cette phrase lapidaire : « L'action est le commencement des soucis ... »

Et derrière ce réflexe se cachait un problème grave : à cette époque, dans notre magistrature debout, toute information vivante partait de la base et remontait la hiérarchie échelon par échelon, perdant à chaque fois un peu plus de sa substance pour aboutir totalement aseptisée au niveau ministériel. Il faut savoir que le parquet, par sa nature, son organisation mais surtout ses mauvaises habitudes, ne décidait plus rien pour les affaires importantes ou sensibles, celui qui prenait la décision au plus haut niveau étant, par définition, celui qui était le plus éloigné du terrain. Comment pouvait-il en être autrement puisqu'il était le dernier maillon d'une longue chaîne ? Dans un tel contexte, il est aisé de comprendre l'ambiguïté et la frilosité qui régissaient les rapports entre la magistrature et le pouvoir exécutif. La magistrature ne pouvait pas se permettre de rappeler à l'exécutif les exigences de la justice ou de la sécurité publique.

Alain Marsaud, *Avant de tout oublier*, pp. 51-52

Les gérants de portefeuilles

La performance du gérant est mesurée sur quelques mois. Avec une sanction nette et sans appel : ceux qui ne sont pas bons sont virés, ceux qui sont meilleurs les remplacent.

Quand la concurrence devient féroce entre tous ces gérants, l'enjeu impératif est d'être un tout petit peu plus performant que le voisin. Mais sur quel critères ? Comme il s'agit de payer des retraites, l'essentiel devrait être de maximiser le capital dans les 10 ou 20 ans – et non pas, bien évidemment, le gain sur 2 mois. Eh bien, malheureusement, assez souvent, les règles mises en place font qu'un gérant est obligé de maximiser son rendement sur une période très courte qui ne correspond en rien à son horizon naturel. Que l'on ajoute à cela une situation d'excès de capacités, et on va à la guerre des prix. Conséquence : pour battre le voisin, il n'y a plus qu'une solution – augmenter le niveau de risque de l'actif. Pire : comme tout le monde, ensuite, va augmenter la dose de risque dans les mêmes directions, les primes de risque vont complètement s'écraser ; l'augmentation du risque ne rapporte plus rien (on arrive même à l'absurde : ce sont les actifs les moins risqués qui ont les rendements anticipés les plus élevés).

On subit encore une autre exigence drastique : si votre concurrent commence à investir énormément sur un actif très risqué, et si dans un premier temps ceci est rémunérateur, vous ne pouvez pas ne pas

faire comme lui. Le plus troublant et le plus grave, c'est que ce mimétisme n'est pas un effet de bêtise : il est complètement assumé et on rencontre même aux Etats Unis, pendant la crise mexicaine, des gens qui disaient : « Je sais que cela va très mal se finir, mais si je ne mets pas mon argent au Mexique comme tout le monde, j'aurais des performances épouvantables et je me ferai virer, sans avoir eu le temps d'avoir raison. »

Ce n'est pas tout : prise de risque excessive et mimétisme voient encore leurs conséquences renforcées par le développement de techniques de gestion (« benchmarking ») qui privilégient non pas une norme de performance dans l'absolu, mais une norme de performance relative à un certain portefeuille. En clair, ce n'est pas très grave si je fais -19 : dès lors que le voisin fait -20, je suis gagnant. On pourrait juger que mon -19 fait de moi un mauvais gérant ; mais non, en termes relatifs, je suis gagnant. On est jugé en performance relative et plus du tout en performance absolue. Cela conduit à prendre énormément de risques : si cela tourne mal, mais un tout petit peu moins mal que chez les autres, il n'y a pas de problèmes. Le fait d'être passé à des critères de performance relative au lieu de garder un critère de performance absolue est ainsi une incitation énorme à la prise de risque.

Patrick Artus in Patrick Lagadec, *Ruptures Créatrices*, pp. 240-242

Mais la critique de gestion abstraite est sans doute trop générale, même si elle est parfois suggestive, car en effet, cette critique s'appliquera à de nombreux cas de gestion malheureuse.

2. Le danger d'une trop forte influence des considérations financières déconnectées des réalités de la production.

Scania face à la Bourse

Scania, une entreprise de poids lourds de qualité rentable régulièrement depuis plusieurs dizaines d'années, serait bien mal inspirée d'adopter les stratégies à la mode, pilotées par les résultats et consistant en réductions aveugles des coûts, en économies d'échelle, en incitations financières à la 'performance', etc. C'est pourtant ce que les analystes financiers et la presse économique ont pressé les dirigeants de faire depuis 1997.

Cette pression a suivi l'introduction des actions Scania sur les Bourses de Stockholm et de New York fin 1996. En 1995, l'année précédente, Scania avait enregistré un taux de rentabilité record de 15,9% (return on sales, rentabilité des opérations). Les journalistes et analystes financiers clamèrent que 'le marché exigeait' de l'entreprise un minimum de 15% de rentabilité, alors qu'il n'était que de 7,6% en 1997. Ils suggéraient qu'il était temps que Scania change sa façon de travailler.

Ces journalistes reflétaient la fascination des milieux financiers pour le MBR américain, pourtant complètement à l'opposé du sérieux avec lequel Scania soigne les moyens depuis plusieurs générations. Or, en 1995 et 1996 Scania ne vendait qu'une gamme de camions qu'elle produisait depuis les années 1980, alors qu'en 1997, elle ne vendait plus que sa nouvelle gamme introduite fin 1996. Insensibles à cet aspect opérationnel, les journalistes financiers suédois suggéraient que Scania soit vendue à une autre compagnie dont les managers 'sauraient ce qu'il faut faire' pour ramener rapidement les résultats aux niveaux de 1995. Un de ces articles, ô ironie,

comparait les constructeurs européens. Scania était en tête avec des profits positifs, Volvo en seconde place avec des comptes équilibrés, et Mercedes en troisième position avec des revenus négatifs. Les nouveaux dirigeants devaient-ils provenir de ces compagnies moins performantes ? Non. On pensait probablement aux managers américains tels le sinistre Al Dunlap alias 'la tronçonneuse' tant il a tranché dans les entreprises qu'il a dirigé pour leur plus grande perte. Dans ce cas, la poursuite de la série de profits positifs que Scania dégage sans faillir depuis 1934 ne serait pourtant plus prioritaire...

La rentabilité à long terme ne semble guère être la préoccupation majeure des actionnaires qui pressent aujourd'hui les compagnies comme Scania d'abandonner leur management des moyens en faveur d'objectifs à court terme 'imposés par les marchés financiers'.

Les milieux d'affaires européens parlent souvent de 'virus américain' quand ils se réfèrent au MBR. C'est fort approprié parce que ces pratiques, entièrement tournées vers les intérêts des seuls actionnaires, sont capables de vider de sa substance n'importe quelle entreprise. En effet, 'le virus américain' se développe en tuant son hôte par licenciements, désengagements, externalisation et autres mesures drastiques destinées à réduire les coûts. Puis, on vendra à n'importe quel acheteur anonyme qui, lui aussi, ne pensera qu'à réduire les coûts.

(D'après Profit Beyond Measure, pp. 136-138)

3. Le danger d'une 'virtualisation' de la production. C'est ainsi qu'Enron a fait faillite, mais aussi que nombre de dirigeants américains ont conçu leur métier comme consistant en grande partie à produire des résultats financiers, même s'ils étaient le fruit de la créativité comptable et nullement de la production de produits ou de services (voir chapitre 14). C'est aussi en grande partie sur des espoirs financiers virtuels qu'a été créée la bulle boursière des sociétés de l'Internet et de l'économie virtuelle.

4. Plus grave est l'influence d'une culture du résultat mal comprise sur la moralité des affaires. C'est ainsi que les investigations qui ont suivi la faillite d'Enron ont démontré que le secteur américain du trading de l'énergie se livrait à des pratiques malhonnêtes multiples au dépens, par exemple, des consommateurs d'énergie de Californie.

5. Ce qui est sans doute plus triste encore, c'est la destruction de 'valeur intrinsèque' au profit de la valeur financière.

L'industrie du parfum

Des champs de Grasse où l'on cultivait le jasmin ou la rose pour en extraire les essences qui entraient dans l'alchimie des parfums, il ne reste que quelques échantillons. Les promoteurs immobiliers ont eu raisons des terres.

Longtemps aussi, Grasse a été LE pôle de la parfumerie. Mais fusions acquisitions aidant, la plupart des grandes maisons ont disparu. Celles qui ont survécu ont du affronter la concurrence mondiale et s'y adapter. Parce que le parfum est devenu une industrie mondiale où se jouent des batailles de géants. Chacun rêve de créer LE parfum qui séduirait la planète. Sa fragrance importe un peu, ce sera surtout la réussite du lancement qui fera la différence. Et aujourd'hui, le ticket d'entrée avoisine le demi milliard de francs.

Longtemps, le temple de la parfumerie fut en France. Mais aujourd'hui, de même que l'artisanat de la haute couture est marginalisé par le prêt à porter ou que les savonniers de Marseille ont été déclassés par le lancement des détergents, la parfumerie française est en passe de se voir confinée dans l'élitisme. Saura-t-elle déjouer la stratégie de confinement orchestrée par la concurrence américaine ?

« L'univers impitoyable du parfum! » ...

L'émission expliquait qu'un parfum, c'est l'addition de trois tiers :

- une campagne de publicité internationale ;
- une présentation (le 'flacon') ;
- le parfum lui-même (le 'jus')

Cette équation découle de la logique financière. Celle-ci est, elle aussi, basée sur trois éléments :

- la concurrence par les prix (par les coûts) ;
- la puissance des économies d'échelle ;
- les exigences de rémunération du capital.

D'où la nécessité pour réaliser un 'grand parfum' mondial, de convaincre les consommatrices des deux côtés de l'Atlantique et, si possible, également en Asie. Les fabricants de 'jus' (trois grandes entreprises mondiales), devenus sous-traitants des parfumeurs, ont donc très peu de marge de manœuvre. Conclusion : la parfumerie mondiale ne favorise pas la créativité. La parfumerie perd son sens. « Le parfum sent l'argent ».

Rue des Entrepreneurs, 22 décembre 2001 et 27 juillet 2002 sur France Inter.

6. L'exemple emblématique en matière de risques reste l'accident gravissime de Bhopal. La récente publication d'un livre par un spécialiste de l'Inde apporte de nouveaux éclairages sur cette affaire déjà ancienne (*Il était minuit cinq à Bhopal*, Dominique Lapierre & Javier Moro, Laffont 2001, réédité en collection de poche).

L'ampleur de la catastrophe est soigneusement analysée. Le nombre de victimes la nuit du drame a été estimé sur la base des enterrements pour les musulmans, des lindeuls et des incinérations pour les hindous. En effet, l'élimination des cadavres a posé d'énormes problèmes aux professionnels en raison de la surcharge tout à fait exceptionnelle à laquelle ils ont été confrontés. L'estimation aboutit à la fourchette 14 000 – 30 000 morts contre 2 500 victimes officielles.

Les causes de ce désastre sont évidemment multiples. La plus flagrante reste néanmoins la gestion financière de l'établissement. Dans un premier temps, les résultats financiers décevants d'un projet naïvement optimiste ont poussé les américains d'Union Carbide à se défaire de leur usine indienne. La transmission à une structure de gestion indienne a été conduite avec une conscience faible — en tous cas insuffisante — du niveau de la culture du risque en Inde. En effet, la gestion de l'usine fut confiée à une entité indienne dépourvue de toute culture des établissements de haute technologie.

Dans un second temps, la structure de gestion indienne s'évertua essentiellement à réduire les coûts de fonctionnement. Comme directeur de l'usine, on nomma un distingué financier bengali devant lequel le jeune ingénieur de sécurité pesait fort peu. Les américains faisaient pourtant toute confiance à ce dernier, car il était brillant et avait donné toute satisfaction aux USA. C'était sans compter sur le poids de la culture locale.

On se reportera au livre pour le détail technique des manquements de sécurité dans l'installation.

On remarque donc, ici encore, le danger des structures de gestion indirectes qui rendent presque impossible la conscience réelle du risque au niveau des dirigeants. En d'autres termes, avec des hommes normaux, faillibles et non omniscients, la structure organisationnelle joue un rôle important dans la gestion des risques.

La faible rentabilité d'un établissement à risques est un facteur de risque.

En particulier, les établissements en fin de vie présentent le risque de voir les crédits de sécurité réduits au delà de ce qui serait souhaitable.

Synthèse

En guise de synthèse des points abordés dans les trois derniers chapitres, voici un extrait de François Dupuy, *L'Alchimie du Changement*, Dunod, 2001 (pp.142-145). Ce texte (dont nous avons pris connaissance après la rédaction de ces chapitres) replace la différence entre MBM et MBR dans le cadre plus général du changement dans les organisations.

[Une approche du risque inspirée par le management basé sur les moyens est, on l'aura compris,] « loin d'être universellement acceptée [...] Elle privilégie la participation, le facteur humain, la recherche de l'adhésion du plus grand nombre. Mais en prenant un peu de recul on peut voir que les nécessités du monde moderne, notamment la brutale accélération des cycles économiques, qui se traduit par l'apparition et disparition rapide de nombreuses entreprises et par l'importance croissante accordée à la satisfaction de l'actionnaire, conduisent à opposer deux théories et donc deux pratiques du changement.

La première est à l'opposé de ce qui vient d'être proposé. Les spécialistes l'appellent la théorie E, parce qu'elle donne la priorité absolue dans l'action à la valeur économique. Ils s'accordent à reconnaître qu'elle est *hard*, puisqu'elle considère que la seule mesure légitime du succès de l'entreprise est la valeur créée pour l'actionnaire. Elle implique, dans un processus de changement, l'utilisation massive des incitations financières, le recours drastique et sans états d'âme aux licenciements, au *downsizing*, aux restructurations qui ont marqué la fin de ce siècle. Elle est bien sûr caractéristique du monde nord-américain et renvoie de façon insistante à des pratiques qu'un certain nombre d'auteurs n'hésitent pas à considérer comme le facteur clé de succès des Etats-Unis par rapport au reste du monde développé.

La théorie O, appelée ainsi parce qu'elle privilégie la capacité organisationnelle, est beaucoup plus répandue en Asie et en Europe. Cela ne surprendra personne de constater qu'elle est proche de ce qui a été fait dans l'exemple d'Air France. Le but généralement poursuivi est de développer ce qu'il est convenu de nommer une « culture d'entreprise », en investissant sur les capacités humaines au travers d'un processus d'apprentissage individuel et organisationnel. Dans la plupart des cas, les entreprises l'adoptent lorsque existait, préalablement à l'apparition de la nécessité de changer, un contrat implicite de loyauté-protection entre elles et leurs salariés – c'était bien le cas d'Air France – et quand la rupture de ce contrat de façon abrupte comporterait des risques sérieux d'explosion définitive de l'organisation. De façon sous-jacente, on voit que ce qui est privilégié dans cette approche, c'est le maintien de liens forts dans la durée entre l'entreprises et ceux qui y travaillent. On peut même penser que plus ces liens ont été tissés sur une longue période, par petites touches successives, par l'obtention de toujours plus d'avantages, plus de recours à la stratégie soft s'impose, sauf à jouer le pourrissement de la situation.

Et, en effet, ces deux approches diffèrent encore plus qu'il n'y paraît au premier abord sur six points clés :

- Les buts, tout d'abord, qui, comme nous l'avons noté, sont dans un cas de maximiser le retour sur investissement à court terme de l'actionnaire, et, dans l'autre, le développement des capacités organisationnelles. On retrouve ici une distinction classique sur laquelle nous avons déjà insisté et qui, si à côté de l'actionnaire on met le client, permet d'opposer la logique de la mission (théorie E) à la logique d'organisation (théorie O). On comprend pourquoi plus les univers sont de nature bureaucratique – priorité donnée à leurs propres contraintes – c'est-à-dire plus les protections dont disposent leurs membres sont importantes et plus ceux-ci poussent vers la seconde.
- La conduite du changement ensuite qui, dans la théorie E, se fera par l'injonction venue du sommet, à laquelle les membres de l'organisation obéiront sans s'interroger sur le bien fondé ni sur ses conséquences. Cela s'observe tous les jours dans le monde nord-américain sans provoquer plus de réaction que cela. A l'inverse, comme on l'a vu plus haut, la théorie O encouragera la participation de tous, selon des modalités que nous nous sommes efforcé de préciser.
- De façon plus profonde, dans la théorie E, priorité sera donné à ce que l'on appelle les « systèmes », au sens anglo-saxon des structures, des règles et des procédures, à partir de la croyance, solidement ancrée sur des modes de contrôle stricts, que les acteurs font bien ce que ces systèmes leur enjoignent de faire. Curieusement, cela renvoie au rêve initial d'une bureaucratie – cette fois au sens classique du terme – telle que l'avait pensée Max Weber et qui serait une organisation à la fois capable de produire des règles générales et impersonnelles et de les faire appliquer : ce n'est possible qu'avec l'appui d'un sévère système de sanctions. L'approche O, vue sous

cet angle-là, est plus pragmatique : ce qu'on se propose de changer en priorité, ce sont les comportements des acteurs plus que leurs attitudes, en leur créant de nouveaux contextes. Ici, les systèmes sont utilisés comme des leviers, dans une perspective qui est, elle, systémique, mais au sens sociologique du terme. On parie sur les capacités de jeu de ces acteurs, plus que sur leur diligence à suivre à la lettre ce qui est prévu par les textes.

- Du même coup, le process sera différent. [...] Il consistera, dans la théorie E, à établir des plans et des programmes aussi précis, exhaustifs et contraignants que possible, mais, cette fois-ci, en s'assurant de leur mise en œuvre effective et rapide. La vision O privilégiera l'expérimentation, l'évaluation, les allers et retours entre les buts à atteindre et les résultats observés, puis la généralisation, quitte à veiller en permanence à effectuer les adaptations nécessaires.
- Les leviers employés ne seront ni les mêmes, ni surtout utilisés de la même façon. La stratégie E se concentrera sur les incitations monétaires, en les liants directement aux résultats financiers à court terme, tels que les cours de bourse permettront de les évaluer de façon permanente et considérée comme incontestable. On est quasiment de retour à une vision taylorienne de la motivation des individus au travail. Dans la stratégie O, les récompenses financières sont davantage utilisées pour accompagner le changement que pour le produire. Mais surtout, c'est l'ensemble des outils d'une politique de gestion des ressources humaines – évaluations, promotions, affectations, rémunérations – qui seront utilisés comme leviers de changements. Bien entendu, plus l'organisation aura tendu à les rigidifier dans une phase antérieure et plus leur mise en œuvre sera délicate et demandera à être négociée avec les intéressés.
- Enfin, dans le deux cas, l'appel à des consultants extérieurs prend des tours différents. Dans le premier cas (théorie E), ce sont ceux qui analysent les problèmes – en fait, se concentrent la plupart du temps sur les symptômes – qui dessinent les solutions et prennent en charge la mise en œuvre de leurs propres recommandations. Tous les grands cabinets ont d'ailleurs élaboré sur ce point des méthodologies facilement duplicables. Dans le second cas (théorie O), les consultants sont un support, apparaissent comme des facilitateurs qui aident non seulement le management – comme semblent le souhaiter Beer et Nohria – mais, comme nous avons essayé de le montrer, l'ensemble des personnels à trouver leurs propres solutions, qui feront ensuite l'objet d'une validation formelle par les responsables. Mais la – légère – distinction que nous venons d'introduire quant à ceux qui ont besoin d'être réellement soutenus et aidés boucle la boucle : elle indique que la confiance, celle que l'on accorde à tous ceux qui sont impliqués dans un processus de changement, est encore loin d'être universellement admise. »

17. MONDIALISATION ET RISQUE DE MORALITÉ

Le risque de moralité (ou « aléa moral ») survient quand un individu, au motif qu'il est assuré, relâche ses efforts de prudence. « Pourquoi m'inquiéter, l'assurance paiera ! » Ainsi, par exemple, telle entreprise pollue un cours d'eau sans prendre toutes les précautions nécessaires car son assurance de responsabilité civile paiera. Prévenir la pollution lui reviendrait plus cher que de faire jouer son assurance, même si cela reviendrait moins cher que le montant des dommages. Ainsi, le fait d'être assuré modifie la 'moralité' de l'agent.

D'une certaine façon, toute forme de mutualisation, et même de communauté, court ce risque. La mutualisation offre une sécurité commune à l'ensemble de la mutualité dont tel individu peut être tenté de profiter. Tout comme un passager clandestin, ce qui pose de nombreux problèmes (assurance santé, indemnisation des catastrophes naturelles, ...). C'est pourquoi les nombreuses formes de mutualité se dotent d'une 'police' explicite ou implicite.

Un établissement de production isolé, constituant à lui seul une entreprise à établissement unique, est tout naturellement profondément concerné par sa survie. Seul l'aveuglement peut le conduire à adopter des conduites mettant en jeu son avenir même. La situation est similaire dans une entreprise qui comprend deux ou trois établissements. Mais si, à la suite des nombreux regroupements que l'actualité ne cesse de mettre en scène, l'établissement considéré fait maintenant partie d'un groupe complexe exerçant de nombreuses activités diverses et possédant des établissements de production divers et dispersés, alors la même prudence n'est plus aussi naturellement imposée par la tête de groupe. Car, la disparition d'un établissement n'affectera que marginalement les résultats globaux de l'entreprise et le cours de l'action. L'exemple typique de cette situation est celle de notre groupe national phare TotalFinaElf : en dix ans, il a connu trois gros sinistres, l'explosion de la raffinerie de La Mède, la marée noire de l'Erika et l'explosion d'AZF à Toulouse. Malgré ce triste record, l'action accumule les succès, l'entreprise se porte à ravir. Il ne s'agit pas de suggérer que cette diversification du risque est le moteur principal des regroupements, mais tout se passe comme si chaque établissement n'était qu'une ligne d'un portefeuille boursier savamment diversifié.

Les assureurs sont bien conscients du risque de moralité et ont établi des procédures pour le contrer. Il s'agit essentiellement de faire porter à l'assuré (ou au réassuré) une partie dissuasive des coûts qu'il pourrait provoquer par son manque de prudence. Les contrats de réassurance de portefeuilles d'assurance comportent trois mécanismes protecteurs : ils ne jouent qu'à partir d'un certain montant, ce qui correspond à une franchise d'assurance, ils s'arrêtent à un certain niveau de remboursement maximal et, enfin, ils peuvent ne rembourser qu'une partie des dommages entre les deux limites qui viennent d'être évoquées. Quant aux assurances, elles peuvent faire jouer ces trois mécanismes, le plus fréquent demeurant, de loin, la franchise même si l'indemnisation d'une proportion des dommages existe aussi (le « ticket modérateur » de l'assurance santé, par exemple). Une autre pratique consiste à n'assurer qu'une partie, spécifiée par contrat, des pertes encourues. Par exemple, un contrat d'assurance incendie ne couvre pas les pertes d'exploitation consécutives à un éventuel sinistre. Ou bien, un système de bonus/malus répartira la perte encourue sur les primes d'assurance futures. En

tous cas, quelle que soit la méthode, il faut faire porter à l'assuré une partie suffisante des dommages pour que, même si sa survie n'est plus en jeu, il reste néanmoins d'une grande prudence²⁵.

Ces mécanismes peuvent-ils jouer pour inciter les grandes entreprises multinationales à soigner la sûreté de tous leurs établissements ? Il ne le semble pas. D'une part, elles sont assurées ; d'autre part, les dommages restant à leur charge seront mutualisés entre de nombreux établissements et n'ont donc que peu de chances d'avoir un effet dissuasif.

En réalité, il en est de même de la franchise : elle est beaucoup plus dissuasive pour un assuré ordinaire que pour un assuré très fortuné puisqu'elle représente une perte réelle et cuisante pour le premier, mais seulement un épisode insignifiant pour le second. Ce qui peut retenir ce dernier c'est bien plus le risque de sanctions pénales que le poids de pertes économiques. Certes, même une puissante multinationale peut être affectée si la sécurité de ses établissements est trop mauvaise, soit que de nombreux sinistres finissent par entamer la marge de profit, soit qu'un énorme sinistre cause sa disparition comme dans le cas de Bhopal (2 500 morts officiels, entre 14 000 et 30 000 d'après une récente étude). Encore faut-il, pour que cette possibilité ait un rôle incitatif, qu'elle soit bien perçue comme telle. Personne à Union Carbide n'imaginait un désastre comme Bhopal. Le risque de sanctions pénales effectives serait-il à même de délier l'imagination des dirigeants en ce qui concerne les risques ?²⁶

D'une façon générale, la responsabilité civile ne répercute donc pas correctement les risques : (1) en raison de l'assurance, (2) parce que la probabilité d'être condamné au civil est rarement égale à 1 et (3) parce que le montant des indemnités ne peut qu'être inférieur au dommage causé (absence de « dommages punitifs » à la mode américaine). Il semblerait donc judicieux, au niveau du droit des entreprises, de donner également un rôle significatif aux sanctions pénales pour que le risque soit réel pour les responsables concernés.

²⁵ On prétend souvent que le régime actuel d'indemnisation des catastrophes naturelles n'incite pas suffisamment à la prévention, oubliant ainsi qu'il ne rembourse ni la vétusté ni les frais financiers de remise en état ni la pénibilité de cette remise en état (élaboration des contrats, surveillance des travaux, temps perdu hélas trop familier pour quiconque a fait construire) ni l'inconfort de la période de remise en état ni les jours de travail perdus ni la souffrance (pertes d'objets suscitant un attachement sentimental, souffrances physiques pendant le désastre, par exemple dans le Sud, et, bien entendu, la perte de proches).

²⁶ Rappelons que le PDG américain de Union Carbide au moment de Bhopal est en fuite, disparu au regard de la justice indienne (on dit que les services américains lui auraient fourni une nouvelle identité).

IV - GÉRER LES RISQUES, CULTIVER LA SÛRETÉ

Nous ouvrons cette partie en présentant une typologie des situations de décision des divers acteurs en matière de risque (chapitre 18). La gestion des risques implique tout un réseau d'acteurs de niveaux hiérarchiques différents et plus ou moins proches du danger. Des contraintes et des limites différentes s'imposent à chacun. Ces contraintes ne favorisent pas une prise de décision idéale, notamment aux niveaux supérieurs de la hiérarchie et à proximité immédiate du risque. Cette situation pourrait être améliorée par une relation plus étroite de ces acteurs avec les spécialistes de l'analyse du risque. Plus généralement, le *risk management* requiert la définition des rôles, des responsabilités et des interactions entre acteurs.

On perçoit les enjeux d'une meilleure intelligence du risque : il est indispensable de 'créer du lien' entre les divers acteurs, on ne peut pas se contenter de développer des panoplies d'instruments à l'usage des analystes et que les autres acteurs ne comprendront guère et n'utiliseront pas.

Pour 'gérer les risques, cultiver la sûreté', qu'apporte le domaine, connu et reconnu, de la qualité à ceux dont la mission est d'assurer la sûreté ? Le chapitre 19 compare sûreté et qualité à partir de leurs meilleurs représentants. En termes de sûreté, les bons élèves²⁷ possèdent cinq caractéristiques : (1) l'autorité est déléguée de façon souple ; (2) il existe une organisation spécifique en cas de crise ; (3) les apports des opérateurs sont reconnus ; (4) la transparence est favorisée, on recherche ouvertement les erreurs ; (5) le changement organisationnel est jugé à l'aune de la sûreté. Dans le domaine du management de la qualité, on retrouve des principes semblables aux quatre premiers traits. En revanche, la priorité qu'exprime 'le changement organisationnel est jugé à l'aune de la sûreté' ne se retrouve pas nécessairement dans le domaine de la qualité.

Cette priorité donnée à la sûreté, caractéristique des entreprises à hauts risques et pourvues d'une bonne culture de sûreté, n'est évidemment pas une priorité absolue, même si elle est parfois affichée comme telle. La sûreté absolue, ce serait de ne rien entreprendre de dangereux ! Son statut est probablement complexe, une part relevant de gestion multicritère, une autre de communication.

D'un point de vue économique, « la sûreté n'a pas de prix, mais elle a un coût ! » Quand on observe les comportements d'industries à risques telles que le nucléaire ou l'aviation, le budget alloué à la sûreté n'est pas infini. Ainsi, le discours sur la priorité de la sûreté est perçu avec scepticisme par l'économiste. Un niveau de sécurité *acceptable* est, certes, une condition *nécessaire* de fonctionnement des usines à risques et nous envisageons donc, dans ce sens et en termes de théorie économique, cette 'priorité' de la sûreté (chapitre 20). Plusieurs notions de coût de la sûreté se dégagent. Leur perception par les décideurs est cruciale. Nous comparons avec le domaine voisin de la qualité : si le coût de la non qualité est répercuté

²⁷ Ce sont, par exemple, les HRO, *High Reliability Organizations*, étudiées aux États Unis, à l'université de Berkeley

assez directement par le marché, il n'en est pas de même du coût de la non sûreté. Non seulement le coût de la sûreté n'est que difficilement relié à des avantages économiques, mais en outre, la pression du marché va plutôt à l'encontre des objectifs de sûreté.

Ce type d'analyse suggère que la sûreté devrait être conçue dans un esprit d'amélioration tenace, persévérante et jamais achevée des méthodes de production avec la conscience qu'elle a de nombreux effets positifs sur ladite production et sa qualité. D'ailleurs, les ingénieurs qualité qui améliorent les 'process' pour garantir une excellente fiabilité des produits, contribuent ainsi à améliorer la sûreté.

Comment œuvrer dans ce sens au niveau des autorités ?

L'intelligence du risque dans le domaine de l'aviation civile (chapitre 9) permet de mesurer combien la gestion indirecte des risques par l'autorité de régulation est susceptible de faire progresser la culture de sûreté. Peut-on étendre ce type de régulation au domaine des établissements à risques ? Certains soutiennent que l'obligation de tenir un système de gestion de la sûreté (SGS) existe déjà en France pour les entreprises présentant des risques significatifs. Nous montrons (chapitre 21) : (1) que le champ des entreprises à risques est loin d'être couvert ; (2) que les SGS existants ne sont pas nécessairement satisfaisants en raison de la difficulté à auditer ces systèmes et à prendre des mesures contraignantes le cas échéant.

Plus généralement, le style d'action de l'administration a bien progressé depuis le commandement régalien descendant de Paris. Il est aujourd'hui fondé sur une culture de dialogue entre l'administration et l'industrie et sur l'établissement de plans d'action nationaux concertés. Nous montrons sur un exemple (chapitre 22) qu'une étape supplémentaire pourrait être suivie, inspirée par le souci de développer la culture du risque et orientée vers la responsabilisation des acteurs.

De tels changements d'attitude, de stratégie, ne sont peut-être pas aussi difficiles à intégrer que le suggèrent certains observateurs, même si, à l'instar d'un exemple documenté dans le cas de l'administration suisse (chapitre 23), les résistances sont parfois profondes dans les administrations.

Nous terminons avec un point capital : les inspections sont-elles efficaces ? (chapitre 24). Les contre-exemples ne manquent pas ! Certes toutes les inspections ne sont pas totalement inefficaces. Si, néanmoins, les inspections ne fournissent qu'une garantie assez médiocre contre les désastres, ne vaut-il pas mieux s'appuyer sur des stratégies de responsabilisation et de développement de la culture du risque et de la sûreté ?

18. ANALYSE DES RISQUES ET PRISE DE DÉCISION

Ce chapitre présente une typologie des situations de décision des divers acteurs en matière de risque²⁸. Des contraintes et des limites s'imposent dans chaque cas. On constate que :

1. la gestion des risques implique un réseau d'acteurs divers, en particulier selon leur niveau hiérarchique et leur proximité au risque ;
2. la décision est fortement contrainte, notamment aux niveaux supérieurs de la hiérarchie ainsi qu'à proximité du risque, de diverses façons qui ne favorisent pas une analyse de risque conforme aux prescriptions de la théorie ;
3. les risques pourraient être mieux gérés par ces acteurs en relation étroite avec les spécialistes de l'analyse du risque ;
4. le *risk management* requiert la définition des rôles, des responsabilités et des interactions entre acteurs.

On perçoit les enjeux d'une meilleure intelligence du risque : il est indispensable de 'créer du lien' entre les divers acteurs, on ne peut pas se contenter de développer des panoplies d'instruments à l'usage des analystes et que les autres acteurs ne comprendront guère et n'utiliseront pas.

²⁸ Ce chapitre est basé sur "On the Use of Risk Analysis in Different Decision Settings", Aven T., Korte J. and Rosness R., communication présentée au Colloque européen de sûreté de fonctionnement, Lyon, 2002. Cet article est issu d'une analyse de l'industrie pétrolière norvégienne.

1. Les acteurs du risque et leurs approches de la décision

Les décisions concernant les risques sont prises à des niveaux organisationnels divers et dans des conditions variées. Le graphique ci-dessous positionne les acteurs selon leur proximité au risque (en abscisses), à savoir la proximité dans l'espace et le temps, et leur niveau hiérarchique (en ordonnées), dans le cas particulier de l'industrie pétrolière norvégienne :

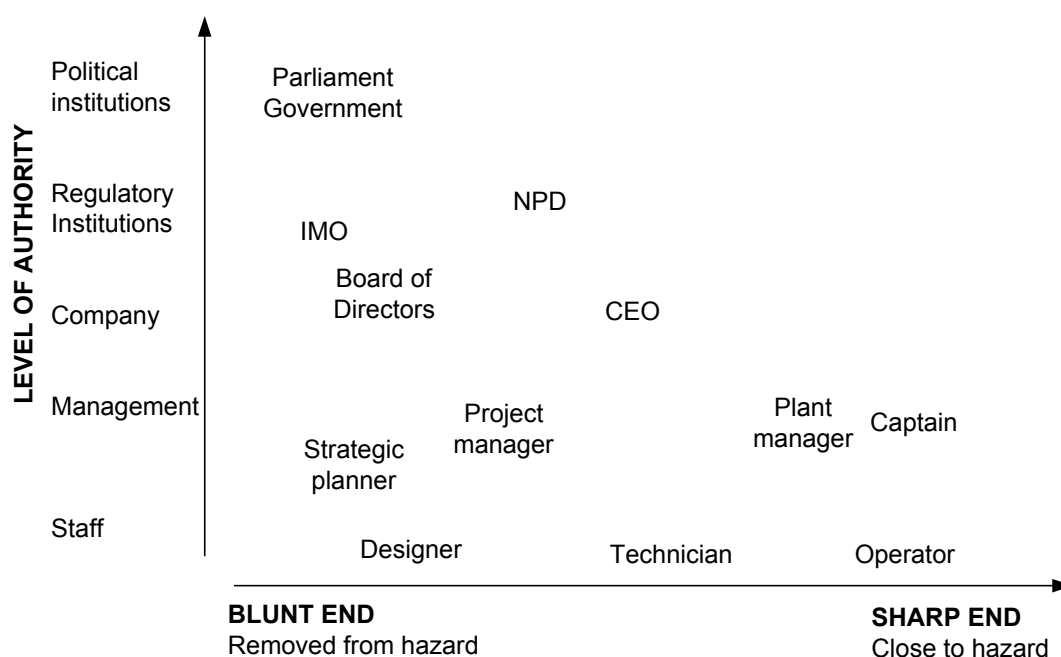


Figure 1 Position de différents acteurs liés au risque dans le cas de l'industrie pétrolière norvégienne (IMO – The International Maritime Organisation; NPD – The Norwegian Petroleum Directorate; CEO – Chief Executive Officer)

Les acteurs proches du risque doivent souvent réagir aux événements dans un laps de temps réduit qui ne permet qu'une analyse limitée. En revanche, ils sont, en général, plus au fait des derniers développements concernant le système qu'ils gèrent et en ont une connaissance plus détaillée, plus pratique et plus « réelle ». En général, les décideurs de haut niveau hiérarchique ne se livrent pas (et ne peuvent pas se livrer) à une analyse méticuleuse du risque. C'est ce que montrent des études empiriques. D'où, des oppositions observées entre préceptes théoriques de *risk management* et décisions pratiques du monde réel.

Les deux dimensions explicatives (proximité du risque et niveau hiérarchique) contribuent à expliquer les styles de prise de décision des différents acteurs. La typologie des modes de décisions proposée par les auteurs apparaît sur la figure 2 :

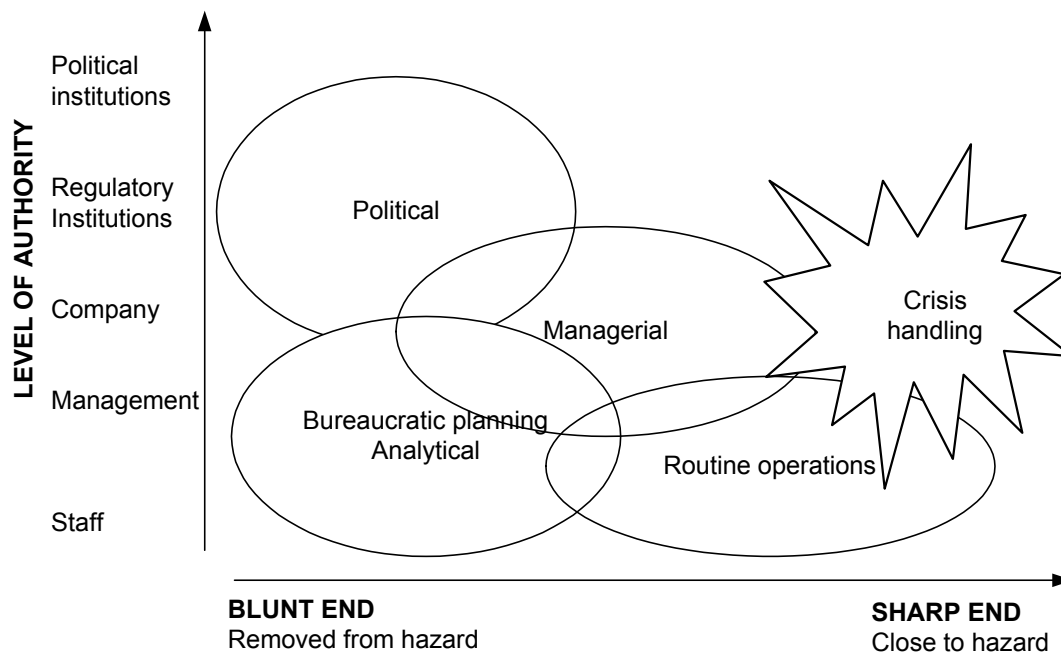


Figure 2 Modes de décision des acteurs

Les cinq modes de décision sont détaillés ci-dessous :

Opérations de routine. À la suite de Rasmussen²⁹, Reason³⁰ distingue trois modes d'action à ce niveau : le savoir-faire, la règle et la connaissance. L'activité basée sur le savoir-faire traduit des informations ou des indications directes en action, dans un style assez automatique tourné vers le résultat immédiat ; elle n'est pas liée à la résolution d'un problème. L'activité basée sur la règle (règle intériorisée, procédure, check-list, recette, etc.) n'est efficace que quand la situation est adéquatement couverte par la règle ; sinon, elle risque d'être dangereuse. L'action basée sur la connaissance intervient quand il n'y a plus de savoir-faire ou de règle applicable ; elle est proche de la résolution de problème.

Management. Les grands dirigeants d'entreprise ont régulièrement une cinquantaine de problèmes non résolus à traiter. Des études montrent que, contraints par leur capacité de traitement de l'information, ils cherchent souvent à poser le problème en termes de critères multiples à satisfaire (*satisficing behaviour*³¹) avec un effort de réalisme qui rend justice à la complexité de la question, plutôt qu'en termes d'optimisation celle-ci impliquant de simplifier voire de caricaturer. Les critères considérés dans ce style de décision peuvent être extérieurs et généraux ou bien spécifiques à l'organisation. Les décisions de management se basent aussi parfois sur des règles et des codes de conduite éprouvés, sans toujours analyser les conséquences très à fond. Si les enjeux sont importants, l'analyse du problème est souvent

²⁹ Rasmussen est une des grandes figures de l'analyse des risques. Sa bibliographie est forte de nombreux articles (voir [8] et [20]). Il est, en particulier, le responsable de la première étude probabiliste de sûreté dans le nucléaire américain (1975) connue sous le nom d'étude Rasmussen.

³⁰ James Reason est un des grands penseurs du risque. Ses ouvrages principaux sont [6] et [9]

³¹ Ce néologisme maintenant classique est dû à Herbert Simon (voir <http://cepa.newschool.edu/het/profiles/simon.htm>)

déléguée à un service spécialisé chargé d'élaborer des recommandations, les décideurs conservant l'autorité et la responsabilité de la prise de décision.

Décision politique. Elle est marquée par les conflits d'intérêt et requiert d'engendrer un niveau suffisant de consensus. Plutôt que des solutions à des problèmes, les décisions sont le résultat de compromis issus d'un processus de marchandage. Le consensus est difficile voire impossible à réaliser quand des modifications majeures sont en cause. D'où les politiques de 'petits pas', les progressions 'à tâtons' dans lesquelles la politique se tresse graduellement de décisions mineures basées sur des analyses limitées. De tels processus sont en général inefficaces quand une décision stratégique de long terme est requise. Autrement dit, toutes les décisions ne peuvent pas être décomposées en une succession de décisions mineures. En outre, si les coalitions en présence se modifient elles peuvent aboutir à des décisions dont l'ensemble se révèle incohérent³².

Analyse. Loin du risque et des hautes sphères décisionnelles se trouvent des fonctions telles que le design, l'ingénierie, la planification, le contrôle et de nombreuses formes d'analyse. Les acteurs concernés constituent un groupe hétérogène et nombreux. Ils disposent en général de temps, de moyens de calculs et de données. Ils adoptent des approches analytiques et formelles. Ils tentent souvent d'optimiser un critère explicite, par exemple un rapport coûts/avantages.

Gestion de crise. Elle couvre des situations très diverses qui ont en commun d'être rapidement évolutives et lourdes de conséquences. La prise de décision est largement orientée vers la minimisation des conséquences fâcheuses. Les acteurs principaux sont des dirigeants ordinairement éloignés du risque et qui se trouvent soudain projetés dans la tourmente. Ils doivent donc aussi gérer leur stress et leur anxiété. S'ils sont livrés à eux-mêmes, la probabilité que leur décisions soient inappropriées est forte.

2. La place et le rôle possible de l'analyse des risques

Opérations. D'après les auteurs, les acteurs proches du risque se livrent rarement à une analyse systématique des options possibles et de leurs conséquences. D'où le besoin que de telles analyses soient conduites ailleurs — même si elles impliquent les mêmes opérateurs, elles seront menées en dehors des opérations ordinaires (lieu éloigné du risque, temps disponible, aides spécialisées). A titre d'exemple, le *Safe Job Analysis* pratiqué sur les plates-formes de forage, conduit un examen des gestes et actions ordinaires afin de les rendre plus surs. Le Crew Resource Management³³ des pilotes de ligne en fournit un exemple plus approfondi et plus développé.

³² Le mode de décision politique prend une dimension internationale à travers les agences internationales de normalisation et de régulation (ISO : International Standards Organisation ; OIAC : Organisation internationale de l'aviation civile ; OMI : Organisation maritime internationale, etc.) où c'est implicitement le consensus qui fonde la décision plutôt que la recherche de l'optimum.

³³ Ce CRM, fort développé dans le monde de l'aviation civile, consiste à étudier les modes de conduite des équipages d'un point de vue non-technique. On y parle beaucoup de culture du risque. La prise de conscience de leur style de conduite par les équipages leur permet une lucidité plus grande qui fait gagner en niveau de sécurité et amène une précieuse homogénéisation de la culture du risque au sein de la compagnie.

Faire progresser la culture de risque des opérateurs passerait par une meilleure perception des aspects de risque dans leurs métiers. Il y a, en effet, des limites aux réponses pré-programmées. Une meilleure perception du risque favoriserait la conduite sûre des opérations. Elle serait soutenue par des indicateurs signalant les limites de sûreté, les marges au delà desquelles on entre dans des zones à risque. Les automatismes de niveau 1 des opérateurs — je réponds à tel cas de figure par telle action — devraient évoluer vers des automatismes de niveau 2 : quoi que je fasse, je dois rester vigilant et prendre le temps de la prudence³⁴.

La fonction de dirigeant. L'évaluation des risques par le dirigeant d'entreprise se base sur une analyse préparée par des experts. Cette prise de connaissance de l'analyse experte peut être plus ou moins approfondie. Le dirigeant peut l'exercer en continu ou se limiter à une vérification finale plus superficielle.

L'analyse formelle (coûts/avantages ou espérance d'utilité) requiert de connaître l'échelle de valeurs du décideur. Sous forme de fonctions de préférence ou bien sous forme de règles et de normes d'éthique, de règles de justice, en quelque sorte. Pourtant, d'après les observations de Mintzberg³⁵, les dirigeants n'ont pas de système prédéterminé et absolu de préférences globales : leurs préférences et leurs valeurs se forgeraient plutôt tout au long du processus décisionnel. C'est pourquoi il est souhaitable que le dirigeant suive le processus d'analyse, particulièrement pour les décisions importantes, et qu'il communique ses préférences et ses valeurs tout au long du processus.

Les études montrent aussi que les dirigeants limitent volontairement la quantité de données qu'ils traitent ; ils se limitent aux prévisions, aux mesures résumées du risque, par exemple aux valeurs moyennes attendues. Ou bien, plutôt que de considérer le risque lui-même et ses évaluations chiffrées, ils recourent à des pratiques acceptées, par exemple en achetant le 'prêt-à-porter' de la gestion HSE (Hygiène, Sécurité, Environnement).

Les urgences et les imprévus ne sont guère anticipés : on '*éteindra les incendies*' le cas échéant.

La société impose aux industriels de plus en plus d'obligations dans le domaine du risque. Or, les normes techniques des divers secteurs de l'industrie ne sont pas orientées risque. Se contenter de ces normes n'est pas de bonne stratégie. Les risques devraient au contraire être décrits et gérés de façon active.

Les décisions politiques. L'aspect parfois chaotique des processus décisionnels issus de négociations politiques est en général dû aux variations des préférences plutôt qu'à des désaccords au sujet de la connaissance impliquée (autrement dit, la science et l'analyse des risques ne sont guère responsables de certaines insuffisances politiques). Lorsqu'un problème est parvenu à être inscrit à l'ordre du jour des questions politiques, la question bénéficie d'une analyse plus ou moins détaillée. Le processus d'analyse précède la décision.

Comme pour les décisions des dirigeants, les aspects de risque et d'incertitude devraient jouer un rôle important dans les décisions politiques. Mais comme il n'y a guère d'accord sur les objectifs et les points délicats, que différents groupes valorisent différemment les divers aspects, il n'est peut-être pas toujours opportun d'insister pour que l'analyse adopte un cadre formel. Il est délicat de prendre en compte tous les points de vue (et les divers aspects de théorie des jeux), surtout si une telle clarification n'est pas souhaitée par certains acteurs.

³⁴ Quand les opérateurs n'ont aucun temps de réflexion, on peut considérer que leur mode de décision est celui de la crise.

³⁵ Professeur de management, analyste des organisations, il est l'auteur reconnu d'une dizaine de livres et de nombreux articles, particulièrement [10]

Le mode analytique.

- (1) Quand ils prennent des décisions, les analystes ne recourent pas toujours à l'optimisation ; ils peuvent suivre des règles ou des codes, ou chercher à satisfaire une batterie de critères (*satisficing*). Un designer, par exemple, satisfait à des contraintes de coût, de poids, de fonctionnalité, de possibilités de production, de fiabilité, etc. Ce designer et son chef, généralement un manager de niveau intermédiaire, analysent les diverses alternatives mais n'entreprennent pas une optimisation globale.

Dans le cas de composants critiques (d'aéronefs, par exemple), une analyse de risque est menée sur le composant, puis incluse dans l'analyse globale de l'appareil. On se rapproche de l'analyse de risque idéale. Mais, en termes de décision, il s'agit plus de réponse acceptable que d'optimisation. L'optimisation requiert l'analyse de *toutes* les alternatives alors que, par exemple dans le cas ci-dessus, la grande majorité des solutions possibles sont en général éliminées *avant* l'analyse de risque détaillée.

- (2) Quand ils préparent des décisions à prendre par d'autres, les analystes traitent un problème de choix classique. Le problème et l'étendue des ressources disponibles (le coût) sont définis par le décideur. Il revient aux analystes de faire préciser les objectifs, d'établir les alternatives, de réunir les données nécessaires, d'établir un modèle explicatif des risques (par exemple, un arbre de défaillances) et enfin de proposer des recommandations.
- (3) Quand ils agissent en soutien des opérateurs exposés au risque, les analystes peuvent, schématiquement, soit leur établir des règles toutes faites, soit améliorer leurs moyens et méthodes de prise de décision. Les analystes doivent rester conscients des limites du préprogrammé, ainsi que de l'acceptabilité des règles pour les opérateurs. Ces règles devraient toujours être accompagnées des hypothèses et objectifs utilisés pour aboutir à ces règles. Il est important que les analystes mettent constamment à jour leurs recommandations en fonction de l'expérience du terrain.

Donner aux opérateurs les moyens de gérer leurs propres risques passe par :

- (a) la communication efficace des informations relatives aux limites de la sûreté,
- (b) la formation à utiliser lucidement ses capacités et à les développer.

La gestion de crise. L'analyse de risque ne peut pas fournir *la* bonne décision puisque les crises sont, par définition, imprévisibles et rares. Le but pourrait être, néanmoins, de dégager des types de décisions adaptées à des types de situations. Par exemple, indépendamment des causes, il est possible de s'intéresser à des procédures d'atterrissage d'urgence ; procédures qui varieront avec les circonstances et le type d'aéronef. Il est bon d'anticiper l'atterrissage d'urgence même si l'on fait tout pour éviter que le cas ne se produise pas.

Le temps de la crise présente des spécificités en termes d'organisation. Les crises sont trop imprévisibles pour pouvoir être efficacement prévenues. Elles sont, en quelque sorte, le résidu de la démarche préventiviste du *risk management*. Elles requièrent d'autres approches et particulièrement de : identifier les situations critiques, autant que possible ; établir des stratégies génériques ; prévoir les rôles et responsabilités ; allouer des ressources pour les crises. Mintzberg (1973) estime que les analystes doivent élaborer des solutions en période calme et même fournir des solutions grossières en temps réel. Mais cela paraît difficile à réaliser, compte tenu de ce qui précède ; depuis l'ouvrage de Mintzberg, les crises ont déjoué toutes les prévisions. En revanche, Lagadec (par exemple dans *Gestion de crise*) recommande lui aussi de monter, en cas de crise, une cellule de réflexion en soutien des décideurs.

3. Schéma des interactions entre analystes et autres acteurs

Ce qui précède montre que la gestion des risques requiert des interactions entre les différents modes de décision (qui peuvent parfois être du ressort des mêmes acteurs). Les figures 3 et 4 fournissent un cadre de description des relations entre analystes et autres acteurs du risque : les analystes sont soumis à diverses influences et fournissent en retour des analyses qui sont rarement transmises telles quelles, mais plutôt dans des formats résumés et adaptés aux divers interlocuteurs. Ces relations sont appelées à se développer car la société requiert de plus en plus d'analyses de risque, alors que les contraintes qui s'imposent aux acteurs ne leur permettent que rarement de mener eux-mêmes une analyse formelle.

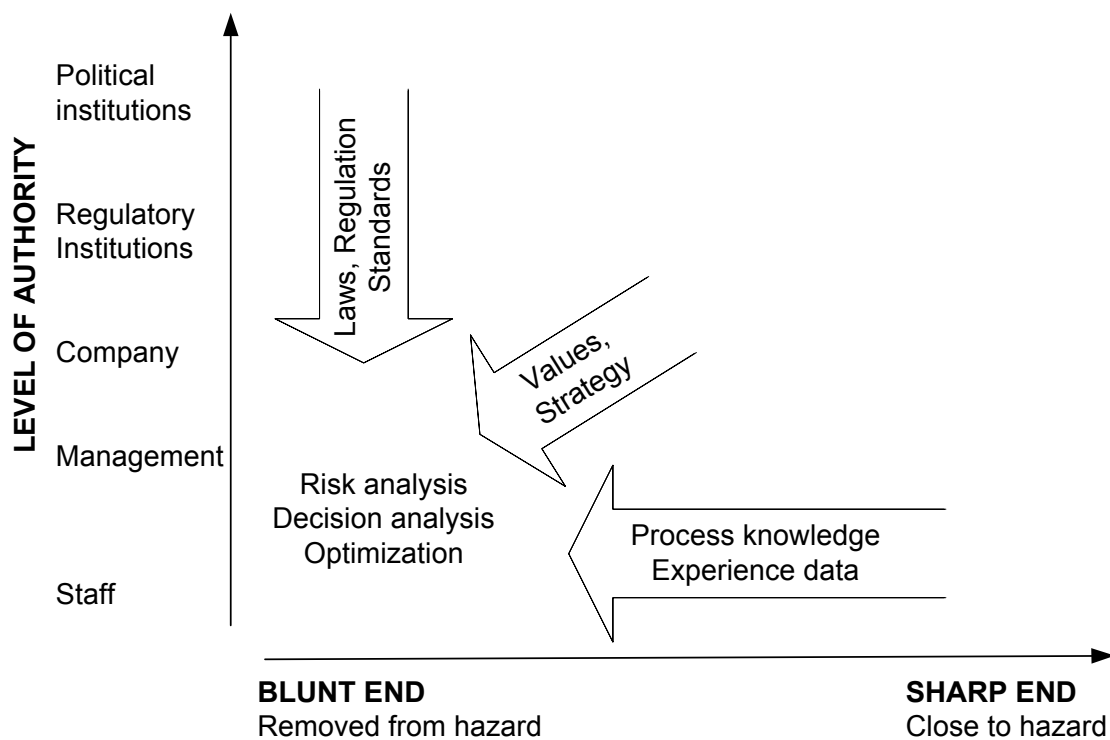


Figure 3 Influences s'exerçant sur les analystes

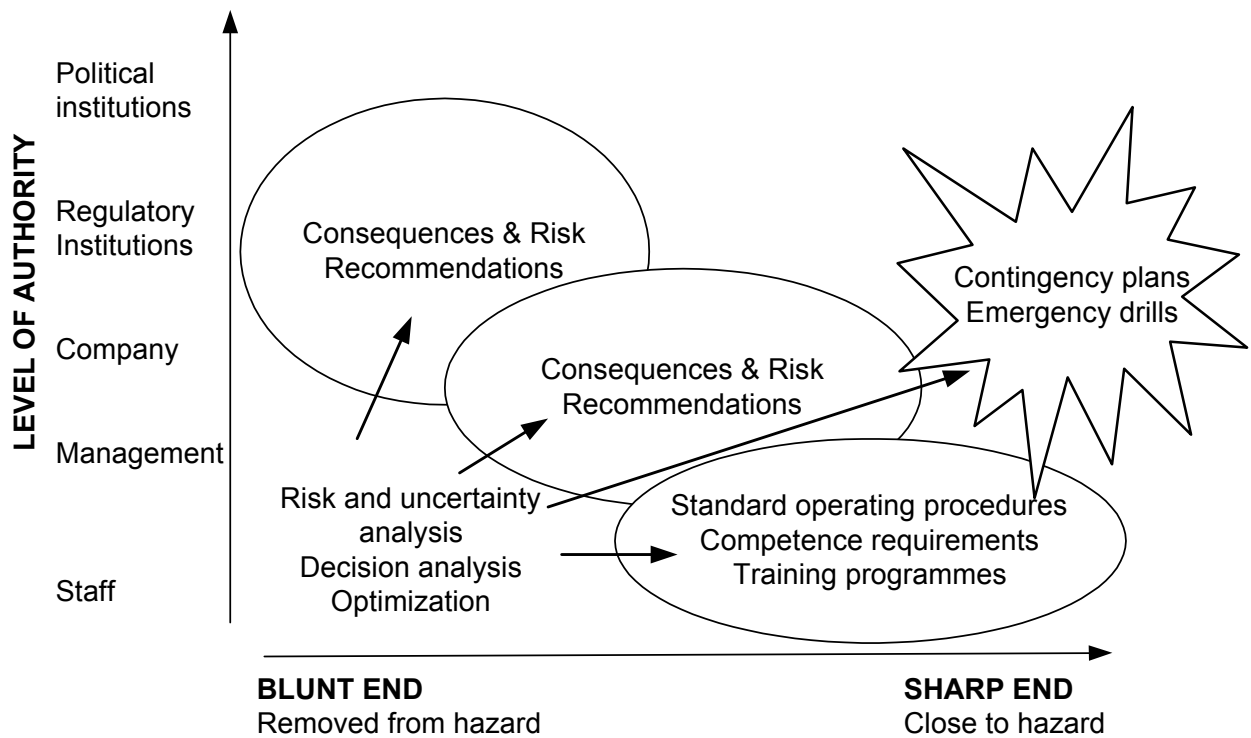


Figure 4 Types de soutien fourni par les analystes

L'image rudimentaire et statique qui vient d'être donnée est limitée par sa généralité. Des réseaux d'interactions plus détaillés pourraient être établis pour des domaines particuliers d'intérêt, des industries spécifiques, des périodes particulières du cycle de vie ou des organisations données. Il apparaît clairement que pour les interactions formelles et pour la gestion du risque, une compréhension et une terminologie communes sont nécessaires.

4. Conclusions

La typologie des décisions présentée ci-dessus précise des contraintes et des limites qui s'imposent aux individus dans différentes situations de décision. Il en résulte que :

1. la gestion des risques implique un réseau d'acteurs divers, en particulier selon leur niveau hiérarchique et leur proximité au risque ;
2. la décision est fortement contrainte, notamment aux niveaux supérieurs de la hiérarchie ainsi qu'à proximité du risque, de diverses façons qui ne favorisent pas une analyse de risque conforme aux prescriptions de la théorie ;
3. les risques pourraient être mieux gérés par ces acteurs en relation étroite avec les spécialistes de l'analyse du risque ;
4. le *risk management* requiert la définition des rôles, des responsabilités et des interactions entre acteurs.

BIBLIOGRAPHIE

- [1] UKOOA, "A framework for risk related decision support - Industry guidelines," UK Offshore Operators Association May 1999 1999.
- [2] NORSOK, "Risk and emergency preparedness analysis - Norsok Standard," Norwegian Technology Standards Institution, Oslo, Standard Z-013, March 1998.
- [3] R. P. Pape, "Developments in the tolerability of risk and the application of ALARP," *Nuclear energy*, vol. 36, pp. 457-463, 1997.
- [4] R. Rosness, "Om jeg hamrer eller hamres, like fullt så skal det jamres," presented at Sikkerhetsdagene 2000, Trondheim, Norway, 2000
- [5] D. D. Woods, L. J. Johannesen, R. I. Cook, and N. B. Sarter, "Behind Human Error: Cognitive Systems, Computers, and Hindsight," CSERIAC, Wright-Patterson Airforce Base, Ohio State of the Art Report 94-01, 1994.
- [6] J. Reason, *Managing the risks of organizational accidents*: Ashgate Publishing Company, 1997 vol. Aldershot.
- [7] R. Rosness and J. Hovden, "From power games to hot cognition - A contingency model of safety related decision-making," presented at Molde seminar, Molde, 2001
- [8] J. Rasmussen, *Information Processing and Human-Machine Interaction*: North Holland, 1986 vol. Amsterdam.
- [9] J. Reason, *Human Error*: Cambridge University Press, 1990 vol. Cambridge.
- [10] H. Mintzberg, *The nature of managerial work*: Harper Collins publishers, 1973 vol.
- [11] J. D. March and H. A. Simon, *Organizations*: John Wiley & Sons Ltd., 1958 vol. New York.
- [12] R. M. Cyert and J. D. March, *A Behavioral Theory of the Firm*: Blackwell Publishers, 1992 vol., 2 ed. Massachusetts.
- [13] G. Allison and P. Zelikow, *Essence of Decision - Explaining the Cuban crisis*: Addison Wesley Longman, Inc., 1999 vol., 2 ed.
- [14] N. Brunsson, "A World of Standardization as a Social Form," Stockholm Centre for Organizational Research SCORE, Stockholm 1998.
- [15] C. Lindblom, "The science of muddling through," in *Public policy*, S. Z. Theodoulou, Ed. New Jersey: Prentice Hall, 1995.
- [16] P. R. Schulman, "Nonincremental policy making," in *Public policy*, S. Z. Theodoulou, Ed. New Jersey: Prentice Hall, 1995.
- [17] I. Janis and L. Mann, *Decision making*: The Free Press, 1977 vol.
- [18] R. Samurcay and J. Rogalski, "A Method for Tactical Reasoning in Emergency Management," in *Distributed Decision Making*, B. Brehmer, J. Rasmussen, and J. Leplat, Eds. Chichester: John Wiley & Sons Ltd., 1991.
- [19] G. Klein and B. W. Crandall, "The role of mental simulation in problem solving and decision making," in *Local applications of the ecological approach to human machine systems*, vol. 2, P. Hancock and e. al., Eds. Hillsdale, NJ: Erlbaum, 1995, pp. 324-358.
- [20] J. Rasmussen, "Risk management in a dynamic society: a modelling problem," *Safety Science*, vol. 27, pp. 183-213, 1997.
- [21] A. Klinke and O. Renn, "Precautionary principle and discursive strategies: classifying and managing risks," *Journal of risk research*, vol. 4, pp. 159-173, 2001.
- [22] T. Aven, *How to Approach Risk and Uncertainty to Support Decision Making (to appear)*: John Wiley & Sons Ltd., 2002 vol. New York.
- [23] J. Rasmussen, "Event analysis and the problem of causality," in *Distributed decision making*, J. Rasmussen, B. Brehmer, and J. Leplat, Eds. Chichester: John Wiley & Sons Ltd., 1991.

19. GESTION DES RISQUES ET MANAGEMENT DE LA QUALITÉ

Ce chapitre cherche à comparer sûreté et qualité à partir des meilleurs représentants de ces deux aspects de la production.

En termes de sûreté, les bons élèves sont par exemple les HRO, *High Reliability Organizations*, étudiés aux États Unis, à l'université de Berkeley. On en décrit cinq caractéristiques : (1) l'autorité est déléguée de façon souple ; (2) il existe une organisation spécifique en cas de crise ; (3) les apports des opérateurs sont reconnus ; (4) la transparence est favorisée, on recherche ouvertement les erreurs ; (5) le changement organisationnel est jugé à l'aune de la sûreté.

Dans le domaine du management de la qualité (MQ), par exemple chez General Electric, grand défenseur des méthodes quantitatives de gestion de la qualité, on retrouve des principes semblables aux quatre premiers points ci-dessus : (MQ1) mobilisation des acteurs et décentralisation ; (MQ2) organisation par projets ; (MQ3) reconnaissance des apports des collaborateurs ; (MQ4) transparence et culture de la mesure et du retour d'expérience. En revanche, la priorité qu'exprime 'le changement organisationnel est jugé à l'aune de la sûreté' ne se retrouve pas nécessairement dans le domaine de la qualité.

Cette priorité donnée à la sûreté, caractéristique des entreprises pourvues d'une bonne culture de sûreté, n'est évidemment pas une priorité absolue. La sûreté absolue, ce serait de ne rien entreprendre de dangereux ! Son statut est probablement complexe, une part relevant de gestion multicritère, une autre de communication.

Le concept de HRO, *High Reliability Organization*

Charles Perrow publie en 1984 son fameux ouvrage *Normal Accidents*. Il y explique que les accidents deviennent inévitables. Les systèmes sont trop complexes pour être parfaitement prévisibles. En outre, leur fonctionnement est trop rigide pour être fiable, trop d'éléments sont liés pour éviter l'accident systémique. Cette approche conclut que la seule solution de prévention est de favoriser des systèmes moins complexes et plus souples. Elle ne croit pas à l'addition de systèmes de sécurité, avec barrières de défense et redondances, car ces systèmes sont eux-mêmes complexes et sources d'aléas imprévisibles.

La question se pose alors de savoir pourquoi il n'y a pas plus d'accidents dans les systèmes hautement complexes et dangereux comme les centrales nucléaires ou les porte-avions. Le 'groupe de Berkeley' (La Porte, Roberts, Rochlin, Schulman) s'est attaché à cette problématique et a défini la notion d'organisation hautement fiable : les HRO, High Reliability Organizations.

Les cinq points d'une HRO

G. Rochlin, un des membres du groupe de Berkeley décrit les caractéristiques des HRO comme suit³⁶ :

1. **L'autorité est déléguée de façon souple.**
2. **Il existe une organisation spécifique en cas de crise.** Ce phénomène a été particulièrement remarqué sur les porte-avions et autres navires de guerre : l'organisation ordinaire est, comme on s'y attendrait, assez hiérarchique, mais en cas d'alerte, l'expertise des agents joue un rôle prépondérant même si leur grade n'est pas élevé (« on est passé aux choses sérieuses, efficacité avant tout »).
3. **Les apports des opérateurs sont reconnus.** Comme dit Rochlin : « Les cultures de sûreté et de fiabilité favorisent, entretiennent et nourrissent un engagement responsable des opérateurs. »
4. **Transparence en matière de sûreté : on recherche ouvertement les erreurs, on récompense la découverte d'erreurs.** Il y a ici une exigence de lucidité. La sûreté, comme le risque, est largement question de perception de sûreté ; d'où la tentation de se donner le confort de la sûreté par un effort d'affichage destiné à engendrer cette perception de sûreté. Contrairement à cette tendance, les HRO vivent en sachant que : « Il y a de vieux pilotes et des pilotes intrépides, mais il n'y a pas de vieux pilotes intrépides ».
5. **Le changement organisationnel est jugé à l'aune de la sûreté.**

Dans les HRO, les opérateurs maîtrisent en faisant face lucidement. Ce sont des professionnels calmes et fiers.

³⁶ G. Rochlin, *Les organisations « à haute fiabilité » : bilan et perspectives de recherche*, in Organiser la fiabilité, M. Bourrier, L'Harmattan, 2001, p. 47.

Les équivalents en management de la qualité

Quand on cherche ce qui correspond aux points ci-dessus dans le management de la qualité on trouve les éléments suivants :

MQ1. Mobilisation des acteurs aux divers niveaux de la structure hiérarchique, ce qui implique, en pratique, une bonne dose de décentralisation. En théorie, poser la décentralisation de l'autorité comme principe de la qualité ne semble pas nécessaire si des mesures chiffrées de performance sont disponibles. Toutefois un spécialiste dit que *« la notion de décentralisation est fondamentale. Pour améliorer l'efficacité d'un process de production par exemple, rien de tel que les techniciens et ingénieurs de production qui travaillent au jour le jour avec les process. Ce sont eux qui ont l'expertise des process. Ce sont les techniciens de production qui savent pourquoi les process ont été réglés de telle ou telle façon (le "fine tuning" des process). Lors de missions en environnement de production, je me suis rendu compte qu'il y avait toute une expertise non-dite : le pourquoi des réglages n'était pas consigné sur papier mais dans la tête des techniciens. »*

MQ2. Organisation par projets. On peut dire qu'une alerte sur un vaisseau de guerre correspond à l'entrée dans un projet particulier. Inversement, en poussant un peu la notion, on peut dire qu'un projet, avec ses objectifs et ses contraintes, est une bataille pour la réussite, une forme de crise, surtout si l'échec est synonyme de licenciement.

MQ3. La reconnaissance des apports des 'collaborateurs' est proche de la responsabilisation évoquée ci-dessus. Dans les démarches qualité, le manager dispose en général d'un indicateur simple de qualité. Il peut alors souvent baser des récompenses sur la performance mesurée par cet indicateur. Tout particulièrement des récompenses monétaires fondées sur des augmentations de profits ou de chiffre d'affaires. Mais on peut trouver des incitations sous forme de pénalités par exemple : *« Arrangez-vous pour faire baisser le taux d'accidents du travail de 10 %, sinon vous serez mal noté ».*

La culture de sûreté étant beaucoup plus difficile à mesurer, et le domaine des risques pouvant avoir des tonalités dramatiques où 'l'erreur humaine' peut avoir des conséquences catastrophiques, la reconnaissance prend des formes souvent moins mesurables, moins brutales.

MQ4. La transparence est nécessaire à la gestion de la qualité et se traduit généralement par une culture de la mesure et du retour d'expérience. Une part des difficultés d'acceptation du management de la qualité par les opérateurs est cette introduction de la mesure, de la performance mesurée, qui impose une lumière crue dans des domaines qui étaient auparavant ouverts à la discussion et à la négociation. Ainsi, la méthode Six Sigma, emblématique du développement de la qualité chez General Electric, a-t-elle pour objectif de ramener l'écart type à moins de un sixième de la plage d'erreur tolérée, ce qui revient à ramener la fréquence de défaut à moins de $3,4 \cdot 10^{-6}$ (sous hypothèse de normalité).

Sur ce dernier point, on pourrait renchérir sur Rochlin : de nombreux auteurs ont souligné qu'une bonne culture de sûreté implique un souci d'amélioration continue. À l'inverse, l'autosatisfaction et le laxisme sont caractéristiques d'une mauvaise culture de sûreté. De même, dans le management par la qualité, le souci est l'amélioration constante de la satisfaction des clients. Ce type de préoccupation à long terme soutient efficacement une culture et crée des échelles de 'fierté du travail'.

Les différences entre sûreté et qualité

Sur le dernier point, en revanche, « le changement organisationnel est jugé à l'aune de la sûreté », il n'y a pas nécessairement d'équivalent dans le domaine de la qualité. La démarche qualité '*mobilise les acteurs*', suscite un '*comité de pilotage avec le Directeur Général et les directeurs concernés*', met en place une '*structure de qualitiens aguerris*' et aboutit à '*des solutions, de nouvelles normes, procédures ou modes d'emploi*'. La qualité implique des changements. Et les changements suscités par d'autres causes doivent respecter la contrainte de qualité. Mais la qualité ne semble pas être un critère en elle-même ; elle est une méthode, un ensemble de méthodes, voire une culture, suscités en vue de l'amélioration du fonctionnement et des produits et donc, finalement, de la rentabilité de l'entreprise.

Il semble donc émerger de cette analyse que :

- dans les HRO la sûreté est une valeur fondamentale ; elle n'est pas nécessairement la seule valeur, mais elle a un rôle de valeur ultime ;
- alors que dans des organisations à la pointe de l'excellence, mais éloignées du risque, les valeurs correspondant à la qualité — l'amour du produit, la satisfaction des clients avant tout — n'ont pas de valeur ultime. Ce sont des façons de faire pour atteindre un objectif ultime autre, à savoir de bonnes performances économiques.

On rejoint ici la définition première de la (bonne) culture de sûreté (INSAG-4, chapitre 1) :

La culture de sûreté est l'ensemble des caractéristiques et des attitudes qui, dans les organismes et chez les individus, font que les questions relatives à la sûreté bénéficient, **en priorité**, de l'attention qu'elles méritent en raison de leur importance.

Dans ce texte, c'est le terme **priorité** que nous soulignons. La qualité est une méthode dans les entreprises d'excellence, la sûreté est une priorité dans les HRO.

20. LA SÛRETÉ EN TERMES ECONOMIQUES

« La sûreté n'a pas de prix, mais elle a un coût ! » Quand on observe les comportements d'industries à risques telles que le nucléaire ou l'aviation, le budget alloué à la sûreté n'est pas infini. Par exemple, les dépenses de sécurité imprévues (dans ce qui suit sécurité et sûreté sont synonymes) sont très mal venues dans un secteur concurrentiel comme celui de l'aviation. Du point de vue des professionnels de la sûreté, le budget est même toujours trop restreint et il y aurait des gains économiques réels à l'augmenter ! Ainsi, le discours sur la priorité de la sûreté est perçu avec scepticisme par l'économiste.

Il est peut-être perçu avec un mélange d'incompréhension et de respect par les financiers responsables des budgets : incompréhension en raison de la difficulté technique liée aux questions de sûreté, renforcée par l'absence d'indicateurs qui rendent compte de façon satisfaisante de l'ensemble des aspects du risque ; et respect en raison de la 'priorité' que représente le risque, de la conscience qu'il s'agit d'enjeux importants.

La modélisation en termes de satisfaction multicritères (*satisficing*, chapitre 18) pourrait peut-être rendre compte de ces contradictions apparentes. Les objectifs poursuivis en termes de sûreté sont multiples, l'une des contraintes, parmi d'autres, étant la contrainte budgétaire. Nombre de décisions ne passent pas par un processus budgétaire et dans ces cas là, la sûreté peut bénéficier d'une priorité. Par exemple, le responsable HSE d'Aventis dispose d'un droit de veto sur les investissements.

De même, un niveau de sécurité *acceptable* est une condition **nécessaire** de fonctionnement des usines à risques. En ce sens, c'est une priorité. Alors que dans une usine de pantalons, par exemple, il ne semble pas devoir en être ainsi.

Dans ce qui suit, nous tentons de replacer quelques questions relatives à la sûreté dans le cadre de la théorie économique classique.

1. Prise en compte de la sûreté dans le comportement des producteurs

La théorie microéconomique décrit le comportement des producteurs dans un modèle désormais classique :

y décrit l'output (ou les outputs), q les prix correspondants,

x les inputs, p les prix correspondants, donc le coût de production est $C(x) = p \cdot x$,

$y = f(x)$ est la fonction de production et l'on suppose pour simplifier qu'à un y donné correspond une solution de production x unique.

Le producteur maximise son profit ; son comportement est dicté par le programme :

$$(1) \quad \left| \begin{array}{l} \text{Max} \\ x \end{array} \right. \quad q \cdot f(x) - C(x)$$

Une façon très simple de prendre en compte la sûreté est de rajouter explicitement les risques qui pèsent sur ce profit. Le programme du producteur devient alors

$$(2) \quad \left| \begin{array}{l} \text{Max} \\ x \end{array} \right. \quad q \cdot f(x) - C(x) - R(x)$$

Formellement, les risques sont représentés par une fonction R exprimée en termes monétaires. Ces risques peuvent être de nature très diverses ; ils ne se limitent pas à la sûreté des établissements à risques. Mais, dans cette prise en compte, les risques doivent pouvoir être exprimés sous forme d'une fonction, d'une évaluation monétaire. Cette fonction peut se limiter à l'espérance mathématique des dommages possibles (le producteur est alors neutre vis-à-vis du risque) ou bien faire intervenir des formulations plus sophistiquées.

Le coût du risque R peut être qualifié de façon plus précise de 'Coût des Risques Résiduels'. En effet, le producteur consacre en général une partie de ses inputs à se protéger des risques les plus évidents. Ce sont par exemple les primes d'assurance incendie, d'assurance auto, d'assurance pertes d'exploitation, mais aussi les coûts imposés par la législation, par exemple sur la prévention des accidents du travail, etc., ou encore parce que les installations doivent être agréées, etc. Dans ce sens, ce coût résiduel peut aussi être appelé coût de la non sûreté.

Le sens de variation de R en fonction des différents inputs x_i n'est pas unique. R est fonction décroissante de certains inputs, par exemple ceux liés au risque ou à la sûreté, ce qui traduit le fait qu'investir dans la sûreté permet de baisser le niveau de risque. Elle est fonction croissante d'autres inputs, par exemple ceux qui font directement et uniquement augmenter la production, car en général, lorsque l'on pousse la production, le niveau de risque augmente ou, au moins, ne diminue pas.

Le programme qui définit le choix de la firme implique : $\partial C/\partial x_i = q \cdot \partial f/\partial x_i - \partial R/\partial x_i$. Pour tout input x_i , le coût marginal doit être égal à la productivité marginale diminuée du coût marginal du risque ou de la non sûreté. Cette relation s'interprète différemment selon les inputs :

1. pour les inputs qui sont indépendants du risque (comme dans le cadre de la microéconomie classique) : $\partial f/\partial x_i \geq 0$ et $\partial R/\partial x_i = 0$; leur productivité marginale est positive et leur influence sur les risques est nulle ; par conséquent, résultat classique, le coût marginal doit être égal à la productivité marginale $\partial C/\partial x_i = q \cdot \partial f/\partial x_i$;
2. pour les inputs qui n'affectent que la sûreté, $\partial f/\partial x_i = 0$ et $\partial R/\partial x_i \leq 0$; la productivité marginale en output marchand est nulle, mais le risque résiduel marginal diminue avec l'emploi de ce type d'input (par exemple les primes d'assurance) ; par conséquent, $\partial C/\partial x_i = -\partial R/\partial x_i$ le coût marginal doit être égal à la réduction marginale de risque, un résultat de type classique ;
3. pour les inputs de production, en général, $\partial f/\partial x_i \geq 0$ et $\partial R/\partial x_i \geq 0$; la productivité marginale est positive ainsi que le risque résiduel marginal ; par conséquent, l'équation ci-dessus ne se simplifie pas, la prise en compte de la sûreté amène à utiliser moins de ces inputs et donc à diminuer la production ;
4. certains inputs améliorent la sûreté, mais au détriment de la production, $\partial f/\partial x_i \leq 0$ et $\partial R/\partial x_i \leq 0$ (par exemple l'équipements de sûreté qui bride un moteur, qui pèse dans un avion, etc.) ; la productivité marginale en output marchand est négative, mais le risque résiduel marginal est amélioré par l'emploi de ce type d'input ; par conséquent, l'équation ci-dessus ne se simplifie pas, la prise en compte de la production amène à utiliser moins de ces inputs de sûreté que dans le cas classique (cas 2) ;
5. enfin, certains inputs ont toutes les qualités ; ils agissent favorablement sur la production et sur la sûreté , $\partial f/\partial x_i \geq 0$ et $\partial R/\partial x_i \leq 0$; ces inputs doivent être utilisés plus que s'ils étaient considérés uniquement dans le cadre de la production ou uniquement dans le cadre du risque et de la sûreté, car il faut tenir compte de leur double productivité sur ces deux plans³⁷.

Où l'on perçoit que l'opposition entre production et sûreté n'est pas inéluctable du point de vue de la théorie économique. On peut même penser que l'énumération de la liste ci-dessus milite en faveur de l'utilisation de procédés ou de modes de production privilégiant les inputs doublement positifs (type 5).

³⁷ On pourrait encore ajouter les inputs qui ont tous les défauts, étant à la fois contre-productifs et néfastes pour la sûreté. C'est le cas des réformes qui dégradent le climat social qui, à son tour, nuit à la production et à la sûreté. C'est aussi le cas de certaines erreurs de management.

2. A la recherche du coût de la sûreté

La séparation entre production et sûreté que l'on perçoit dans certains styles de gestion de risques ne peut donc être introduite qu'en éliminant les inputs de type 3, 4 et 5.

Dans le cas général, une notion simple de coût de la sûreté est loin d'être justifiée :

- partons d'une petite baisse de risque exogène δ ; par exemple, un changement de législation fait que, en dernier ressort, l'évaluation par le producteur de ses risques diminue de δ (ce δ est une quantité complexe qui résulte d'un calcul qui peut prendre en compte tout un ensemble de modifications, un calcul d'espérance, une fonction d'utilité propre au producteur, etc.) ;
- δ équivaut, du point de vue du producteur, à une hausse de la production dy qui laisse le profit identique, donc :

$$q.dy - C'(y).dy - R'(y).dy = \delta^{38}$$

On peut ainsi donner un équivalent en production (par exemple en tonnes) d'une amélioration du risque ;

- mais la valorisation de cette production dy serait $q.dy - C'(y).dy - R'(y).dy$, c'est-à-dire δ ; on tourne en rond, en quelque sorte ; la fonction R inclut déjà la notion de coût du risque ; le coût de la sûreté n'est rien d'autre que son inverse, le coût de la réduction du risque.

Si maintenant nous désirons nous rapprocher d'un modèle implicitement assez courant — qui ne correspond pas à la réalité de la production —, modèle qui sépare abusivement production et sûreté, supposons qu'il n'existe que des inputs de type 1 et 2 ci-dessus, soient :

x les inputs de pure production (type 1), p les prix correspondants ;

s les inputs de pure sûreté (type 2), p' les prix correspondants ;

le coût de production est $C(y) = p.x + p'.s$ qui se décompose en

$$CP(y) = p.f^1(y) \text{ coût de production et } CS(s) = p'.s \text{ coût de sûreté ;}$$

le risque résiduel R dépend maintenant de x et de s , ou bien de y et de s avec

$$\partial R / \partial y \geq 0 \text{ et } \partial R / \partial s_i \leq 0.$$

La sûreté optimale s^* est alors déterminée par les équations marginales $\partial C / \partial s_i = - \partial R / \partial s_i$.

Cette simplification — encore une fois nous pensons qu'elle ne doit pas être encouragée —, permet d'examiner plusieurs notions de coût de la sûreté :

- la somme globale $CS(s^*)$; ce coût est partie intégrante de l'activité, au même titre que le coût des inputs de production ; dans cette acception, la sûreté peut être assimilée à un input comme un autre, le spécialiste de la sûreté est apprécié au même titre qu'un 'acheteur' (spécialiste des achats d'inputs et de matériels) ;

³⁸ Comme nous avons supposé, pour simplifier, qu'une production y correspond à une combinaison d'inputs x unique, les fonctions de x sont également des fonctions de y , par exemple $C(y)$ désigne $C(f^1(y))$.

- la somme $CS(s^*) + R(y^*, s^*)$ qui comprend le coût de la sûreté, au sens restrictif, et le coût de la non sûreté ; cette ‘version non expurgée’ est moins confortable, mais plus réaliste... ;
- le coût marginal $CS'(s)$, pris en s^* ;
- comme ci-dessus, le coût marginal $d[CS(s^*) + R(y^*, s^*)] / ds$, pris en s^* ;

Ces notions ne sont pas opérationnelles. Elles ne débouchent pas sur des recommandations utiles ni sur des représentations valables. Elles ne font qu'éloigner des solutions les plus avantageuses, celles qui consistent à soigner l'ensemble du système de production considéré et à gagner sur les deux tableaux. L'intelligence organisationnelle d'ensemble (y compris une conception des installations qui donne toute sa place aux questions de sûreté) est probablement la grande ressource en matière de sûreté. En tous cas, le réflexe de tout observateur confronté à un ‘coût de la sûreté’ devrait être de *s'interroger sur le coût de la non sûreté* qu'il laisse subsister...

Pour faire plus de place à une possible opposition de la sûreté et de la production, considérons maintenant directement une contrainte budgétaire $C(y) = p \cdot x + p' \cdot s \leq k$, avec un input de production qui n'a aucun effet risqué et un input de sûreté qui n'a aucun effet sur la production. L'optimum de gestion implique dans ce cas que la productivité marginale de l'input de production est égale à la productivité marginale de l'input de sûreté en termes de sûreté³⁹. L'opposition entre sûreté et production n'apparaît donc toujours pas :

- il n'y a pas de coût d'opportunité : disposer d'une partie ∂k des dépenses de sécurité (ou de l'investissement en sécurité) ne permettrait pas d'améliorer le résultat global en l'investissant en améliorations de production. Comme l'entreprise optimise l'utilisation de ses moyens, il est indifférent qu'elle investisse ∂k en production ou en sûreté. L'amélioration attendue de profit de production serait contrebalancée par un excès équivalent de dépenses (d'une autre nature que ∂k et probablement imprévues : pertes dues à des incidents plus nombreux, par exemple, ou excès de coûts de maintenance si la notion de sûreté retenue inclut la maintenance).

Pour pousser jusqu'au bout la possibilité d'opposition entre sûreté et production, dans le cadre ci-dessus, il faut introduire directement une contrainte de sûreté. En effet, l'optimisation ci-dessus conduit à des niveaux x^* , et donc s^* , optimaux du point de vue de la firme, mais qui ne vérifient pas nécessairement une contrainte extérieure de sûreté du type $s \geq s_0$. Rajouter une telle contrainte fait alors baisser la production et le profit.

En l'absence d'une telle contrainte de sûreté qui force le producteur à plus de dépenses de sûreté qu'il n'en prendrait au vu de l'optimisation de son profit privé, il est difficile de proposer une notion de coût de la sûreté unique et satisfaisante. En revanche, une telle contrainte extérieure peut être justifiée, notamment au regard du :

- coût social total du risque. Cette notion englobe tous les risques que la production laisse subsister malgré les dépenses de sûreté consenties : risques résiduels pour l'entreprise, comme ci-dessus, mais aussi les risques pour tous les autres acteurs. Dès qu'il y a de telles externalités, par exemple si les riverains d'une usine à risques doivent subir des dommages au cas où une catastrophe surviendrait, ce coût est supérieur à la somme globale $CS(s^*) + R(y^*, s^*)$.

³⁹ $q \cdot f'(x)/p = -R'(s)/p'$ où s est déterminé par x à partir de la contrainte budgétaire.

3. La sûreté et le marché

La fonction objectif ci-dessus, $q.f(x) - C(x) - R(x)$ se décompose en deux parties bien distinctes :

- $q.f(x) - C(x)$ est le profit comptable ; c'est une grandeur dont le statut dépasse largement celui de la théorie économique ; elle intervient dans les règlements de comptabilité qui la définissent avec précision ; elle sert à l'administration fiscale pour prélever l'impôt ; elle est observée avec attention par les investisseurs, agences de notations, et autres analystes financiers et joue, par leur intermédiaire, un rôle crucial sur les capacités du producteur à recourir au marché des capitaux à des conditions intéressantes ;
- $R(x)$ est une grandeur largement inconnue ; certes elle joue un rôle qui devrait être décisif sur les politiques de sûreté du producteur, mais elle le fait nécessairement par l'intermédiaire de ce que l'on en sait. On pourrait poser : $R(x) = RR(x) - RI(x)$, où le risque résiduel pris en compte R est le risque réel RR dont il est séparé par le risque ignoré RI . Ce verbe 'ignorer' décrit parfaitement les deux actes qui séparent le réel et le perçu : ignorer sans le vouloir, en raison de la difficulté à connaître, et ignorer volontairement parce que cela semble avantageux...

Le profit ordinaire est une donnée qui s'impose au producteur avec toute la force dont le marché est capable. En revanche, la sûreté perçue — qui s'identifie donc au risque résiduel perçu — n'est pas une donnée. Elle est produite par la culture de l'entreprise et peut varier en fonction des personnes et des circonstances, dans la mesure où elle ne s'éloigne pas trop des obligations réglementaires. Par exemple, dans le cas où le profit passe en-dessous d'un certain seuil⁴⁰, la firme est en danger de mort économique. Dans ce cas, la tentation du gestionnaire est grande de rogner sur les 'coûts de sécurité' : plutôt risquer un accident incertain (le pire n'est jamais sûr) que d'accepter une mort économique annoncée.

Certains facteurs favorisent une telle dégradation de la culture de sûreté :

- faible considération pour les autorités qui « ne servent à rien », « empêchent les forces vives de travailler », « mangent l'argent du contribuable », « ne connaissent rien aux difficultés de la vie économique », etc. ;
- faible capacité des autorités (à quelque niveau que ce soit, la force de la chaîne n'excède pas celle du maillon le plus faible), inspection ou répression ;
- décisions relatives à la sûreté prises à des niveaux où prévaut l'abstrait voire le virtuel (finances, direction générale) et où dominent les considérations économiques.

Ce schéma peut mettre en jeu des violations caractérisées de la sûreté ou bien se traduire par une série d'actes moins flagrants tels que réduction des 'budgets de sécurité' ou nomination de personnels moins expérimentés et disposant de moins de prestige et d'autorité (donc moins chers mais aussi moins efficaces en moyenne). Il peut intervenir en cas de menace de mort économique ou bien quand les responsables concernés sont sous pression (de la hiérarchie pour un chef d'établissement, des marchés pour un PDG, etc.).

⁴⁰ En général, la théorie économique simple envisage un seuil de zéro, mais certaines entreprises protégées peuvent se permettre des profits négatifs (des entreprises de transport ferroviaire, de distribution de courrier, etc.), alors que d'autres sont confrontées à des 'exigences du marché' se traduisant par des taux de profit nettement positifs (par exemple, le fameux 15 % de retour sur investissement de la période de la bulle).

Autrement dit, l'entreprise est soumise à deux pressions qui correspondent à des termes séparés de la fonction objectif ci-dessus : la pression économique et les exigences de sûreté. Or, ceux qui prennent les décisions importantes sont susceptibles de baigner dans la pression économique beaucoup plus que dans les exigences de sûreté. Ils penseront beaucoup plus à maximiser le profit qu'à assurer la sûreté. Ils sont mus et jugés par une culture du résultat — du combien —, alors que les questions de sûreté sont largement des questions de méthode (de moyens au sens de Management basé sur les Moyens) — de comment.

La pression du marché va donc plutôt à l'encontre des objectifs de sûreté.

4. Sûreté perçue et dommages subis

Le risque résiduel réel, **RR**, n'est que très imparfaitement connu, même dans des domaines classiques comme celui des accidents de la route. On cite le cas emblématique d'une 2CV, voiture modeste dont les primes d'assurances sont des plus modiques, qui, tombant d'un pont avait provoqué un déraillement qui avait à son tour provoqué une grave pollution... L'ensemble des dommages se chiffrait en millions d'euros.

Ainsi, dans la modélisation ci-dessus, l'optimisation incluse dans le 'Max' n'est qu'apparente puisqu'on n'optimise pas la véritable fonction de sûreté **RR**, celle à laquelle voudraient se référer les purs théoriciens du risque, mais seulement **R**, ce que les décideurs connaissent et acceptent de connaître des risques résiduels (et sans doute plus généralement des coûts de la sûreté).

Cette incertitude — pas toujours combattue avec énergie si la culture de sûreté n'est pas excellente — milite encore un peu plus pour quelques tolérances envers certains écarts en matière de sûreté. La menace que la sûreté tombe à des niveaux trop bas garantit néanmoins que les critères qui président aux choix de SP ne soient pas trop relaxés.

Afin d'éclairer ce qui précède, nous passons maintenant à une formalisation parallèle de la qualité.

5. Différences entre sûreté et qualité

Formellement, la gestion de la qualité pourrait se représenter comme ci-dessus :

$$\left| \begin{array}{l} \text{Max} \\ x \end{array} \right. \quad \mathbf{q.f(x) - C(x) - NQ(x)}$$

où **NQ** représente le coût de la non qualité.

Le coût de la qualité est une notion aussi contestable que le coût de la sûreté, pour les mêmes raisons que celles évoquées ci-dessus. Il serait en général conçu comme les dépenses nécessaires aux services qualité (personnel, documentation, formation, sondages et inspection, etc.); y seraient parfois ajoutés les surcoûts éventuels de production imposés par les exigences de qualité.

Les coûts de la non-qualité, **NQ**, comportent : production de produits hors normes, à réformer, coûts des retours, gestion des réclamations, etc.

On aperçoit immédiatement le parallèle avec la modélisation de la sûreté. On observe néanmoins des différences :

- le coût de la non-qualité est imposé par les clients, il fait partie des données du marché, les retours et réclamations sont réels et incontournables, ils ne sont ni ‘perçus’ ni négociables ;
- c’est une notion moins complexe que le risque résiduel **R** ; celui-ci peut impliquer une estimation des courbes dommages/probabilités pour un grand nombre de risques bien définis ; une agrégation de ces dommages avec l’estimation d’effets croisés ; un calcul d’espérance, la prise en compte d’une fonction d’utilité propre au producteur, etc. ; **NQ** n’est que l’ensemble des coûts mesurables indiqués ci-dessus⁴¹ ;
- un produit de qualité dispose de conditions de marketing très supérieures à un produit de moindre qualité. En effet, la qualité signifie précisément répondre aux besoins et aux desiderata des clients (et non pas ‘être un produit haut de gamme’ ; un stylo bille de type Bic peut très bien être d’excellente qualité —dans les deux sens du terme —, alors qu’un stylo haut de gamme peut ne pas être un produit ‘qualité’ — à nouveau dans les deux sens du terme).

Les dépenses de qualité consenties aujourd’hui sont donc une forme d’investissement destiné à garantir le marché de demain. Une véritable culture de la qualité cherche à fidéliser les clients et va jusqu’à orienter l’entreprise vers la satisfaction des besoins du client. Ceci va bien au delà de la production d’un produit ‘plus fiable’ ou ‘mieux conçu’ : il s’agit de détecter les besoins futurs des clients pour les satisfaire avant et/ou mieux que les concurrents (voir, par exemple le manuel de qualité de la société américaine de composants Atmel, <http://www.atmel.com/atmel/acrobat/doc2043.pdf> dont est issu le diagramme ci-dessous) :



6. Utiliser le marché pour soutenir la sûreté ?

Les forces du marché concurrentiel soutiennent les démarches qualité alors qu’elles vont plutôt à l’encontre des efforts consentis pour garantir la sûreté. La seule façon d’aller contre cette tendance serait de créer un ‘client’ intéressé à la sûreté :

⁴¹ En cas de fortes variations de qualité, il faut y ajouter une estimation des effets d’image.

- Par exemple, les inspections des installations à risque ne coûteraient rien aux établissements inspectés et donneraient lieu au paiement de primes non négligeables aux bons élèves (il faut alors concevoir que les coûts correspondants proviennent d'un fond alimenté par les preneurs de risques). Un tel système rendrait plus palpable et plus attractif l'intérêt d'une bonne sûreté.
- Pour se rapprocher d'un système directement lié au risque réel RR, on peut imaginer que les agents les mieux placés sont les assureurs. Leur mesure du risque est, en théorie, une espérance mathématique des dommages qui devrait, a priori, être une des meilleures expressions de RR. En pratique, néanmoins, la fixation des primes d'assurance est un exercice très éloigné de l'estimation 'scientifique' de RR⁴² et les primes ne reflètent que très imparfaitement les efforts de prévention consentis par les assurés. Dans ces conditions, le fait de disposer d'une assurance peut même dissuader certains investissements de sûreté.
- Les courtiers en assurance, avec l'aide de leurs experts, sont probablement plus à mêmes de contribuer à établir RR et à suggérer des voies classiques d'amélioration de la sûreté. Néanmoins, nous avons suggéré que l'intelligence organisationnelle est souvent l'input le plus important pour améliorer la sûreté et d'autres aspects de la production. On voit mal les courtiers en assurance s'aventurer dans ce domaine. De plus, comme pour les assureurs, mais dans une moindre mesure, la recherche de leur profit personnel risque d'entrer en conflit avec l'intérêt financier de leur client.
- Le risk manager d'entreprise a précisément pour rôle d'optimiser l'utilisation des instruments financiers de réduction de risque opérationnel (en majorité les assurances), d'identifier les risques et d'estimer RR, d'inciter les unités à la prévention. Mais le cloisonnement des tâches et la technicité des questions de sûreté éloignent le risk manager des questions de sûreté proprement dites et tendent à le rapprocher de la direction financière. Dans les grandes entreprises, il existe un manager QHSE (Qualité, Hygiène, Sécurité, Environnement) dont le rôle est de veiller à la sûreté. En général, l'ampleur de ses actions est limitée par un budget consacré à la sûreté.
- Dans le domaine de l'utopie, on peut imaginer des inspections conduites par des certificateurs indépendants, relayées auprès des clients et jouant sur leurs comportements d'achat d'une façon significative, repérable par le producteur...

Il existe donc un vaste chantier autour de la question : comment inciter les entreprises à prendre en compte la pérennité et la régularité de leur action ? Le MEDD pourrait s'intéresser à ce chantier.

Ainsi, il n'y a pas contradiction entre qualité et profit même si, à court terme, la qualité impose des coûts. Il y a même synergie entre qualité et profit voire impérieuse nécessité de qualité pour survivre. Il nous semble que la sûreté devrait être conçue dans cet esprit, celui de l'amélioration tenace, persévérante et jamais achevée des méthodes de production avec autant d'effets positifs sur ladite production.

⁴² Les assurances utilisent leurs inspecteurs pour éviter de grosses surprises et pour avoir des arguments de négociation face au client. Elles ne sont nullement motivées à répercuter le risque réel ; leur comportement consiste à tenter d'imposer la prime la plus élevée possible tout en ne perdant pas le client. Si elles cherchaient à connaître le risque réel, elles ne pourraient pas se contenter de visites de terrain parfois aussi brèves qu'une seule demi-journée pour les risques environnementaux. De plus, elles pratiquent par type de risque (incendie, auto, etc.) et non pas du point de vue global du producteur.

D'ailleurs, les ingénieurs qualité sont amenés à améliorer les 'process' pour garantir un excellente fiabilité des produits. Ce faisant, ils contribuent en général à améliorer la sûreté.

21. LES SYSTÈMES DE GESTION DE LA SÛRETÉ EN FRANCE

L'intelligence du risque dans le domaine de l'aviation civile (chapitre 9) permet de mesurer combien la gestion indirecte des risques par l'autorité de régulation est susceptible de faire progresser la culture de sûreté. Nous envisageons ici la possibilité d'étendre ce type de régulation au domaine des établissements terrestres à risques.

Certains soutiennent que l'obligation de tenir un système de gestion de la sûreté (SGS) existe déjà en France pour les entreprises présentant des risques significatifs. Nous montrons : (i) que le champ des entreprises à risques est loin d'être couvert ; (ii) que les SGS existants ne sont pas obligatoirement satisfaisants en raison de la difficulté à auditer ces systèmes et à prendre des mesures contraignantes le cas échéant.

Le champ couvert par les SGS

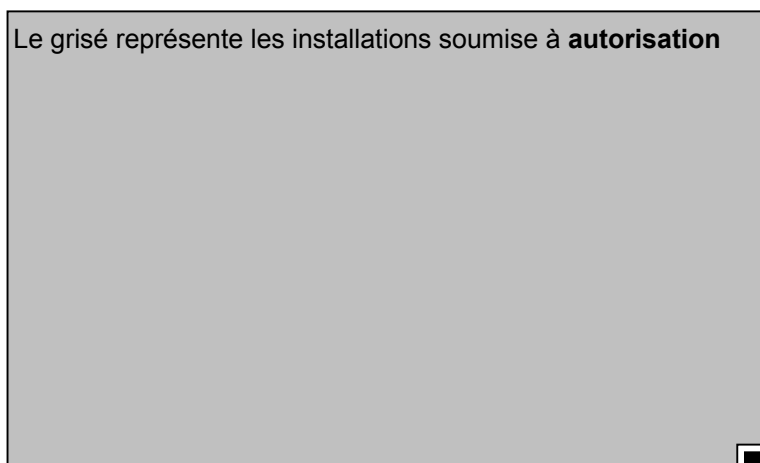
Depuis les textes du 10 mai 2000 (arrêté : <http://www.environnement.gouv.fr/infoprati/bulletin-officiel/bo-200205/A0050028.htm>, circulaire : idem [/bo-200009/A0090054.htm](http://www.environnement.gouv.fr/infoprati/bulletin-officiel/bo-200009/A0090054.htm)), les installations SEVESO dites à seuil haut sont soumises à l'obligation d'utiliser un SGS. Mais ce sont ainsi quelques 600 installations qui sont concernées. Or, en chiffres ronds, il y a :

600 000	installations soumises à déclaration (ICPE, loi de 1976)
60 000	installations soumises à autorisation
1 200	installations SEVESO
600	installations SEVESO seuil haut avec SGS obligatoire

Ainsi, 1% seulement des installations potentiellement dangereuses sont soumises à cette obligation. Une installation n'est, en principe, pas soumise à autorisation si elle ne présente pas de danger. Un expert de l'Ineris estime qu'environ 20 000, parmi les 60 000, présentent des risques d'atteintes sérieuses à l'homme ou à l'environnement.

Le graphique ci-dessous permet de visualiser les proportions en cause.

La surface de l'ensemble de la feuille représente les installations soumises à **déclaration**



Le rectangle blanc représente les installations SEVESO au sein desquelles le noir représente les installations SEVESO seuil haut soumises à SGS.

Pourquoi les installations SEVESO sont-elles ‘privilegiées’ ? C’est en raison de l’existence d’une législation européenne qui se focalise sur les installations manipulant des substances dangereuses. Ainsi, dans l’ensemble des installations à risques, on a privilégié, de fait, le risque chimique, spécifiquement celui des substances dangereuses. Si une entreprise ne manipule pas de produits dangereux, elle ne peut pas être classée SEVESO.

Parmi les autres risques, on pourrait citer le risque d’explosion. Il concerne aussi des installations non liées à la chimie ou aux substances dangereuses, par exemple les silos (explosion de Blaye, 1997, 11 morts) ou les chaufferies (explosion de la chaufferie de La Défense, 1994⁴³, 2 morts, une soixantaine de blessés).

Efficacité des SGS

Motivation. Gérer les risques à partir d’un SGS est la meilleure façon de procéder. Mais l’existence du SGS ne garantit une meilleure gestion que si le SGS est utilisé en pratique, si les conclusions des analyses se traduisent par des mesures sur le terrain.

Les entreprises les meilleures n’ont pas attendu l’obligation SEVESO pour utiliser les SGS. Les premiers ont été mis en place par des entreprises soucieuses de limiter leurs risques, notamment aux États Unis où les primes d’assurance des accidents du travail sont considérables. Aujourd’hui, en France, ce sont ces entreprises responsables, pourvues d’une forte culture du risque, qui sont les meilleures en matière de SGS. Celles, au contraire, qui gèrent au minimum d’effort, les yeux rivés sur des indicateurs comptables, peuvent ne pas tirer du SGS tout le profit possible. C’est une question d’attitude et de motivation.

On retrouve ici l’importance de la *culture* du risque pour la mise en œuvre des *techniques* de traitement du risque. Il y a entre les deux une différence de nature et un ordre ‘hiérarchique’. C’est bien pourquoi les actions au niveau de la culture du risque sont beaucoup plus profondes, plus nécessaires, mais aussi plus délicates à appliquer.

Le but essentiel du SGS n’est pas la gestion des incidents, ni même des accidents ordinaires, mais la prévention des accidents majeurs. Son efficacité, la maîtrise opérationnelle, concerne le passage de la gestion documentaire à l’application sur le terrain ; l’expérience manque encore dans ce domaine, notamment en raison de la rareté des accidents graves.

Audit. Il est donc nécessaire que le SGS soit audité. Les inspecteurs des installations classées ont commencé à remplir cette tâche. Pour ce faire, ils ont bénéficié de programmes de formation, notamment avec l’aide de l’Ineris. Il n’en reste pas moins que le métier d’inspecteur et celui d’auditeur sont très différents. Il est relativement simple de vérifier un taux d’émission ou la présence de tel dispositif de sécurité. Auditer un système de management est d’une autre nature. On peut donc estimer qu’une période d’adaptation sera nécessaire.

Compte tenu du nombre d’inspecteurs disponibles, il sera nécessaire de mettre en place une expertise extérieure confiée à des professionnels dont le métier sera l’audit des systèmes de management et particulièrement des SGS. C’est la recommandation du rapport Essig ainsi

⁴³ Le mercredi 26 septembre 2002, le journal télévisé de FR3 était en direct de Toulouse : dans le quartier de la Défense, l’explosion de Toulouse a fait ressurgir des souvenirs chez tous les riverains de la centrale Thermique de Nanterre qui avait explosée en 1994. Aujourd’hui les riverains ne cachent pas leur inquiétude. Jacques Kossowski, le maire de Courbevoie, vient donc d’écrire au Ministre de l’environnement pour lui demander de prendre des mesures de sécurité ou tout simplement la délocalisation de cette installation.

que, semble-t-il, la voie suivie dans la version actuelle du projet de loi sur la maîtrise des risques technologiques. Les récents scandales américains, notamment concernant Andersen, montrent que la certification ou la tierce expertise (dans le cas présent) posent des questions délicates. Les pouvoirs publics pourraient se préoccuper, a minima, de certifier les experts. Actuellement, n'importe qui peut s'installer expert en SGS.

L'aspect répressif. Le SGS doit, en priorité, amener au respect des normes. Il doit aussi aller beaucoup plus loin dans l'identification et le suivi des risques. Que se passe-t-il si l'autorité de surveillance constate des manquements ?

L'idée de la régulation indirecte des risques est basée sur la bonne volonté des entreprises, sur leur désir d'éviter des risques extrêmement coûteux qu'elles ont identifiés comme tels. Mais il faut néanmoins qu'une menace crédible existe à disposition de l'autorité. Ces deux conditions sont réunies dans le cas de l'aviation (chapitre 9) : les compagnies sont très sensibilisées au risque et l'autorité de surveillance a la possibilité de mettre fin à l'habilitation d'une compagnie aérienne.

Dans le cas des entreprises à risque soumises à SGS, les meilleures sont sensibilisées et répondront certainement à une remarque de l'autorité, remarque qu'elles accueilleront probablement avec intérêt comme pouvant leur permettre d'améliorer les risques. Les plus mauvaises, en revanche, considèrent probablement qu'elles ne courent elles-mêmes aucun risque et que le SGS n'est qu'une lubie de plus de l'administration, des coûts supplémentaires inutiles. Elles traitent alors le SGS comme un élément de communication. Les qualités d'un auditeur doivent alors être faites d'une extrême rigueur (c'est le revers du côté indirect du contrôle), d'une persévérance sans faille unie à un certain messianisme. Il faut, enfin, que l'autorité puisse réagir si nécessaire.

Or, la répression passe en France, non pas par une autorité technique comme dans le cas de l'aviation civile, mais par le préfet. Celui-ci est responsable de peser les avantages et les inconvénients d'une mesure répressive. Une vision souvent exprimée à ce sujet est que le préfet n'a ni la pérennité ni l'expertise d'une autorité technique et qu'il est parfois sensible au chantage à l'emploi et autres arguments économiques de court terme. Pour lui, la sûreté n'est qu'une priorité parmi d'autres, au contraire des HRO (voir chapitre 17), alors qu'elle est la raison d'être d'une autorité de contrôle. Dans le passé, les préfets auraient donc assez rarement suivi l'inspection des installations classées, ce qui aurait eu pour effet de créer une certaine auto-censure au niveau des inspecteurs eux-mêmes. En termes de défense en profondeur, la première ligne de défense était alors mise en brèche par l'incurie de l'entreprise, la deuxième ligne de défense par la frilosité et les délais de l'action des pouvoirs publics.

Dans ces conditions, un audit extérieur du SGS pourrait se traduire par la possibilité d'alertes sur certains sites, alertes qui ne concerneraient pas directement le préfet, mais surtout les inspecteurs. La menace serait alors une visite d'inspection (et non d'audit)...

22. LE STYLE D'INTERVENTION DE L'ADMINISTRATION

Quand l'administration cherche à mettre en œuvre une action nationale dans le domaine des risques, elle ne se contente plus de définir seule ce plan et d'en commander l'exécution dans un style régalién. Le style actuel est basé sur la culture de dialogue administration-industrie. Néanmoins, les industriels ne se précipitent évidemment pas pour proposer des actions onéreuses. Ils se contentent bien entendu de réagir, ce qui fixe l'administration dans son rôle proactif. Il faut aboutir. Et l'on arrive donc, au terme de la concertation, à l'établissement de plans nationaux concertés. Cette concertation permet-elle d'assurer la responsabilisation des exploitants ? Nous estimons qu'une étape importante pourrait être franchie dans ce sens en se focalisant sur le développement de la culture du risque.

Malgré le dialogue administration/industrie, la nécessité d'agir aboutit, en effet, à faire peser sur l'administration la charge de l'évaluation des risques (c'est elle qui prend l'initiative). La nécessité du dialogue incite à réunir l'ensemble des parties prenantes administratives (afin d'assurer la cohérence de l'action de l'administration) et les représentants des industriels concernés (afin que les conclusions soient acceptables). Mais le groupe de travail ainsi créé a pour objectif un programme d'actions. Au final, les actions adoptées sont issues de l'initiative de l'administration qui dirige ce groupe de travail.

Avec une méthode d'intervention inspirée par l'amélioration de la culture de sûreté, le groupe de travail aurait pour but de proposer un objectif de risque qui s'impose à tous les établissements. On se mettrait d'accord non pas sur des actions, mais sur :

1. les méthodes d'évaluation des risques ;
2. le niveau de risque visé sur le territoire national⁴⁴ ;
3. l'obligation pour les établissements d'atteindre ce niveau par des moyens laissés à leur initiative et à leur responsabilité ;
4. la mise en place d'un système de gestion des risques permettant aux établissements de suivre l'évolution de leurs risques dans le futur ; ce système serait harmonisé, en ce sens qu'il comprendrait un certain nombre de caractéristiques obligatoires, un noyau commun permettant à la fois l'harmonisation nationale et la vérification par l'administration ;
5. les mécanismes de contrôle (voir 1.) et d'attribution des responsabilités en cas de sinistre (par exemple, les règles de responsabilité environnementale).

Dans le premier cas, l'administration a un rôle de partenaire prépondérant du dialogue. Dans le second, son rôle est d'assurer le dialogue et de l'arbitrer. Il paraît alors logique d'adjoindre au groupe des représentants de la population, par exemple des maires de France et des riverains ce qui va dans le sens des objectifs affichés de dialogue et de transparence.

⁴⁴ Le niveau de risque lui-même peut dépendre des conditions locales, mais la manière de définir ce niveau doit être sans ambiguïté au niveau national.

Dans le premier cas, l'administration impulse et négocie un programme d'actions à entreprendre par les établissements ; dans le second, elle conduit les établissements à prendre en main leurs risques et suscite les actions plutôt que de les impulser.

Ces différences peuvent paraître superficielles, mais elles sont profondes. Car, dans le premier cas, la charge du risque repose en large partie sur l'administration. Les entreprises n'ont aucun intérêt à précéder le 'réveil' de l'autorité ; au contraire, elles sont incitées à attendre un événement, par exemple une catastrophe dont on se rassure qu'elle « n'arrivera pas chez nous », catastrophe qui donnera à chacun au sein de l'entreprise la légitimité d'effectuer les dépenses, d'autant plus que ces dépenses seront imposées par 'l'extérieur'. D'une certaine façon, ce style de relation entre administration et entreprises permet à ces dernières d'externaliser leur responsabilité au titre de la gestion des risques. En quelque sorte : « Tant que l'administration n'intervient pas, c'est que je suis en règle. Et pourquoi voulez-vous que j'aie dépenser de l'argent alors qu'on ne me le demande pas ? »

Non seulement l'approche par l'amélioration de la culture de sûreté responsabilise les preneurs de risques, mais encore elle pérennise l'action de l'administration. Dans le premier cas ci-dessus, une fois le 'programme d'action' achevé, rien n'empêche la pression sur les établissements de retomber. En période de rigueur budgétaire, par exemple, la probabilité est forte qu'il en soit ainsi jusqu'au nouveau 'réveil' des responsables. Alors que si les établissements sont amenés à gérer eux-mêmes leurs risques, s'il est bien clair qu'ils en sont responsables, alors le problème se pose beaucoup moins.

Nous donnons ci-après un exemple illustratif de ces idées.

Création d'un groupe de travail d'harmonisation de la sécurité des sites industriels de stockage de GPL classés SEVESO

Le Communiqué de presse officiel
(juillet 2002)

La Direction de la Prévision des Pollutions et des Risques (DPPR) du Ministère de l'Ecologie et du Développement Durable et le Comité Français du Butane et du Propane (CFBP) ont fait le point des problèmes posés par la mise en œuvre et le stockage des gaz de pétroles liquéfiés (GPL). A l'issue de cet examen, la DPPR a décidé de créer un groupe de travail d'harmonisation des actions de renforcement de la sécurité des sites industriels de stockage de GPL présentant des risques d'accident.

Ce groupe de travail sera composé de représentants de la DPPR, des Directions Régionales de l'Industrie, de la Recherche et de l'Environnement (DRIRE), du CFBP et de l'industrie des Gaz de Pétrole Liquéfiés (GPL); et aussi de représentants de la Direction de la Défense et de la Sécurité Civile du ministère de l'Intérieur, de la Sécurité Intérieure et des Libertés Locales, et de représentants du ministère de l'Equipement, des Transports, du Logement, du Tourisme et de la Mer.

Il est créé dans le but de proposer un programme d'actions visant à réduire les risques dans les sites industriels classés SEVESO et à en harmoniser la gestion. Après un travail de classification de ces sites selon des critères objectifs, il proposera un programme adapté aux risques inhérents à chaque site pour garantir un niveau de sécurité satisfaisant sur l'ensemble du territoire national. Un échéancier de réalisation sera élaboré pour chaque site.

Le groupe de travail rendra ses conclusions pour la fin du mois de novembre 2002, en dégageant un premier programme d'actions à entreprendre au cours des deux prochaines années.

Possible rédaction dans l'esprit du développement de la culture de sûreté

La Direction de la Prévision des Pollutions et des Risques (DPPR) du Ministère de l'Ecologie et du Développement Durable et le Comité Français du Butane et du Propane (CFBP) ont fait le point des problèmes posés par la mise en œuvre et le stockage des gaz de pétroles liquéfiés (GPL). A l'issue de cet examen, la DPPR a décidé de créer un groupe de travail d'harmonisation ~~des actions de renforcement~~ de la sécurité des sites industriels de stockage de GPL ~~présentant des risques d'accident~~.

Ce groupe de travail sera composé de représentants de la DPPR, des Directions Régionales de l'Industrie, de la Recherche et de l'Environnement (DRIRE), du CFBP et de l'industrie des Gaz de Pétrole Liquéfiés (GPL); et aussi de représentants de la Direction de la Défense et de la Sécurité Civile du ministère de l'Intérieur, de la Sécurité Intérieure et des Libertés Locales, et de représentants du ministère de l'Equipement, des Transports, du Logement, du Tourisme et de la Mer; *et enfin de représentants des maires de France et des riverains des installations à risques.*

Il est créé dans le but de proposer un *programme d'évaluations des risques résiduels* dans les sites industriels classés SEVESO et à harmoniser le niveau de ces risques. Après un travail de *définition en commun d'une méthodologie d'évaluation harmonisée, basée sur des outils pratiques*, il proposera un *niveau de risque applicable sur l'ensemble du territoire national*. *Les établissements devront définir quelles méthodes ils comptent mettre en œuvre pour atteindre ce niveau.*

Un échéancier de mise en place d'un système de gestion des risques sera élaboré par chaque site. Ce système sera vérifiable à tout moment par les inspecteurs des installations concernées.

23. RÉSISTANCES À LA FORMATION ET AU RETOUR D'EXPERIENCE

Un exercice intitulé “*The Day After... in Cyberspace... in Switzerland*” (*Training Civil Servants for Crisis Management*, Journal of Contingencies and Crisis Management, December 2000, extraits ci-après) a révélé des manques au niveau de la réponse à une guerre de l’information et a donné lieu à :

- création d’une Fondation pour l’Assurance de l’Information ;
- élaboration d’un système d’alerte ;
- organisation d’un nouvel atelier de formation ;
- création d’un groupe chargé d’assister le Conseil Fédéral dans le domaine de la protection des infrastructures.

Voilà un exemple d’excellence : des mesures sérieuses prises après un exercice. En revanche, ne rien faire après une véritable catastrophe comme celle de Toulouse serait, en comparaison, le niveau zéro de l’apprentissage.

Il ne manque sans doute pas de résistances. L’article cite :

- la crise est tellement spécifique qu’on ne peut pas vraiment s’y préparer ;
- les procédures et les pense-bête sont inutiles ;
- puisque les crises sont imprévisibles, il vaut mieux ne pas s’y entraîner et éviter ainsi de penser, à tort, que l’on est préparé ;
- ne vaut-il pas mieux garder l’esprit ouvert pour être réactif et créatif lors de la crise ?
- la plupart des crises se résolvent finalement d’elles-mêmes, pourquoi y perdre du temps et de l’argent ?
- la crise est perpétuelle de nos jours, la gestion courante est, en fait, gestion de crise...

L’article dit : « La plupart des fonctionnaires occupant des positions élevées sont réticents à s’exposer à un processus de formation. » D’où, en écho à « On ne peut rien faire, Madame la Ministre », la réponse qu’il rapporte, aux besoins de formation :

“No time — No need — No money”.

Training Civil Servants for Crisis Management (extraits)

Laurent F. Carrel

This article describes and reflects upon actual experiences in training leaders in the Swiss government. Five thematic areas that are fundamental to preparing a government for leadership in a crisis are presented. Additionally, planning the training, the use of expertise and factors which facilitate or hinder strategic learning are discussed. The author recommends the development of a model learning strategy for governments, with the assistance of the European Academy for Crisis Management.

The 'Yes's' Reason

Crisis management is essentially the ability to solve by adapting very quickly to a fast changing situation. While governmental institutions are historically very slow to affect changes, experience has shown that training can be a rapid and efficient way of improving change management within government. Training prepares the group mind-set to cope with new possibilities, provides structures that frame the decision-making process, and offers learning tools such as checklists which can later serve as the procedural backbone during a crisis. Training practitioners take lessons learned *after* a crisis as valuable inputs for leadership *before* the next crisis, as well as for preventing a crisis.

The following example shows how training can assist a government in preparing for crisis. In 1997, the exercise 'The Day After ... in Cyberspace ... in Switzerland' illuminated a series of shortcomings in the Swiss government for preparing and coping with Information Warfare. As a result, an ad hoc group of participants of the exercise assisted representatives of the government and private industry in the formation of an Information Assurance Foundation which became operational in 1999. One of the Foundation's Missions is to create an IT early warning system. In addition, the Foundation is co-operating with the Staff of Strategic Leadership Training to prepare a Workshop in 2000, and a major event in 2001 on the topic of Leadership in, after and before a crisis brought about by disturbances in the IT infrastructure. Another result of the 1997 exercise was the formation of the Joint Staff for Information Assurance, set up by the Strategic Information Agency to

Assist the Federal Council in the Field of Critical Infrastructure Protection.

The 'No's' Reason

There have been many reasons voiced for not training governmental institutions for crisis management. The training professionals in Switzerland heard loud, defensive voices asserting that each crisis is so unique that it is not possible to prepare for them. Standing Operating Procedures and checklists are useless. Since crises come unexpectedly, it is better not to train and mistakenly think that one is ready. Isn't it better to keep an open mind, to be adaptive and creative in a crisis? Since most crises resolve themselves, why spend the time and money? There is a constant and ongoing crisis in governing nowadays, so that everyday management of governmental affairs equals crisis be needed. *No time – No need – No money.*

Behind this barrage of NO reasons lies the simple observation that most civil servants in high positions are reluctant to expose themselves to a training process. They do not want to admit what they do not know and they are fearful of making mistakes that could jeopardize their careers. While every civil servant would gladly come to an inspiring, high-level discussion, leading a crisis management team in a scenario-based simulation game is a totally different story. Thus, the real 'no' is psychological and emotional, and difficult to reason with.

To alleviate some of the fear and to increase the level of participation, training professionals in Switzerland arranged such safeguards as barring media from the exercise games, planning scenarios with a reduced level of surprise, operating on the philosophy of 'no

fault learning', and providing extensive preparation of the participation of some of the Federal Council members, The Swiss 'presidents,' served as an incentive for every other level of government employee. In the final analysis, however, it was outside pressure, or the prospect of outside pressure, and not insight that led to the acceptance of training by Swiss civil servants: a string of 'case studies' of real crises during which the performance of the government was less than optimal led to bad press and parliamentary reprimands.

Because of the resistance encountered, achieving participation in an exercise for civil servants may seem to be the highest hurdle that crisis management training professionals face. Having won the battle of attendance, however, the professional must be ready and understand what to teach, when and how to teach it.

Factors that facilitate or hinder strategic Learning

Every practitioner will find in his course of training a large number of factors that facilitate or hinder strategic training. The following have been important in the Swiss Strategic Leadership Training program:

Compartmental thinking. In an administration, issues are often staked off and fiercely guarded within departments. This poses a problem to learning and crisis prevention, because the increasing complexity of political issues makes maintaining boundaries a difficult task. The crisis management training strategy must work towards interdisciplinary thinking, encouraging sharing and transdepartmental thinking. Joint staffs or task forces formed around issues can be helpful techniques.

Benchmarking, a method of comparing one's performance with another, can facilitate strategic training and crisis preparation by raising awareness of any performance gap. Comparison is also a natural motivating force. There is an increasing number of resources available to the training professional on how to do benchmarking

Restricted organizational curiosity and openness complicates the task of training administration officials for crisis management. Even if a hypothetical scenario is used in a crisis simulation game, the willingness of civil servants to 'play around' with new ideas and policies is very limited. The group-think phenomenon can quickly punish people who try something new (tHart, 1994). The climate of openness is further suffocated by tight internal rules regarding who participates at which level, from which department, and at which training. One possible solution would be the introduction to crisis management training course of the 'court fool', someone with the freedom to express wildly differing opinions and options openly.

Involved leadership and allocated resources can be called the most essential factors that facilitate strategic training. As it is in the private sector with the involvement of the CEO, the participation and the backing by the Federal Council in Strategic Leadership Training and crisis preparation sends a clear signal to the entire administration how important learning is. Leaders can use their high position to demonstrate that they understand and have learned what they want their directors and general secretaries to learn. Unfortunately, leaders often miss this opportunity, having failed to understand that learning is an investment and not a cost. The development of an enhanced capability of crisis management cannot be accomplished without a significant and ongoing commitment of resources.

Summary Recommendation

As seen in this article, providing crisis management training for a government administration is tough job, but one which all countries must undertake. The newly established European Academy for Crisis Management could assist national efforts by serving as a forum to exchange ideas, and by spearheading the development of a model learning strategy for governments. Additionally, the Academy could co-ordinate international co-operation during specific training exercises, drawing on the expertise of its members.

24. LES INSPECTIONS SONT-ELLES EFFICACES ?

Dans le cas d'AZF, Toulouse, on se souvient que le site avait fait l'objet d'une inspection quelques mois avant l'explosion. Celle-ci avait trouvé que les normes de sûreté étaient bonnes. Or, le premier rapport rendu public par la Justice semble au contraire trouver une série de défaillances des procédures de sûreté.

Il est intéressant de constater que cette inversion du jugement après accident n'est pas un phénomène isolé. C'est peut-être, au contraire le cas général. C'est ce que l'annexe 11 montre dans le cas de l'usine américaine d'Institute, fleuron de Union Carbide, de Piper Alpha, de Barings. À tel point que Lord Cullen qui dirigeait la commission d'enquête sur la plate-forme Piper Alpha a pu dire des inspections : « qu'elles étaient superficielles au point d'être de peu d'utilité pour juger de la sûreté. »

Les inspections sont souvent incapables de déterminer les erreurs latentes, par exemple le fait que les responsabilités ne soient pas clairement définies, elles ne peuvent mesurer les conditions générales du risque, l'amont des incidents. Peut-on le leur reprocher ? Pour avoir assisté à des inspections dans des classes où nous étions élèves, nous savons que l'inspection ne peut apercevoir que la surface. Combien plus quand il s'agit d'organisations compliquées, impliquant des catégories variées de personnel, des tâches diverses qui s'entrecroisent et des techniques nombreuses et pointues...

En outre, l'inspection peut être déresponsabilisante, elle prend peu ou prou en charge le risque, ou du moins elle délivre un satisfecit, au lieu de replacer systématiquement (au sens propre, c'est-à-dire par le simple fait du système de régulation lui-même) la responsabilité du risque sur les établissements.

La production de sécurité est la production de non-événements. Quand la production de sécurité fléchit, les incidents n'apparaissent pas immédiatement — les conditions latentes se dégradent, ce qui n'est pas facile à déterminer. Avec de la chance, des incidents apparaissent en assez grand nombre pour que l'on se préoccupe d'améliorer la sûreté avant la catastrophe. Quand on n'a pas de chance, la catastrophe se produit avant cette réaction. On se rappelle la note de service AZF notant la baisse de la sécurité...

Dans leur malheur, les toulousains ont eu de la chance : il n'y a pas eu de nuage toxique.

CONCLUSION : LA CONDUITE DU CHANGEMENT

L'ensemble de cet ouvrage plaide pour une évolution vers une meilleure culture du risque et de la sûreté. Mais comment ce changement peut-il s'opérer ? Par le pari de la connaissance, et le pari de la confiance⁴⁵ c'est-à-dire l'intelligence du risque et son partage à l'intérieur des organisations à risques (établissements de production, mais aussi communes soumises à des risques naturels importants ? etc.), avec toutes les personnes concernées, mais aussi à l'extérieur, avec toutes les parties prenantes, ainsi qu'à l'intérieur des administrations, mais aussi à l'extérieur, avec toutes les parties prenantes. Nos organisations sont davantage conçues pour la stabilité que pour le changement, elles préfèrent souvent ne rien faire, se protéger, attendre. Il faut accepter l'incertitude du changement, observer la réalité telle qu'elle est, partager les analyses.

Développer l'intelligence du risque et de la sûreté prendra du temps, un réel investissement intellectuel, de nouveaux modes de raisonnement et d'abandonner les modèles insuffisants (par exemple, 'l'erreur humaine' chère aux médias) même s'ils rassurent, car ils obscurcissent la vue et brouillent l'écoute.

* * *

Nos organisations sont davantage conçues pour la stabilité que pour le changement, de même d'ailleurs que leurs dirigeants ont été davantage formés à assurer la continuité qu'à gérer ou mettre en œuvre la rupture.

Il en résulte une véritable obsession du « plan d'action », à travers lequel on cherche à tout prévoir, tout organiser, tout contrôler dans les moindres détails, et dont l'élaboration devient à la fois la condition indispensable pour se « lancer » et, en même temps, une fin en soi. Cette façon d'appréhender les choses est bien entendu paralysante car rien ne peut être totalement prévu ni planifié. L'entrée dans le processus lui-même se trouve toujours repoussé jusqu'à ce que, nécessité faisant loi, c'est-à-dire les contraintes extérieures étant de plus en plus pressantes, on n'ait plus le choix, on soit le dos au mur ou, pour le dire plus brutalement, en situation de crise. Mais le changement par la crise, si bien décrit et analysé depuis longtemps par Michel Crozier, est encore plus coûteux. Il ne correspond donc plus aux nécessités du moment, et seules les organisations qui ne sont pas encore tout à fait contraintes à rendre des comptes – les administrations, par exemple – peuvent se le permettre.

La tentation demeure de ne rien faire, de se protéger, d'attendre que l'orage passe et de couvrir cet immobilisme d'une impressionnante fumée de plans d'action sophistiqués, de projets savamment hiérarchisés, de groupes de réflexion, d'étude et de travail. Bref, de substituer l'agitation à l'action, jusqu'à ce que le processus se paralyse de lui-même et se perde dans les méandres incontrôlables dont, au bout d'un certain temps, personne ne se soucie plus.

Ceux qui ont réussi le changement n'ont pas cherché à tout contrôler ni à tout diriger. Ils n'ont pas jugé absolument indispensable de savoir où ils allaient pour y aller. Ils ont fait le pari de la connaissance – faire face à la réalité – et le pari de la confiance – partager cette connaissance avec les premiers concernés : leur personnel.

⁴⁵ Voir François Dupuy, *L'Alchimie du Changement*, Dunod, 2001, dont nous tirons l'essentiel de ce qui suit.

Cette approche ne va pas de soi. Se confronter à la réalité, accepter de la regarder telle qu'elle est et non pas telle que l'on souhaiterait qu'elle soit, en d'autres termes écouter peut être dérangent pour certains dirigeants. Ceux là estiment qu'ils doivent savoir plus et mieux que les autres ce que les choses sont, ce qu'elles doivent être et comment y parvenir. Il y a, dans cette acceptation de la réalité, une modestie mais aussi un courage qui doivent s'apprendre, comme le suggère Chris Argyris.

Cet accès à la connaissance ne peut pas être spontané. Pour y parvenir, il faut du temps et non de la précipitation, de l'agitation ou de la suractivité. Il faut un réel investissement intellectuel, qui suppose l'acquisition et la maîtrise de nouveaux modes de raisonnement, la plupart du temps très éloignés de ceux qui sont enseignés. En particulier, il faut accepter d'abandonner les modèles — modèles quantitatifs, modèles d'organisations, modèles de comportements... — qui rassurent en même temps qu'ils obscurcissent la vue et empêchent d'écouter. Il n'y a nulle surprise à ce que chacun d'entre nous cherche à raccrocher la part de réalité à laquelle il fait face à un ensemble plus vaste et déjà connu. Dans une situation tendue, telle que celles qui exigent la mise en œuvre d'un changement, cela réduit l'incertitude et permet d'utiliser des solutions « qui ont fait leurs preuves » dans des circonstances que l'on pense analogues. Mais le risque est grand alors de renoncer à comprendre la réalité spécifique à laquelle on est confronté. L'expérience nous apprend qu'il faut écouter, elle ne nous dit pas ce que l'on entend.

Le pari de la confiance

Le partage de la connaissance est encore plus inhabituel que l'exigence d'intelligence, parce qu'il suppose une confiance aussi peu familière à nos organisations que l'investissement dans la connaissance. Elles consentent un effort immense et constant pour tenter de réduire l'incertitude inhérente aux hommes : règles, organigrammes, prescriptions, procédures... L'homme, peu digne de confiance. D'où l'idée de « résistance au changement » qui sert de paravent à l'immobilisme de bon nombre de dirigeants.

Une organisation est avant tout un ensemble de comportements, de stratégies rationnelles. Les acteurs peuvent modifier ces comportements si on leur fait partager la nécessité du changement, c'est-à-dire, finalement, la connaissance. Ce postulat de l'intelligence des acteurs s'éloigne des approches traditionnelles du management, marquées par la suspicion, le doute et la nécessité du contrôle au sens le plus étroit du terme. Mais c'est lui qui fonde l'évolution possible du comportement de ces acteurs intelligents et soutient le passage par la confiance.

L'autonomie, l'information, la capacité de choix augmentent dans les organisations. Il y a de plus en plus de travailleurs de la connaissance, de l'intelligence et de l'information⁴⁶. Ces nouveaux travailleurs questionnent les injonctions, critiquent ce qui leur est proposé quand il ne correspond pas à une appréhension fondée de la réalité, de leur réalité.

Partir de la réalité, donc de la connaissance, est une nécessité d'autant moins contestable qu'il faut réduire les coûts humains et financiers du changement. Cet investissement est valorisé en associant toutes les parties à la connaissance, et en les impliquant dans la recherche de solutions pratiques.

⁴⁶ 'knowledge workers'

ANNEXE 1

CULTURE DE SÛRETÉ

Rapport du
Groupe consultatif international
pour la sûreté nucléaire

AGENCE INTERNATIONALE DE L'ENERGIE ATOMIQUE
VIENNE, 1991

COLLECTION SECURITE N° 75-INSAG-

TABLE DES MATIERES

RESUME	1
1. INTRODUCTION	3
2. DEFINITION ET NATURE DE LA CULTURE DE SURETE	5
3. CARACTERISTIQUES UNIVERSELLES DE LA CULTURE DE SURETE	6
3.1. EXIGENCES IMPOSEES AUX RESPONSABLES DE LA POLITIQUE	8
3.1.1. Déclaration de politique de sûreté	8
3.1.2. Structures de direction	9
3.1.3. Ressources	10
3.1.4. Autocontrôle	10
3.1.5. Engagement	11
3.2. EXIGENCES IMPOSEES AUX DIRIGEANTS	11
3.2.1. Définition des responsabilités	11
3.2.2. Définition et contrôle des pratiques de sûreté	12
3.2.3. Qualifications et formation	12
3.2.4. Récompenses et sanctions	13
3.2.5. Audit, examen et comparaison	14
3.2.6. Engagement	14
3.3. REACTION DES INDIVIDUS	15
4. ELEMENTS D'APPRECIATION	17
4.1. GOUVERNEMENT ET ORGANISMES GOUVERNEMENTAUX ... 17	
4.2. ORGANISMES EXPLOITANTS	19
4.2.1. Echelon des responsables de la politique	19
4.2.2. Echelon de la centrale	19
4.2.2.1. L'environnement de travail	20
4.2.2.2. Attitudes individuelles	21
4.2.2.3. Expérience de la centrale en matière de sûreté	22
4.3. ORGANISMES DE SUPPORT	22
5. OBSERVATIONS FINALES	24
Appendice: INDICATEURS DE LA CULTURE DE SURETE	25
A1. Gouvernement et organismes gouvernementaux	25
A2. Organisme exploitant	26
A3. Organismes de recherche	33
A4. Organismes chargés de la conception	34
MEMBRES DU GROUPE CONSULTATIF INTERNATIONAL POUR LA SURETE NUCLEAIRE	37

RÉSUMÉ

Les réactions suscitées par la publication précédente du Groupe consultatif international pour la sûreté nucléaire (INSAG), intitulée «*Principes fondamentaux de sûreté pour les centrales nucléaires*» (n° 75-INSAG-3)⁴⁷, ont montré qu'à l'échelon international beaucoup souhaitaient que le concept de culture de sûreté soit développé de façon que l'on puisse juger du niveau atteint sur des exemples concrets. Le présent rapport répond à ce besoin. Il s'adresse plus spécialement à la direction de tous les organismes dont les activités influent sur la sûreté des centrales nucléaires.

Lorsqu'il a entrepris d'établir un rapport sur la culture de sûreté, l'INSAG a été confronté au fait que ce concept n'avait pas été parfaitement défini dans les études antérieures et qu'il n'existait pas de consensus sur sa signification. En cherchant à formuler des opinions qui puissent être partagées par tous et qui présentent un intérêt pratique, l'INSAG a jugé nécessaire d'explorer de manière approfondie les facteurs généraux qui contribuent à un régime satisfaisant de sûreté nucléaire. Il en est résulté un document exposant le point de vue commun des membres de l'INSAG.

La première proposition avancée par l'INSAG est la définition de la culture de sûreté:

La culture de sûreté est l'ensemble des caractéristiques et des attitudes qui, dans les organismes et chez les individus, font que les questions relatives à la sûreté des centrales nucléaires bénéficient, en priorité, de l'attention qu'elles méritent en raison de leur importance.

Cet énoncé a été rédigé avec soin de manière à faire ressortir que la culture de sûreté est une question d'attitude tout autant que de structure, qu'elle concerne à la fois les organismes et les individus et qu'elle exige que toutes les questions de sûreté soient perçues et traitées comme il convient.

Cette définition relie la culture de sûreté aux réactions et aux façons de penser habituelles des individus ainsi qu'au style des organismes. E en découle une deuxième proposition, à savoir que, si ces éléments ne sont généralement pas mesurables, ils donnent lieu cependant à des manifestations perceptibles et qu'il est donc nécessaire de définir les moyens d'utiliser ces manifestations tangibles pour examiner ce qu'elles recouvrent.

L'INSAG est d'avis que des procédures rationnelles et de bonnes pratiques ne suffisent pas si elles sont seulement appliquées de manière formelle. Il en découle une troisième proposition: la culture de sûreté exige que toutes les tâches importantes pour la sûreté soient exécutées correctement, avec diligence, de manière réfléchie, en toute connaissance de cause, sur la base d'un jugement sain et avec le sens des responsabilités requis.

La culture de sûreté se manifeste dans deux grands domaines: d'une part, l'organisme et l'action de sa direction et, d'autre part, les individus qui travaillent au sein de cet organisme. Le succès dépend toutefois de l'engagement et de la compétence tant des responsables de la politique et des dirigeants que des individus eux-mêmes.

Les chapitres 1 à 3 du présent rapport développent les idées complémentaires que constituent le cadre mis en place au niveau des responsables de la politique et des dirigeants et les réactions individuelles. Ce développement reste général de façon que les vues exprimées soient applicables à tout organisme dont les attributions influent sur la sûreté nucléaire.

Pour que ce rapport puisse servir concrètement à améliorer la sûreté des centrales nucléaires, il fallait qu'il soit plus étoffé. Tous ceux qui s'occupent de questions touchant à la sûreté nucléaire affirmeront probablement que ce qu'il décrit caractérise parfaitement leur propre façon de voir. Tous diront: «Mais c'est ce que nous faisons déjà.» L'INSAG a donc jugé opportun d'aller plus loin, de sorte que la dernière partie du présent rapport donne plus de détails sur les caractéristiques visibles d'une culture de sûreté satisfaisante dans différents types d'organismes. Dans le corps du texte, ces précisions sont données sous la forme d'assertions indiquant ce que l'on devrait attendre, et dans l'appendice sous la forme d'une série de questions ayant pour objet d'aider les organismes à s'évaluer eux-mêmes et non pas de leur fournir une liste de contrôle appelant des réponses du type oui/non.

Enfin, lors de l'établissement du présent rapport, l'INSAG a pris soin de ne pas se borner simplement à énumérer les bonnes pratiques et les exigences à remplir pour assurer un comportement individuel satisfaisant car, s'il est certainement bon de les réaffirmer, cela ne fait guère avancer les choses. L'INSAG s'est efforcé plutôt d'analyser et d'illustrer la question de manière plus générale en formulant des propositions, et d'indiquer comment les organismes peuvent examiner et améliorer leurs pratiques, leur performance et leurs méthodes de travail. C'est sur cette base que l'INSAG soumet le présent rapport à titre de contribution au renforcement de la sûreté des centrales nucléaires.

⁴⁷ GROUPE CONSULTATIF INTERNATIONAL POUR LA SURETE NUCLEAIRE, Principes fondamentaux de sûreté pour les centrales nucléaires, Collection Sécurité n° 75-INSAG-3, AIEA, Vienne (1990).

1. INTRODUCTION

1. A l'exception de ce que l'on appelle parfois les «cas de force majeure», les problèmes qui peuvent se poser dans une centrale nucléaire ont en général pour origine une erreur humaine. Cependant, l'esprit humain dispose d'une grande aptitude à déceler et à éliminer les problèmes potentiels, ce qui a des effets positifs importants sur la sûreté. Les individus assument donc une double responsabilité. Par-delà le respect des procédures définies, ils doivent agir conformément à une «culture de sûreté». Les organismes exploitant des centrales nucléaires et tous les autres organismes ayant des responsabilités en matière de sûreté doivent instituer une culture de sûreté afin de prévenir les erreurs humaines et de tirer parti des aspects positifs de l'action des hommes.

2. En substance, la culture de sûreté est le moyen d'assurer qu'une grande attention est prêtée à la sûreté tant par les organismes que par les individus. L'INSAG a introduit l'expression «culture de sûreté» dans son Rapport récapitulatif sur la réunion d'analyse de l'accident de Tchernobyl⁴⁸. Dans un rapport ultérieur intitulé «Principes fondamentaux de sûreté pour les centrales nucléaires»⁴⁹, qui sera désigné par la suite sous la cote INSAG-3, il a fait ressortir que la culture de sûreté constitue un principe fondamental de gestion. Le présent rapport fait suite aux observations communiquées après la publication d'INSAG-3 pour proposer que le concept de culture de sûreté soit clarifié et défini de telle manière que son existence puisse être confirmée dans des cas précis.

3. Le présent rapport accorde une attention particulière aux organismes exploitants, car c'est dans ces organismes que le lien entre la performance humaine et la sûreté des centrales est le plus étroit. Il traite cependant aussi de la culture de sûreté chez tous ceux qu'elle concerne, étant donné qu'un très haut niveau de sûreté ne peut être atteint qu'à la condition que chacun adhère à cet objectif commun.

4. La sûreté d'une centrale dépend en outre dans une très large mesure de ceux qui l'ont conçue, construite et mise en service. Il faut citer aussi la communauté des scientifiques et ingénieurs en

général, les organes gouvernementaux chargés de la réglementation et ceux qui s'occupent de la recherche fondamentale.

5. L'INSAG-3 recensait des aspects particuliers de la culture de sûreté. Il traitait également de questions qui n'étaient pas considérées comme des aspects de celle-ci mais qui correspondaient à des pratiques importantes pour que les hommes réagissent correctement. Les paragraphes qui suivent traitent de ces pratiques considérées comme une composante essentielle de la culture de sûreté.

2. DÉFINITION ET NATURE DE LA CULTURE DE SÛRETÉ

6. La culture de sûreté est l'ensemble des caractéristiques et des attitudes qui, dans les organismes et chez les individus, font que les questions relatives à la sûreté des centrales nucléaires bénéficient, en priorité, de l'attention qu'elles méritent en raison de leur importance.

7. Dans l'INSAG-3, il est dit que la culture de sûreté désigne «l'engagement et le sens de la responsabilité personnelle de tous les individus se consacrant à toute activité qui a une incidence sur la sûreté des centrales nucléaires». Il y est dit en outre qu'un de ses éléments clefs est constitué par une «habitude générale de penser en termes de sûreté», qui implique «une attitude de remise en question systématique, un refus de se contenter des résultats acquis, un souci permanent de la perfection, et un effort de responsabilité personnelle et d'autodiscipline de groupe en matière de sûreté».

8. Des attributs tels que le dévouement individuel, le souci de la sûreté et une attitude de remise en question systématique ne sont pas mesurables. Or, il est important de pouvoir juger du niveau de culture de sûreté. Pour résoudre le problème, l'INSAG est parti de la constatation que ces attributs se traduisent naturellement par des manifestations perceptibles pouvant servir d'indicateurs de la culture de sûreté.

9. Les bonnes pratiques sont certes une composante essentielle de la culture de sûreté, mais elles ne suffisent pas en soi si elles sont appliquées de manière formelle. Il faut aller au-delà de leur application stricte, de façon que toutes les tâches importantes pour la sûreté soient exécutées correctement, avec diligence, de manière réfléchie, en toute connaissance

⁴⁸ GROUPE CONSULTATIF INTERNATIONAL POUR LA SURETE NUCLEAIRE, Rapport récapitulatif sur la réunion d'analyse de l'accident de Tchernobyl, Collection Sécurité n° 75-INSAG-1, AIEA, Vienne (1987).

⁴⁹ GROUPE CONSULTATIF INTERNATIONAL POUR LA SURETE NUCLEAIRE, Principes fondamentaux de sûreté pour les centrales nucléaires, Collection Sécurité n° 75-INSAG-3, AIEA, Vienne (1990).

de cause, sur la base d'un jugement sain et avec le sens des responsabilités requis.

10. Les paragraphes qui suivent indiquent donc les bonnes pratiques à encourager, commentent les attitudes individuelles qui sont nécessaires et déterminent les caractéristiques qui peuvent être considérées comme des mesures du niveau de culture de sûreté.

3. CARACTÉRISTIQUES UNIVERSELLES DE LA CULTURE DE SÛRETÉ

11. Dans tous les types d'activités et pour les organismes et les individus à tous les échelons, le souci de la sûreté fait intervenir de nombreux éléments:

- Conscience, chez les individus, de l'importance de la sûreté;

- Connaissances et compétence, conférées par la formation théorique et pratique et par l'auto-apprentissage du personnel;

- Engagement, lequel suppose la démonstration, au niveau de la direction, du degré élevé de priorité accordé à la sûreté, et l'adhésion des individus à l'objectif commun de sûreté;

- Motivation, par le biais du commandement, de l'établissement d'objectifs et de systèmes de récompenses et de sanctions, et grâce aux attitudes adoptées par les individus eux-mêmes;

- Supervision, comprenant des pratiques d'audit et d'examen, jointes à la volonté

de répondre aux attitudes interrogatives des individus;

- Responsabilité, grâce à l'attribution et à la description formelles des tâches

ainsi qu'à leur compréhension par les individus.

12. La culture de sûreté se manifeste dans deux grands domaines. Le premier est constitué par la structure mise en place au sein d'un organisme qui est du ressort de la hiérarchie. Le deuxième est constitué par l'attitude qu'adopte le personnel à tous les échelons pour réagir à cette structure et en tirer profit dans son travail.

13. Ces domaines sont examinés séparément sous les titres «Exigences imposées aux responsables de la politique» (section 3.1), «Exigences imposées aux

dirigeants» (section 3.2) et «Réaction des individus» (section 3.3). Comme la culture de sûreté est surtout une affaire de comportement individuel et que de nombreux individus ont des responsabilités en matière de sûreté, la section 3.3 revêt une importance toute particulière.

14. La figure 1 illustre les principales composantes de la culture de sûreté, et relie les titres du texte à ce schéma d'ensemble.

15. Conformément à ce qui est fait dans le document INSAG-3, il est supposé que

les pratiques dont il est question dans tout le rapport sont des pratiques courantes, en ce sens que les situations décrites sont celles que le rapport cherche à encourager.

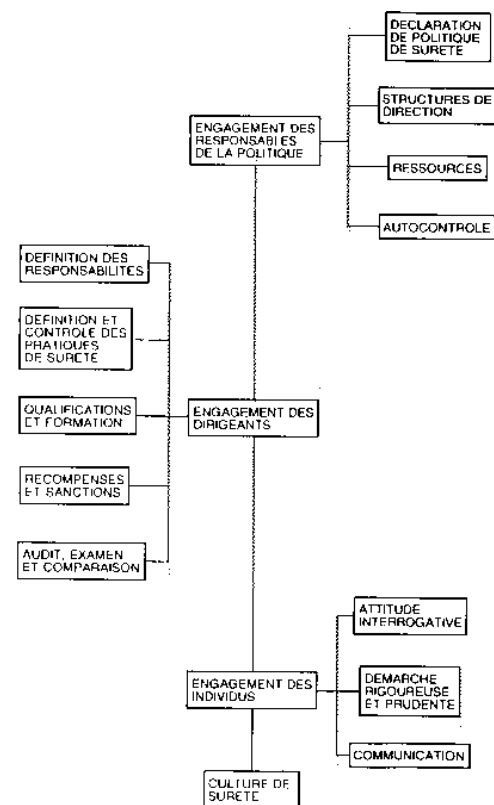


FIG. 1. Illustration de la présentation de la culture de sûreté.

3.1. EXIGENCES IMPOSEES AUX RESPONSABLES DE LA POLITIQUE

16. *Dans toute activité importante, la manière dont agissent les individus est conditionnée par des exigences imposées à un niveau supérieur. Le niveau le plus élevé où s'exerce une influence sur la sûreté des centrales nucléaires est le niveau législatif, où sont posés les fondements nationaux de la culture de sûreté.*

17. Les gouvernements exercent leurs responsabilités en matière de réglementation de la sûreté des centrales nucléaires et des autres installations et activités potentiellement dangereuses afin de protéger les individus, la population en général et l'environnement. Le législateur est secondé par les organes consultatifs et réglementaires nécessaires, qui disposent d'un personnel, de ressources financières et de pouvoirs suffisants pour s'acquitter de leurs tâches, ainsi que de la liberté de le faire sans ingérence indésirable. Cela favorise, dans un pays, l'instauration d'un climat où le souci de la sûreté peut être une préoccupation quotidienne. Les gouvernements encouragent également les échanges internationaux visant à améliorer la sûreté et s'efforcent de réduire le plus possible les obstacles commerciaux ou politiques qui pourraient entraver ces échanges.

18. *Des considérations similaires s'appliquent au sein des organismes. Les politiques préconisées à un niveau élevé façonnent l'environnement de travail et conditionnent le comportement des individus.*

19. Les politiques de sûreté et le détail de leur mise en oeuvre varient selon la nature des organismes et les activités de leur personnel, mais elles présentent d'importants traits communs. Les sections 3.1.1 à 3.1.5 montrent comment un tel engagement au niveau des responsables de la politique est exprimé et appuyé.

3.1.1. Déclaration de politique de sûreté

20. *Un organisme ayant des activités qui influent sur la sûreté des centrales nucléaires fait connaître et comprendre ses responsabilités dans une déclaration de politique de sûreté. Cette déclaration vise à donner des orientations au personnel, ainsi qu'à exposer les objectifs de l'organisme et à manifester publiquement l'engagement de sa direction à l'égard de la sûreté des centrales nucléaires.*

21. Les déclarations de politique de sûreté d'organismes dont les fonctions diffèrent varient dans leur forme et dans leur contenu. Un organisme exploitant est pleinement et formellement responsable de la sûreté de ses centrales nucléaires. Sa déclaration de politique de sûreté est claire et portée à la connaissance de tout le

personnel. Elle exprime son engagement de rechercher l'excellence dans toutes les activités importantes pour la sûreté des centrales nucléaires, en indiquant explicitement que celle-ci est une priorité absolue et prend le pas au besoin sur les impératifs de production ou les calendriers de réalisation des projets.

22. L'organisme réglementaire exerce une grande influence sur la sûreté des centrales nucléaires de son ressort, et lui-même et son personnel sont imprégnés d'une véritable culture de sûreté. Là encore, cette culture se fonde sur une déclaration de politique de sûreté. Dans cette déclaration, l'organisme s'engage à faire appliquer la législation et à agir de façon à favoriser la sûreté des centrales et la protection des individus, de la population en général et de l'environnement.

23. Les organismes de support, qui comprennent ceux qui sont chargés de la conception, de la fabrication, de la construction et de la recherche, influent beaucoup sur la sûreté des centrales nucléaires. Ils sont responsables avant tout de la qualité du résultat, qu'il s'agisse d'un modèle, d'un composant fabriqué, d'un équipement installé, d'un rapport de sûreté, de la mise au point d'un logiciel ou de toute autre production importante pour la sûreté. Dans ces organismes, les fondements de la culture de sûreté sont constitués par la directive définissant la politique et les pratiques à suivre pour assurer la qualité et atteindre ainsi les objectifs de sûreté du futur exploitant.

3.1.2. Structures de direction

24. *La mise en oeuvre de ces politiques de sûreté exige que les responsabilités en matière de sûreté soient clairement définies.*

25. La façon précise dont cela est réalisé dépend du rôle des organismes, mais il y a dans tous les cas une exigence fondamentale: des liaisons hiérarchiques fortes sont établies pour les questions influant sur la sûreté des centrales nucléaires, par des lignes de communication aussi directes que possible ne comportant que quelques interfaces à la mission bien définie.

26. La, responsabilité formelle de la sûreté des centrales incombe à l'organisme exploitant et, par délégation d'autorité, au chef de centrale. Dans les

organismes de support, l'exigence correspondante est de faire en sorte, grâce à la structure de direction et à la définition précise des tâches, que la responsabilité pour obtenir la qualité des résultats soit bien définie.

27. *Les grands organismes ayant un impact important sur la sûreté des centrales nucléaires chargent des services internes de gestion indépendants de surveiller les activités ayant trait à la sûreté nucléaire.*

28. Dans les organismes exploitants, ces services ont pour rôle d'examiner de près les pratiques de sûreté de la centrale. Ils rendent compte à un niveau élevé de la hiérarchie, ce qui permet d'intégrer les responsabilités en matière de sûreté dans la hiérarchie en leur donnant autant d'importance qu'aux autres fonctions principales. Les organismes de support adoptent des méthodes similaires comportant des pratiques d'audit et d'examen en vue d'assurer la qualité de leur résultat, ainsi que des dispositions permettant de rendre compte à un niveau élevé.

3.1.3. Ressources

29. *Des ressources adéquates sont consacrées à la sûreté.*

30. Il y a un personnel expérimenté suffisamment nombreux, complété si besoin est par des consultants ou des sous-traitants, de façon que les tâches liées à la sûreté des centrales nucléaires puissent être exécutées sans hâte ou pression excessive. Les politiques du personnel sont telles que les gens compétents peuvent être promus à des postes clés. La formation du personnel est considérée comme fondamentale et l'on y consacre les ressources nécessaires. Les moyens financiers sont suffisants pour que tout le personnel devant s'acquitter de tâches liées à la sûreté ait à sa disposition le matériel, les installations et l'infrastructure technique auxiliaire nécessaires. L'environnement de travail de ce personnel favorise la bonne exécution de ses tâches.

3.1.4. Autocontrôle

31. *Par principe, tous les organismes prennent des dispositions pour que soient examinées régulièrement celles de leurs pratiques qui contribuent à la sûreté des centrales nucléaires.*

32. Ces pratiques comprennent, par exemple, les nominations et la formation de personnel, le retour d'information sur l'expérience d'exploitation, et le

contrôle des modifications de la conception, des modifications de la centrale et des procédures d'exploitation. L'objectif est de solliciter des points de vue nouveaux et de susciter de nouvelles approches en faisant appel à des personnes ou à des organismes hautement qualifiés qui sont extérieurs à la structure hiérarchique normale. De tels arrangements sont encouragés en tant que moyen naturel et utile d'aider les exécutants, et ils évitent la recherche de culpabilités en cas de carences.

3.1.5. Engagement

33. *Les paragraphes 16 à 32 portent sur les activités qui définissent l'environnement de travail et qui exigent un engagement de l'organisme pour donner de bons résultats. Cet engagement est affirmé publiquement et est bien connu, il montre l'attitude de la direction à l'égard de ses responsabilités sociales, ainsi que la volonté d'ouverture de l'organisme en matière de sûreté.*

34. Sur le plan personnel, les responsables placés au sommet de la hiérarchie témoignent de leur engagement en veillant à ce que les processus qui influent sur la sûreté nucléaire soient examinés régulièrement, en s'intéressant directement aux questions de sûreté nucléaire ou de qualité des produits les plus importantes lorsqu'elles se posent, et en soulignant souvent l'importance de la sûreté et de la qualité dans leurs communications au personnel. En particulier, la sûreté des centrales nucléaires est un point important de l'ordre du jour lors des réunions du conseil d'administration des organismes exploitants.

3.2. EXIGENCES IMPOSEES AUX DIRIGEANTS

35. *Les attitudes des individus sont fortement influencées par leur environnement de travail. La clef d'une véritable culture de sûreté chez les individus réside dans les pratiques qui façonnent cet environnement et favorisent les attitudes contribuant à la sûreté. C'est aux dirigeants qu'il appartient d'instaurer de telles pratiques en conformité avec la politique et les objectifs de sûreté de leur organisme.*

36. Les exigences ainsi imposées aux dirigeants sont examinées dans les paragraphes qui suivent. Sauf indication contraire, les commentaires s'appliquent à tous les organismes ayant des activités qui influent sur la sûreté nucléaire.

3.2.1. Définition des responsabilités

37. *L'exercice des responsabilités individuelles est facilité par des lignes hiérarchiques uniques et bien définies.*

38. La responsabilité assignée aux individus est définie et documentée de façon suffisamment détaillée pour éviter toute ambiguïté. Les définitions collectives de l'autorité et de la responsabilité des individus sont examinées pour qu'il n'y ait pas d'omissions ou de chevauchements, ni de problèmes de responsabilités partagées. Les définitions des responsabilités sont approuvées à un niveau hiérarchique élevé.

Les dirigeants veillent à ce que les individus comprennent non seulement les responsabilités qui leur incombent, mais aussi celles de leurs collègues immédiats et du service dont ils dépendent, et la manière dont ces responsabilités complètent celles d'autres groupes. Cette exigence de rigueur dans la définition des responsabilités revêt une importance particulière dans le cas des organismes exploitants, car ce sont eux qui sont formellement responsables de la sûreté des centrales. Un accent particulier est mis sur la responsabilité déléguée au chef d'une centrale pour la sûreté de cette dernière.

39. Les organismes exploitants étant formellement responsables de la sûreté des centrales en service, ils sont en outre tenus de s'assurer eux-mêmes, en faisant au besoin appel à des tiers, que les autres organismes dont les activités contribuent à la base technique de la sûreté de la centrale s'acquittent de leurs responsabilités de façon satisfaisante.

3.2.2. Définition et contrôle des pratiques de sûreté

40. *Les dirigeants veillent à ce que les travaux en rapport avec la sûreté nucléaire soient exécutés de façon rigoureuse.*

41. C'est là une nécessité évidente dans les organismes exploitants, mais il faut accorder la même attention à la qualité des résultats dans les organismes de support. La base nécessaire est le plus souvent constituée par un ensemble hiérarchisé de documents à jour allant des directives générales aux procédures de travail détaillées. Ces procédures sont claires et non ambiguës et forment un ensemble complet. Les documents sont soumis à un examen critique, à une vérification et à un essai en bonne et due forme au titre des dispositions de l'organisme concernant l'assurance de la qualité, et des moyens formels sont adoptés pour leur contrôle.

42. Les dirigeants veillent à ce que les tâches soient exécutées telles qu'elles ont été définies. Ils instituent des systèmes de supervision et de contrôle et insistent sur l'ordre et la gestion interne.

3.2.3. Qualifications et formation

43. *Les dirigeants veillent à ce que leur personnel ait toutes les compétences requises pour s'acquitter de ses tâches.*

44. Les procédures de sélection et de nomination font en sorte que le personnel possède des qualifications initiales satisfaisantes pour ce qui est de son niveau intellectuel et de son niveau d'instruction. Les formations et les recyclages périodiques nécessaires sont assurés. L'évaluation de la compétence technique fait

partie intégrante des programmes de formation. Dans le cas des tâches critiques d'exploitation des centrales, l'appréciation des aptitudes fait intervenir des considérations physiques et psychologiques.

45. *La formation ne permet pas seulement d'acquérir des qualifications techniques ou de se familiariser avec le détail de procédures à suivre rigoureusement. Elle revêt un caractère plus large et, tout en satisfaisant à ces exigences fondamentales, elle est suffisante pour que les individus comprennent l'importance de leurs tâches et les conséquences d'erreurs imputables à des conceptions fausses ou à un manque de diligence.*

46. Faute de comprendre aussi cela, les individus pourraient ne pas accorder toute l'attention requise aux problèmes qui se posent ou agir de manière erronée parce qu'ils n'ont pas conscience des risques en cause.

3.2.4. Récompenses et sanctions

47. *En dernière analyse, c'est le comportement des individus, influencé par des motivations et des attitudes tant personnelles que collectives, qui fait qu'une pratique est satisfaisante. Les dirigeants encouragent et félicitent, et ils s'efforcent d'accorder des récompenses tangibles pour les attitudes particulièrement louables en matière de sûreté.*

48. Un point important à noter est que, dans les centrales en service, les systèmes de récompense n'encouragent pas des niveaux de production élevés si la sûreté s'en trouve compromise. Les incitations ne sont donc pas fondées uniquement sur le niveau de production, mais sont aussi liées à la performance en matière de sûreté.

49. Lorsque des erreurs sont commises, elles sont moins considérées comme un sujet de préoccupation que comme une source d'enseignements qui peut être profitable. Les individus sont encouragés à identifier, à signaler et à corriger les imperfections de leur propre travail afin d'aider les autres aussi bien qu'eux-mêmes à prévenir des problèmes futurs. Lorsque cela est nécessaire, une assistance leur est fournie pour qu'ils améliorent leur performance ultérieure.

50. Néanmoins, en cas de manquements répétés ou de négligence grave, les dirigeants assument leurs responsabilités en prenant des mesures disciplinaires, faute de quoi la sûreté risque d'être compromise. Il y a toutefois un équilibre délicat à trouver. Les sanctions ne sont pas appliquées d'une manière qui puisse inciter à dissimuler les erreurs.

3.2.5. Audit, examen et comparaison

51. *Les responsabilités des dirigeants incluent la mise en oeuvre d'un certain nombre de pratiques de surveillance qui vont au-delà de l'application de mesures d'assurance de la qualité et comportent, par exemple, des examens réguliers des programmes de formation, des procédures de nomination du personnel, des méthodes de travail, du contrôle des documents et des systèmes d'assurance de la qualité.*

52. Ces pratiques dépendent des activités des organismes considérés. Dans ceux qui sont chargés de la conception, de la fabrication et de l'exploitation, elles portent sur l'analyse des moyens par lesquels sont contrôlées les modifications de la conception ou de l'ingénierie. Dans le contexte de l'exploitation des centrales, elles incluent l'examen minutieux des changements apportés aux paramètres de fonctionnement, des prescriptions de maintenance, des modifications touchant la centrale, du contrôle de la configuration de la centrale, et de tout mode de fonctionnement inhabituel de la centrale.

53. Le fonctionnement des systèmes de gestion de la sûreté est donc vérifié par des processus internes. Une bonne pratique consiste à enrichir ces processus en faisant appel à des spécialistes s'occupant d'autres fonctions que celle qui est examinée ou extérieurs à l'organisme. Cela permet de disposer d'un large

éventail d'opinions et d'expériences, de favoriser l'émulation et d'encourager l'introduction de bonnes pratiques déjà adoptées ailleurs.

54. Les dirigeants font le nécessaire pour pouvoir tirer parti de toutes les sources d'informations concernant les expériences, les recherches, les innovations techniques, les données d'exploitation et les événements qui présentent de l'intérêt pour la sûreté, et qui font toutes l'objet d'une évaluation minutieuse dans leur propre contexte.

3.2.6. Engagement

55. Les dirigeants témoignent ainsi de leur engagement à l'égard de la culture de sûreté et l'encouragent chez les autres. Les pratiques identifiées structurent l'environnement dans lequel travaillent les individus. L'exigence d'un travail ordonné, la bonne compréhension des tâches à accomplir, les récompenses et, au besoin, les sanctions, ainsi que le recours à des spécialistes extérieurs pour les examens, favorisent l'instauration de l'état d'esprit qui permet aux membres du personnel, individuellement et collectivement, de s'acquitter de leurs tâches de façon satisfaisante.

56. *Il incombe aux dirigeants de faire en sorte que leur personnel réagisse à cet ensemble établi de pratiques et en tire profit, et qu'il soit incité constamment, par leur attitude et par leur exemple, à atteindre des niveaux élevés de performance individuelle dans l'accomplissement de ses tâches.*

3.3. REACTION DES INDIVIDUS

57. *Les sections 3.1 et 3.2 indiquent comment sont mis en place tous les éléments nécessaires pour que s'établisse une véritable culture de sûreté et insistent sur les responsabilités des dirigeants. Comme l'indique l'introduction de ces sections, il appartient au personnel à tous les échelons de réagir à ces éléments et d'en tirer profit.*

58. La question est de savoir comment. Pour bien montrer l'importance de cette question clef, une présentation différente a été adoptée pour les paragraphes qui suivent. Ils s'adressent principalement au personnel d'exploitation, car c'est lui qui a les responsabilités les plus directes, encore que les points abordés s'appliquent de diverses manières à toutes les personnes ayant des tâches importantes pour la sûreté nucléaire.

59. *La réaction de tous ceux qui recherchent l'excellence dans les questions influant sur la sûreté nucléaire se caractérise par:*

UNE ATTITUDE INTERROGATIVE

plus

UNE DÉMARCHE RIGOUREUSE ET

PRUDENTE

plus

LA COMMUNICATION

qui apporteront une contribution importante à:

LA SÛRETÉ

60. Avant qu'un individu entreprenne une tâche liée à la sûreté, son *attitude interrogative* l'amène à se poser des questions comme celles qui sont énumérées ci-après:

- Ai-je bien compris la tâche à accomplir?
- Quelles sont mes responsabilités?
- Quel rapport ont-elles avec la sûreté?
- Ai-je les connaissances nécessaires pour m'en acquitter?
- Quelles sont les responsabilités des autres?
- Y a-t-il des circonstances inhabituelles?
- Ai-je besoin d'aide?
- Qu'est-ce qui peut mal tourner?
- Quelles pourraient être les conséquences d'une défaillance ou d'une erreur?
- Que faudrait-il faire pour prévenir les défaillances?
- Que dois-je faire s'il y a une défaillance?

Dans le cas de tâches relativement courantes, pour lesquelles les individus ont reçu une formation complète, les questions et les réponses iront le plus souvent de soi. Les tâches ayant un contenu nouveau demanderont davantage de réflexion. Les tâches nouvelles et inhabituelles ayant un contenu de sûreté important feront l'objet de procédures écrites précisant ces points.

61. Les individus adoptent une *démarche rigoureuse et prudente*, consistant à:

- comprendre les procédures de travail;
- se conformer à ces procédures;
- être prêt à parer à toute éventualité;
- prendre le temps de réfléchir si un problème se pose;
- solliciter une aide si nécessaire;
- prêter attention à l'ordre, à la ponctualité et à la gestion interne;
- procéder avec un soin délibéré;
- s'abstenir de sauter des étapes.

62. Les individus reconnaissent que la *communication* est indispensable à la sûreté. Cela suppose:

- obtenir des autres des informations utiles;
- transmettre des informations aux autres;
- rendre compte des résultats des travaux, tant courants qu'inhabituels, et les documenter;
- proposer de nouvelles initiatives en matière de sûreté.

63. Une attitude interrogative, une démarche rigoureuse et prudente, et la communication nécessaire, tels sont les éléments d'une véritable culture de sûreté chez les individus. Le résultat contribue à un niveau élevé de sûreté et rend fier de s'acquitter de tâches importantes avec professionnalisme.

4. ÉLÉMENTS D'APPRÉCIATION

64. Le chapitre 3 traite de la culture de sûreté considérée comme l'ensemble des attributs louables de tout organisme ou individu contribuant à la sûreté des centrales nucléaires. Cet examen général doit être élargi de manière à couvrir les caractéristiques propres aux différents organismes. En outre, il faut donner des exemples:

- pour montrer que la culture de sûreté est un concept concret indispensable à la sûreté;
- pour offrir une base permettant de juger du niveau de culture de sûreté dans des cas précis;
- pour identifier des possibilités d'amélioration.

65. Le présent chapitre définit certaines caractéristiques générales d'une bonne culture de sûreté dans différentes catégories d'organismes: organismes gouvernementaux, organismes exploitants et organismes de support. Il vise à donner un aperçu, sous différents éclairages, des facteurs qui contribuent à la sûreté des centrales nucléaires. La liste n'est pas exhaustive et le lecteur pourra la compléter. Elle est destinée à servir de point de départ à l'auto-évaluation à laquelle les organismes doivent procéder.

66. L'appendice aborde le même problème, mais de façon différente. Il comprend plusieurs séries de questions qui peuvent aider à juger du niveau de culture de sûreté dans un cas précis.

4.1. GOUVERNEMENT ET ORGANISMES GOUVERNEMENTAUX

67. L'approche pratique adoptée par les gouvernements en ce qui concerne la sûreté en général et la sûreté nucléaire en particulier a un effet déterminant sur tous les organismes influant sur la sûreté nucléaire. L'engagement du gouvernement se manifeste de la façon suivante:

- La législation et les politiques gouvernementales concernant l'utilisation de l'énergie nucléaire fixent des objectifs généraux de sûreté, mettent en place les institutions nécessaires et assurent l'appui voulu pour que cette énergie soit exploitée en toute sécurité.

- Les gouvernements définissent clairement les responsabilités de ces institutions, font le nécessaire pour limiter le plus possible les conflits d'intérêts à propos de questions de sûreté importantes et veillent en particulier à ce que ces questions soient traitées selon leur importance, sans ingérence ou pression indésirable de la part d'organismes qui sont moins directement responsables de la sûreté nucléaire.
- Les gouvernements appuient vigoureusement les organismes réglementaires, en leur accordant notamment des pouvoirs adéquats, des ressources suffisantes pour toutes leurs activités et des garanties leur permettant de s'acquitter de leur tâche sans ingérence indésirable.
- Les gouvernements favorisent l'échange international d'informations relatives à la sûreté et y contribuent.

68. Les autorités réglementaires jouissent d'un pouvoir discrétionnaire considérable en matière de sûreté nucléaire. Ce pouvoir, qui leur est conféré par la législation et par des instruments plus détaillés régissant leurs activités, se manifeste de différentes façons générales:

- L'organisme réglementaire est géré de telle sorte que le souci commun de la sûreté l'amène à entretenir avec les organismes exploitants des rapports qui sont fondés sur la confiance et la coopération tout en conservant le caractère formel et indépendant qui convient pour des organismes aux responsabilités notoirement différentes.
- Les sujets controversés sont traités franchement. Une attitude ouverte est adoptée pour la fixation des objectifs de sûreté de façon que ceux qu'ils concernent aient la possibilité de donner leur avis à ce sujet. On adopte des normes qui prévoient des niveaux de sûreté appropriés tout en admettant l'existence d'un risque résiduel inévitable. Une approche cohérente et réaliste de la sûreté est ainsi assurée.
- Les autorités réglementaires reconnaissent que c'est à l'organisme exploitant et non pas à elles qu'incombe au premier chef la responsabilité d'assurer la sûreté. A cet effet, elles veillent à ce que les prescriptions réglementaires soient claires mais pas astreignantes au point d'imposer des contraintes excessives.
- Lorsqu'il s'agit de résoudre des problèmes nouveaux, une démarche généralement conservatrice peut être adoptée, mais on n'étouffe pas l'innovation en exigeant qu'il soit

fait appel exclusivement à des méthodes déjà employées dans le passé. Les améliorations apportées à la sûreté résultent d'un amalgame judicieux entre l'innovation et le recours à des techniques éprouvées.

69. Ceux qui réglementent les aspects économiques de l'énergie d'origine nucléaire tiennent compte du fait que les décisions fondées sur des considérations purement économiques pourraient être préjudiciables à la sûreté des réacteurs.

4.2. ORGANISMES EXPLOITANTS

4.2.1. Echelon des responsables de la politique

70. La culture de sûreté découle des mesures prises par la direction d'un organisme. Pour juger du niveau de culture de sûreté d'un organisme exploitant, il faut commencer par examiner la politique de l'organisme, car c'est à ce niveau que les attitudes, les décisions et les méthodes d'exploitation adoptées témoignent de la priorité accordée effectivement aux questions de sûreté.

71. Le premier élément qui permet d'apprécier l'engagement de l'organisme à l'égard de la culture de sûreté est le document énonçant sa politique et ses objectifs en matière de sûreté. Ce document est élaboré et diffusé de manière à ce que les objectifs soient compris et mis à profit par le personnel à tous les échelons. En particulier, il précise que la sûreté revêt une importance vitale, de sorte que les préoccupations de sûreté peuvent à l'occasion l'emporter sur les impératifs de la production.

72. La mise en place d'une structure de direction, la répartition des responsabilités en son sein et l'allocation de ressources incombent en premier lieu aux responsables de la politique. Ces dispositions sont compatibles avec les objectifs de sûreté de l'organisme.

73. La direction entreprend périodiquement des examens de la performance de l'organisme en matière de sûreté. Ces examens et la suite donnée à leurs conclusions fournissent des indications importantes sur le niveau de culture de sûreté de l'organisme. Ainsi, on examine par exemple:

- La formation, pour s'assurer qu'elle est satisfaisante et que les ressources qui y sont consacrées sont adéquates.

- Les systèmes de documentation, pour s'assurer que les ressources qui y sont allouées sont suffisantes.
- Les procédures de nomination du personnel, pour s'assurer en particulier que l'évaluation des attitudes des individus à l'égard de la sûreté fait partie intégrante du processus de sélection et de promotion.

4.2.2. Echelon de la centrale

74. A la centrale elle-même, la sûreté est un sujet de préoccupation immédiat, et l'existence d'une bonne culture de sûreté joue un rôle essentiel dans le travail quotidien. Trois aspects différents sont à considérer:

- l'environnement créé par la direction de la centrale, qui détermine les attitudes des individus;
- les attitudes des individus, dans tous les services et à tous les échelons, depuis le chef de centrale jusqu'au bas de la hiérarchie;
- l'expérience effective de la centrale en matière de sûreté, qui témoigne de la priorité accordée effectivement à la sûreté dans la centrale.

4.2.2.1. L'environnement de travail

75. Les responsabilités et des pratiques détaillées sont définies à tous les niveaux de la centrale. Certaines activités, comme les essais ou les modifications de la centrale ayant des incidences sur la sûreté, sont l'objet d'un soin particulier. Dans ces cas-là, un examen systématique et indépendant s'impose. Il est procédé à des examens de la documentation et des relevés pour s'assurer qu'il a été satisfait aux

prescriptions de sûreté.

76. La formation théorique et pratique garantit que tous les membres du personnel savent quelles sont les erreurs qui peuvent être commises dans leur domaine d'activité. Elle se fonde sur une compréhension élémentaire des questions de sûreté enjeu, inclut un examen des conséquences possibles de ces erreurs et traite plus particulièrement des moyens de les éviter ou, le cas échéant, de les corriger.

C'est ainsi que:

- Pour le recyclage sur simulateur des opérateurs de la salle de commande, il est tenu compte de l'expérience d'exploitation, des difficultés rencontrées par le personnel et des questions qu'il a soulevées.

- Des séances de formation à l'aide de maquettes ou de vidéobandes sont organisées avant l'exécution de travaux de maintenance complexes, pour rafraîchir les connaissances du personnel et illustrer les erreurs possibles.
- Les résultats des analyses de sûreté, notamment des analyses probabilistes, sont consultés régulièrement pour étayer les décisions à prendre lorsque des problèmes particuliers se posent et pour donner au personnel un aperçu des principales caractéristiques de la conception et de l'exploitation de la centrale du point de vue de la sûreté.

77. A la centrale, la sûreté nucléaire est maintenue à l'examen en permanence grâce à des inspections et à des audits, à des visites de hauts responsables, à des discussions internes et à l'organisation sur place de séminaires consacrés à des questions de sûreté. Les conclusions sont évaluées et il leur est donné suite en temps opportun.

78. Pour que le personnel puisse s'acquitter aisément de sa tâche, il faut lui en donner les moyens. Les éléments à prendre en considération sont notamment les suivants: aménagement des lieux de travail, caractère adapté des commandes, des instruments, de l'outillage et du matériel, accès aux informations nécessaires, gestion interne et - ce qui est particulièrement important - charge de travail des individus.

79. Les relations qu'entretient la direction de la centrale avec l'autorité réglementaire et ses représentants sur place sont empreintes de confiance et fondées sur le souci commun de la sûreté nucléaire, mais elles supposent une acceptation réciproque des responsabilités de chacun.

4.2.2.2. Attitudes individuelles

80. Les attitudes des individus peuvent être examinées à l'occasion d'échanges avec les membres du personnel à différents échelons pour étayer le jugement relatif au niveau de culture de sûreté et pour dégager des enseignements. Voici quelques exemples des éléments généraux à tester au moyen de questions plus circonstanciées:

- Les procédures sont-elles appliquées strictement, même s'il existe des méthodes plus rapides?
- Les membres du personnel prennent-ils le temps de réfléchir lorsqu'ils sont
- confrontés à une situation imprévue?

- Une bonne attitude à l'égard de la sûreté est-elle respectée par la direction et
- par les collègues?
- Les membres du personnel proposent-ils, de leur propre initiative, des améliorations en matière de sûreté?

81. Les échanges portant sur des questions de sûreté nucléaire mettent en évidence les attitudes des dirigeants et influent sur celles du personnel. En particulier, les dirigeants saisissent les occasions qui se présentent de montrer qu'ils sont prêts à faire passer, au besoin, les exigences de sûreté avant les impératifs de production. En s'entretenant par exemple avec les personnes concernées des retards intervenus dans le redémarrage de la centrale pour des raisons de sûreté, ils font ressortir que l'engagement à l'égard de la sûreté est un objectif primordial.

82. Leur présence sur les lieux de travail leur donne l'occasion de souligner directement l'importance qui s'attache à la sûreté.

83. La mise au point de pratiques locales pour renforcer la sûreté offre un excellent moyen d'apprécier les attitudes des individus et la réaction de la direction, car elle montre que tous les membres du personnel comprennent la nécessité de tirer parti de leur expérience pour améliorer la performance. A titre d'exemple, on peut faire porter ces efforts sur la gestion interne et la qualité des relevés ou alors développer la pratique qui consiste à signaler les erreurs afin de prendre en compte celles qui n'ont apparemment pas de conséquences importantes.

4.2.2.3. Expérience de la centrale en matière de sûreté

84. A long terme, la performance de la centrale en matière de sûreté est le reflet de son niveau de culture de sûreté. Les indicateurs de performance d'une centrale communément admis (disponibilité de la centrale, nombre d'arrêts non programmés ou radioexposition) donnent une mesure de l'attention portée à la sûreté. Ils sont complétés par des indicateurs de sûreté spécifiques comme le nombre et la gravité des événements importants, le nombre d'ordres de travaux en souffrance et la durée de toute indisponibilité des systèmes de sûreté. L'importance de ces indicateurs est expliquée au personnel.

85. Tous les événements importants qui se sont produits sur le site sont analysés en étroite collaboration avec les personnes concernées afin

d'aider tous les membres du personnel à évaluer leurs points forts et leurs points faibles.

86. Ces données d'expérience sont examinées périodiquement pour vérifier que des leçons en ont été tirées et que les mesures correctives nécessaires ont été identifiées et mises en œuvre en temps opportun. L'exhaustivité des examens et la vigueur des mesures correctives constituent des indicateurs importants de la culture de sûreté.

4.3. ORGANISMES DE SUPPORT

87. Les principales dispositions prises en matière de gestion et les attitudes individuelles qui caractérisent une bonne culture de la sûreté dans un organisme exploitant peuvent être adaptées à tous les organismes de support en mettant en particulier l'accent sur la qualité des résultats. Certains problèmes particuliers aux organismes de recherche et de conception sont identifiés ci-après.

88. Les organismes de recherche disposent de mécanismes leur permettant de suivre les travaux menés dans le monde entier qui pourraient influencer sur les conclusions de l'analyse de sûreté. Ce suivi est renforcé par des mécanismes permettant de porter en temps voulu les informations recueillies à l'attention de ceux qui sont responsables de la sûreté, et avec une insistance en rapport avec leur importance.

89. Ceux qui participent aux recherches veillent à ce que leurs travaux ne donnent lieu à aucune interprétation erronée ou utilisation abusive.

90. Les organismes de conception peuvent, au besoin, faire appel à des spécialistes extérieurs pour renforcer leurs propres moyens. Ainsi:

- Lorsqu'un organisme de conception ne connaît pas assez bien une technologie nouvelle, par exemple l'élaboration de logiciels, il peut solliciter le concours de spécialistes pour renforcer ses compétences internes.
- Les examens de conception, qui sont une composante importante et habituelle des procédures internes, peuvent être complétés avec le concours de spécialistes extérieurs.

91. Les organismes de conception suivent de près l'évolution de la technologie de la sûreté des réacteurs et des techniques d'analyse de la sûreté en participant activement à des activités nationales et internationales. Il existe des mécanismes formels permettant d'appeler l'attention des responsables de l'exploitation sur toute

information nouvelle susceptible de modifier ou d'invalider les analyses de sûreté antérieures.

5. OBSERVATIONS FINALES

92. L'expression «culture de sûreté» est désormais employée couramment. Cependant, il est nécessaire de s'entendre sur la nature de la culture de sûreté et de trouver les moyens de transformer ce qui n'était jusqu'ici qu'une expression commode en un concept qui soit utile dans la pratique.

93. Le présent rapport a cherché à remédier à la situation. La première partie expose les vues de l'INSAG concernant la nature de la culture de sûreté. Elle a pour objet de fournir des éclaircissements et d'aboutir à une interprétation commune. La dernière partie du rapport et l'appendice tentent de donner une valeur pratique au concept de culture de sûreté en identifiant les caractéristiques qui peuvent servir à juger du niveau de culture de sûreté dans un cas concret.

94. L'INSAG présente cette description de la culture de sûreté et des moyens de la mettre en pratique pour s'assurer que «les questions relatives à la sûreté des centrales nucléaires bénéficient, en priorité, de l'attention qu'elles méritent en raison de leur importance».

Appendice

INDICATEURS DE LA CULTURE DE SÛRETÉ

Le présent appendice propose une liste de questions qu'il convient de se poser lorsque l'on évalue le niveau de culture de sûreté dans des cas concrets. Il est entendu que cette liste ne peut être exhaustive et qu'aucune liste, aussi longue soit-elle, ne peut s'appliquer à toutes les situations. C'est pourquoi on a voulu, dans ce qui suit, encourager les organismes et les individus à s'interroger eux-mêmes, au lieu de leur fournir une liste de contrôle appelant des réponses du type oui/non. Il s'agit plus d'inciter à la réflexion que de formuler des prescriptions. Le lecteur aura donc tout loisir de compléter cette liste.

A1. GOUVERNEMENT ET ORGANISMES GOUVERNEMENTAUX

Engagement du gouvernement à l'égard de la sûreté

- 1) Les textes législatifs sont-ils satisfaisants?
 - 2) La modification nécessaire des règlements se heurte-t-elle à des difficultés excessives?
 - 3) La législation et les déclarations de politique gouvernementale insistent-elles sur le fait que la sûreté est une condition préalable à l'utilisation du nucléaire?
 - 4) Les budgets des organismes réglementaires ont-ils suivi l'inflation, le rythme de développement de l'industrie et l'accroissement des exigences qui lui sont imposées? Ces organismes disposent-ils de ressources suffisantes pour engager du personnel possédant les compétences voulues?
 - 5) Le gouvernement finance-t-il de façon adéquate les recherches nécessaires sur la sûreté? Les résultats des recherches sont-ils communiqués à d'autres pays?
 - 6) Dans quelle mesure peut-on échanger librement des informations sur la sûreté avec d'autres pays?
 - 7) Le pays appuie-t-il le Système de notification des incidents de l'AIEA, les programmes relatifs aux équipes d'examen de la sûreté d'exploitation (OSART) et aux équipes d'analyse des événements importants pour la sûreté (ASSET) de l'AIEA et d'autres activités internationales pertinentes?
 - 8) Y a-t-il des exemples d'ingérence dans des domaines techniques présentant de l'importance pour la sûreté?
- 1) Les objectifs de sûreté des organismes réglementaires sont-ils énoncés clairement et judicieusement, de façon à n'être ni trop généraux, ni trop normatifs ?
Permettent-ils de maintenir un bon équilibre entre l'innovation et l'application de techniques éprouvées?
 - 2) Des organismes compétents sont-ils consultés au sujet des prescriptions réglementaires ? A-t-on assez souvent tenu compte de leurs observations dans le passé pour qu'ils soient incités à continuer d'en faire à l'avenir?
 - 3) Y a-t-il un processus prévisible et logique pour aborder les problèmes qui demandent la prise en compte simultanée des facteurs de sûreté et des facteurs économiques?
 - 4) Quels ont été les retards dans l'exécution de projets ou les pertes de production
imputables au manque de clarté des prescriptions réglementaires ou au fait que des décisions dans ce domaine n'ont pas été prises à temps?
 - 5) D'une manière générale, les pratiques réglementaires sont-elles conformes aux objectifs du programme de normes de sûreté nucléaire (NUSS) de l'AIEA?
 - 6) Existe-t-il un programme de formation théorique et pratique à l'intention du personnel de l'organisme réglementaire?
 - 7) L'organisme réglementaire participe-t-il activement à des activités internationales pertinentes?
 - 8) Publie-t-il régulièrement des rapports sur les problèmes de sûreté importants?
 - 9) Publie-t-il périodiquement un rapport de synthèse sur les performances des centrales en matière de sûreté?
 - 10) Quelle est la nature des relations avec les titulaires d'autorisation? Y a-t-il un bon équilibre entre le formalisme et les relations professionnelles directes?
 - 11) Y a-t-il entre le personnel de l'organisme réglementaire et celui de l'organisme exploitant un respect mutuel fondé sur le même niveau de compétences? Quelle est la proportion d'experts techniques de l'organisme réglementaire ayant une expérience pratique de l'exploitation ou de la conception?
 - 12) Y a-t-il régulièrement des échanges de vues concernant l'expérience et les problèmes des

Performance des organismes réglementaires

titulaires d'autorisation, ainsi que l'influence des activités réglementaires sur ces problèmes?

- 13) Dans quelle mesure l'organisme réglementaire compte-t-il sur les processus de sûreté internes de l'organisme exploitant?
- 14) Quelles sont les modalités et l'importance de la présence de représentants des autorités réglementaires dans la centrale?

A2. ORGANISME EXPLOITANT

Politique de sûreté à l'échelon de l'organisme

- 1) Une déclaration de politique de sûreté a-t-elle été publiée? Est-elle claire? La politique exprime-t-elle l'importance fondamentale de la sûreté nucléaire?
- 2) Est-elle rappelée à l'attention du personnel de temps à autre?
- 3) Est-elle conforme au concept de culture de sûreté développé dans le présent rapport?
- 4) Le personnel, à tous les échelons, connaît-il bien la politique de sûreté et peut-il donner des exemples illustrant sa signification?

Pratiques de sûreté à l'échelon de l'organisme

- 1) Le conseil d'administration de l'organisme est-il compétent pour ce qui est de la sûreté des centrales nucléaires?
- 2) La sûreté est-elle à l'ordre du jour des réunions officielles tenues à cet échelon?
- 3) Le personnel d'exploitation est-il représenté à ces réunions pour discuter de la performance des centrales en matière de sûreté?
- 4) Existe-t-il un comité d'examen de la sûreté nucléaire actif qui présente ses conclusions à l'échelon de l'organisme?
- 5) Y a-t-il un haut responsable chargé principalement de la sûreté nucléaire? Comment est-il appuyé et secondé dans ses fonctions? Où se situe-t-il dans la hiérarchie par rapport aux responsables d'autres fonctions?
- 6) Y a-t-il un examen périodique des ressources nécessaires pour la sûreté? Quels en sont les résultats?

Définition des responsabilités

- 1) L'attribution des responsabilités en matière de sûreté a-t-elle été clairement énoncée?
- 2) La responsabilité du chef de centrale en matière de sûreté nucléaire a-t-elle été clairement énoncée et acceptée?
- 3) Les documents définissant les responsabilités en matière de sûreté sont-ils tenus à jour et revus périodiquement? Quel en est le résultat?

Formation

- 1) Les formations et les recyclages les plus importants aboutissent-ils tous à une évaluation formelle et à une reconnaissance des aptitudes? Quel est le taux de succès/d'échecs? Quelle proportion de son temps le personnel d'exploitation consacre-t-il à la formation? Comment l'organisme se situe-t-il à cet égard par rapport aux autres exploitants de centrales nucléaires?
- 2) Quel est le montant des ressources allouées à la formation? Comment l'organisme se situe-t-il à cet égard par rapport aux autres exploitants de centrales nucléaires?
- 3) La qualité des programmes de formation est-elle évaluée aux niveaux de l'organisme exploitant et de la direction de la centrale?
- 4) Y a-t-il un examen périodique de l'adéquation, de l'exactitude et des résultats des cours de formation? Cet examen tient-il compte du retour d'information sur l'expérience d'exploitation?
- 5) Laisse-t-on souvent les impératifs de production bouleverser le calendrier des cours de formation?
- 6) Le personnel comprend-il l'importance des limites d'exploitation de la centrale dans son domaine de responsabilité?
- 7) Est-il informé des conséquences pour la sûreté du mauvais fonctionnement des éléments de la centrale?
- 8) Apprend-on au personnel l'importance particulière que revêt le respect des procédures? Le lui rappelle-t-on régulièrement? Lui explique-t-on les principes fondamentaux de sûreté sur lesquels reposent ces procédures?
- 9) Le personnel chargé de la formation peut-il citer des exemples d'erreurs d'exploitation qui ont conduit à modifier un programme de formation?
- 10) Les séances de recyclage sur simulateurs destinées aux opérateurs de la salle de commande tiennent-elles compte des difficultés

rencontrées par le personnel et des questions qu'il a soulevées?

- 11) Les séances de formation destinées au personnel de maintenance font-elles appel à des maquettes et à des vidéobandes avant l'exécution de travaux d'entretien complexes?
- 12) Modifie-t-on le simulateur d'entraînement dès qu'une modification est apportée à la centrale?
- 13) Les programmes de formation traitent-ils de la culture de sûreté?

Sélection des dirigeants

- 1) Le personnel a-t-il conscience que l'attitude à l'égard de la sûreté est importante lors de la sélection et de la promotion des dirigeants? Comment favorise-t-on cette prise de conscience?
- 2) Les rapports annuels d'appréciation du comportement professionnel contiennent-ils une rubrique spéciale sur l'attitude du personnel à l'égard de la sûreté?
- 3) Est-il arrivé que l'attitude d'un dirigeant à l'égard de la sûreté ait joué un rôle important dans l'approbation ou le refus de sa promotion?

Examen de la performance en matière de sûreté

- 1) Des analyses de la performance de la centrale en matière de sûreté sont-elles communiquées régulièrement à la direction? Comportent-elles des comparaisons avec la performance d'autres centrales nucléaires?
- 2) Est-il donné suite sans tarder aux conclusions de ces examens? Les dirigeants sont-ils informés en retour de la mise en pratique des enseignements dégagés? Peuvent-ils discerner les changements consécutifs à ces examens?
- 3) Les dirigeants savent-ils comment se situe leur centrale sur le plan de la sûreté par rapport aux autres centrales de la société? Du pays? Du monde?
- 4) Le personnel lit-il régulièrement et comprend-il les rapports sur l'expérience d'exploitation?
- 5) Existe-t-il un système d'indicateurs de performance en matière de sûreté comportant un programme visant à améliorer cette performance?
- 6) Le personnel comprend-il les indicateurs de performance en matière de sûreté?
- 7) Les dirigeants sont-ils au courant de l'évolution des indicateurs de performance en matière de sûreté et des causes de cette évolution?

- 8) Quelles dispositions sont prévues pour la notification des événements importants pour la sûreté survenant dans une centrale? Existe-t-il des procédures officielles pour évaluer ces événements et en tirer des enseignements?
- 9) Y a-t-il un mécanisme officiel de consultation du personnel ayant été impliqué dans un événement important au sujet du contenu final du rapport?
- 10) Existe-t-il un groupe permanent d'examen de la sûreté rendant compte directement au chef de centrale?
- 11) Y a-t-il des liens efficaces en matière d'information sur la sûreté avec les exploitants de centrales similaires?
- 12) L'organisme apporte-t-il une contribution effective au système international de notification des incidents?
- 13) Quelles sont les tendances en ce qui concerne le nombre de problèmes en suspens, les modifications temporaires et les manuels d'exploitation à réviser?

Mise en valeur de la sûreté

- 1) Le chef de centrale tient-il avec le personnel de direction des réunions périodiques consacrées exclusivement à la sûreté?
- 2) Le personnel ne faisant pas partie de la direction a-t-il l'occasion de participer à des réunions consacrées à la sûreté?
- 3) Ces réunions portent-elles sur des événements importants pour la sûreté qui sont survenus dans la centrale? Dans d'autres centrales de la société? Du pays? Du monde?
- 4) A-t-on envisagé de faire appel à une mission OSART ou à une forme similaire d'examen externe?
- 5) Y a-t-il une procédure permettant au personnel de rang inférieur de faire part directement au chef de centrale de ses préoccupations en matière de sûreté? Cette procédure est-elle connue?
- 6) Y a-t-il un système de notification des erreurs humaines? Comment est-il porté à la connaissance du personnel?
- 7) Les systèmes de récompenses tiennent-ils compte des facteurs liés à la performance en matière de sûreté?

Charge de travail

- 1) Y a-t-il une politique claire de limitation des heures supplémentaires? A quelle catégorie de personnel s'applique-t-elle?
- 2) Comment les heures supplémentaires sont-elles contrôlées, surveillées et signalées au chef de centrale et à la direction?
- 3) Quelle proportion de son temps le chef de quart consacre-t-il à des tâches administratives?

Relations entre les dirigeants de la centrale et les autorités réglementaires

- 1) Les relations sont-elles franches et ouvertes, tout en restant suffisamment formelles?
- 2) Comment est organisé l'accès des représentants de l'organisme réglementaire à la documentation? Aux installations? Au personnel d'exploitation?
- 3) Les rapports destinés à l'organisme réglementaire sont-ils établis en temps voulu?
- 4) A quels niveaux se situent les contacts des inspecteurs de l'organisme réglementaire dans la centrale?
- 5) Le chef de centrale rencontre-t-il régulièrement le personnel de l'organisme réglementaire?

Attitudes des dirigeants

- 1) Lorsqu'il y a apparemment conflit entre la sûreté et les coûts ou entre la sûreté et l'exploitation, les dirigeants examinent-ils avec le personnel la façon de le régler?
- 2) Le calendrier et la liste des travaux à effectuer lors des arrêts annuels font-ils l'objet d'un processus interne d'examen de la sûreté?
- 3) Quand des considérations de sûreté retardent le démarrage d'une centrale, les dirigeants en profitent-ils pour démontrer le caractère prioritaire de la sûreté?
- 4) Dans les périodes où il y a beaucoup de travail, les dirigeants veillent-ils à ce que l'on rappelle au personnel qu'il est contre-indiqué de se hâter excessivement et de sauter des étapes?
- 5) Expliquent-ils leur engagement à l'égard de la culture de sûreté au personnel? Celui-ci est-il régulièrement informé des objectifs, dépenses, réalisations et insuffisances dans ce domaine? Quelles mesures sont prises concrètement pour contribuer à l'engagement des dirigeants, par exemple l'établissement de codes de conduite?

- 6) Y a-t-il souvent eu des directives visant à l'amélioration de la sûreté?
- 7) Les dirigeants font-ils part au personnel des enseignements tirés de leur expérience dans la centrale et dans des centrales similaires? Est-ce un thème de formation?
- 8) Existe-t-il un système permettant au personnel de faire part à la direction de ses préoccupations en matière de sûreté et de proposer des améliorations? Les dirigeants encouragent-ils son utilisation? Y réagissent-ils favorablement? Les membres du personnel qui ont recours à ce mécanisme sont-ils récompensés et leurs mérites sont-ils reconnus publiquement?
- 9) Quelle est l'attitude des dirigeants à l'égard des examens et des audits de sûreté portant sur leurs activités? Examinent-ils les résultats avec leur personnel et discutent-ils avec lui des moyens de remédier aux insuffisances?
- 10) Comment les dirigeants réagissent-ils à l'application de mesures d'assurance de la qualité à leurs activités?
- 11) Examinent-ils régulièrement le comportement professionnel du personnel et notamment son attitude à l'égard de la sûreté?
- 12) Reconnaittent-ils publiquement les mérites des membres du personnel qui prennent des initiatives favorisant la sûreté?
- 13) Comment réagissent-ils à la transgression des règles de sûreté et aux violations des spécifications techniques liées à la sûreté?
- 14) Par quels mécanismes le personnel dirigeant est-il informé des réalisations et des insuffisances en matière de sûreté? Ces mécanismes sont-ils efficaces?
- 15) Les dirigeants sont-ils conscients de la nécessité de connaître les insuffisances de leur personnel, de préciser les besoins de formation ou d'offrir tout autre appui?
- 16) Participent-ils aux cours de formation où l'on expose au personnel les politiques et les procédures suivies en matière de sûreté? Fournissent-ils une partie du matériel de formation? S'intéressent-ils de près à la formation de leur personnel et connaissent-ils son niveau de formation et ses aptitudes? Encouragent-ils les individus compétents à devenir instructeurs? Suivent-ils eux-mêmes des cours de recyclage sur la sûreté?
- 17) Les dirigeants revoient-ils régulièrement la répartition des tâches confiées à leur personnel? Les documents pertinents sont-ils à jour?
- 18) Les dirigeants se rendent-ils régulièrement sur les lieux de travail pour examiner les activités liées à la sûreté?

- 19) Prêtent-ils attention aux conditions matérielles de travail de leur personnel?

Attitudes des individus

- 1) Les membres du personnel sont-ils conscients de l'engagement des dirigeants à l'égard de la culture de sûreté?
- 2) Peuvent-ils indiquer comment la sûreté risquerait d'être compromise par des erreurs qui leur seraient imputables? Ou par celles d'autres personnes travaillant dans des domaines connexes?
- 3) Peuvent-ils énoncer clairement leurs propres responsabilités? Peuvent-ils citer les documents qui les définissent?
- 4) Le personnel d'exploitation et de maintenance peut-il citer des cas récents de transgression des limites d'exploitation de la centrale, décrire ce qui s'est passé et indiquer ce qui a été fait pour qu'ils ne se reproduisent pas?
- 5) Les instructions sont-elles suivies rigoureusement même quand il existe des méthodes plus rapides?
- 6) Le personnel vérifie-t-il soigneusement que les relevés, journaux de bord et autres documents sont complets et précis?
- 7) Que ferait le personnel s'il assistait à des actions risquant de réduire les marges de sûreté?
- 8) Comment réagissent les individus aux erreurs qu'ils commettent et qui sont susceptibles de compromettre la sûreté?
- 9) Que ferait un opérateur ou un agent de maintenance si, en suivant une procédure écrite, une instruction lui paraissait erronée?
- 10) Que ferait un instructeur si, dans une procédure, une instruction lui paraissait erronée?
- 11) Le personnel utilise-t-il les mécanismes qui lui permettent de signaler des insuffisances en matière de sûreté et de suggérer des améliorations? Ces mécanismes sont-ils utilisés pour signaler les erreurs des individus? Sont-ils utilisés même quand aucun effet préjudiciable n'est apparent?
- 12) Le personnel réagit-il de manière satisfaisante à l'étude des problèmes de sûreté en aidant efficacement à la recherche des causes et en introduisant des améliorations?
- 13) Les membres du personnel considèrent-ils d'un =il favorable ceux de leurs collègues dont la bonne attitude à l'égard de la sûreté se traduit notamment par l'attention qu'ils portent à la gestion interne, au caractère complet des entrées dans les journaux de bord et au respect des procédures?

- 14) Le personnel de la salle de commande fait-il preuve à tout moment d'une attitude vigilante et attentive?
- 15) Le personnel connaît-il le système de récompenses et de sanctions lié aux questions de sûreté?
- 16) Tire-t-il pleinement parti des possibilités de formation? Adopte-t-il une démarche responsable, effectue-t-il les travaux préparatoires nécessaires et participe-t-il activement aux discussions?
- 17) Prend-il le temps de réfléchir quand il est confronté à une situation imprévue? Ses actions sont-elles alors «inspirées par la sûreté»?
- 18) Quelle est l'attitude du personnel à l'égard des examens et des audits de sûreté touchant son domaine de travail? Comment réagit-il aux améliorations qui en découlent?
- 19) Le personnel participe-t-il à des examens collégiaux des activités de sûreté visant à lutter contre les erreurs humaines?
- 20) Communique-t-il efficacement son expérience à d'autres personnes et groupes? Y a-t-il des exemples?

Pratiques locales

- 1) Le chef de centrale a-t-il institué des initiatives liées à la sûreté qui vont au-delà des prescriptions fixées à l'échelon de la société?
- 2) De quel mécanisme le personnel dispose-t-il pour signaler les erreurs, même quand celles-ci ont été immédiatement corrigées ou n'ont eu aucun effet décelable? Y recourt-il à l'occasion?
- 3) Les relevés sur la performance ou la maintenance des composants et des systèmes sont-ils facilement accessibles? Complètes? Compréhensibles? Exactes? A jour?
- 4) Quel est l'état général de la centrale - aspect général, propreté, fuites de vapeur et d'huile, bonne tenue des journaux de bord et des relevés?
- 5) Quelles dispositions sont prévues pour la supervision, l'examen et l'approbation des travaux de maintenance effectués par des organismes de support?

Supervision sur le terrain par le personnel dirigeant

- 1) Comment travaillent les principaux responsables de quart? Cherchent-ils à se renseigner? Sont-ils bien informés? Se rendent-ils régulièrement dans les zones où sont effectués des travaux liés à la sûreté? Sont-ils intéressés par les problèmes ou uniquement par les délais?
- 2) Les cadres moyens vont-ils souvent superviser eux-mêmes l'exécution des travaux liés à la sûreté dont ils sont responsables?
- 3) Le chef de centrale va-t-il superviser de temps à autre l'exécution de travaux liés à la sûreté?
- 4) Les hauts responsables visitent-ils régulièrement la centrale? Prêtent-ils attention aux questions de sûreté?

A3. ORGANISMES DE RECHERCHE

Contribution de la recherche aux analyses de sûreté

- 1) Les chercheurs comprennent-ils bien comment les résultats de leurs travaux seront utilisés dans les analyses de sûreté? Savent-ils comment on procède à l'interpolation et à l'extrapolation de leurs données pour des domaines de variation des paramètres différents de ceux qu'ils utilisent dans leurs expériences?
- 2) Déterminent-ils les insuffisances et les limites de leurs résultats?
- 3) Suivent-ils de près les analyses de sûreté pour pouvoir se rendre compte de toute utilisation erronée de leurs travaux? Signalent-ils les risques d'utilisation abusive ou d'interprétation erronée?
- 4) Sait-on clairement quel groupe ou quelle personne est chargé de se tenir au courant des travaux les plus récents ou des nouvelles données internationales se rapportant à un sujet particulier? Quels contacts personnels les chercheurs ont-ils établis pour se tenir informés des nouvelles données?
- 5) Existe-t-il un mécanisme permettant d'attirer l'attention des responsables sur des données nouvelles susceptibles d'invalider les analyses de sûreté antérieures? Y a-t-il une voie de recours si le premier niveau de notification reste sans effet? Ces mécanismes sont-ils souvent utilisés?
- 6) Y a-t-il un moyen de s'assurer que les recherches visant à résoudre les problèmes de sûreté relatifs à la conception et à l'exploitation sont effectuées en temps voulu?

- 7) Au bout de combien de temps les résultats des recherches sont-ils intégrés dans le processus de conception et de réglementation?
- 8) Existe-t-il une politique de publication régulière des résultats des recherches dans des périodiques exigeant que les articles soient contrôlés par des pairs?

A4. ORGANISMES CHARGES DE LA CONCEPTION

Codes pour les aspects de la conception relatifs à la sûreté

- 1) Y a-t-il des processus de vérification et de validation des codes de modélisation sur ordinateur? Les chercheurs compétents y participent-ils?
- 2) Les codes utilisés pour les aspects de la conception relatifs à la sûreté sont-ils vérifiés et validés pour des cas concrets?
- 3) Les limites des codes sont-elles explicitement prises en compte lors du processus d'examen de la conception?
- 4) A l'exécution de quels problèmes standards internationaux les analystes ont-ils participé pour tester des codes nationaux de modélisation sur ordinateur? Quels efforts ont été déployés sur un plan bilatéral ou multilatéral pour comparer les travaux avec ceux d'experts d'un autre pays?
- 5) Lorsque l'on considère que les résultats antérieurs fournis par un modèle informatique ne sont peut-être plus valables, par quel mécanisme officiel le signale-t-on? A-t-il déjà été nécessaire d'utiliser ce mécanisme?

Processus d'examen de la conception

- 1) Dans quels domaines a-t-on fait appel à des spécialistes extérieurs pour compléter l'équipe de l'organisme? Comment a-t-on déterminé la compétence de ces spécialistes?
- 2) Où sont décrites les fonctions et les responsabilités des équipes d'examen de la conception?
- 3) Le processus d'examen de la conception a-t-il fait l'objet d'un contrôle par des vérificateurs intérieurs de l'assurance de la qualité? Par l'organisme réglementaire? Par un groupe d'experts nationaux ou internationaux?

**MEMBRES DU GROUPE CONSULTATIF INTERNATIONAL
POUR LA SURETE NUCLEAIRE**

Beninson, D.

Birkhofer, A.

Chatterjee, S.K.

Domaratzki, Z.

Edmondson, B.

Gonzalez-Gomez, E.

Höhn, J.

Kouts, H.J.C. (*Président*)

Lepecki, W.

Li, Deping

Sato, K.

Sidorenko, V.A.

Tanguy, P.

Vuorinen, A.P.

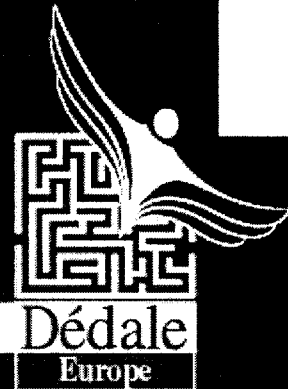
Note: A.M. Bukrinski a remplacé M. Sidorenko.

ANNEXE 2

Activité de la PME Dédale dans le domaine de la culture de sûreté

<http://www.dedale-sa.com>

Products



Products

Training
Incidents & Accidents
Organizational
Critical Incident Stress Management Programs

Projects

Instructor Guide (Aviation)
Incident Reporting System
Cabin Evacuation Study

Problems / Solutions



History & Myth • Our Philosophy
Dedale Team • Products • Customers
Contact Us • Jobs

I. PRODUCTS

I.1. TRAINING

I.1.1, TRAINING OPTIONS

WE PROVIDE THE TRAINING THAT THE CLIENT PREFERS. TRAINING OPTIONS CAN VARY FROM OFF-THE-SHELF DEDALE-PREPARED GENERIC COURSEWARE, TO HIGHLY CUSTOMISED TRAINING. WE BELIEVE THAT INVOLVING THE END-USER IS A MAJOR PREREQUISITE FOR SUCCESS IN ANY TRAINING ENDEAVOUR. THE FOLLOWING STEPS, UNDERTAKEN IN A RECENT PROJECT, HIGHLIGHT DEDALE'S PREFERRED METHOD FOR CULTURALLY CUSTOMISED TRAINING:

- *A field analysis was conducted to gain a preliminary understanding of the domain, the work practices, and characteristics of the site culture.*
- *During the course development and production phase, a working group made up of field agents (including team managers) and Dedale staff analyzed and iteratively designed a training course through a series of seminars.*
- *Modules, exercises, role plays, case studies and on-site videos were produced and refined during one year.*
- *Some of the development group members were given "Train the Trainer" training by Dedale, and then delivered the training to their peers.*

In sum, because the course was designed, developed, and delivered by field agents under the general guidance and support of Dedale, the end-result was more culturally relevant and more quickly accepted by line personnel.

I.1.2. DOMAIN

I.1.2.1. AVIATION

I.1.2.1.1 BRIEFINGS `

"BRIEFINGS" is an intensive yet comprehensive Human Factors training package, including a 200-page reference manual accompanied by an instructor guide, 11 aviation-specific videos and PowerPoint presentation slides sufficient for a five day course. It has been adopted by the French Civil Aviation Authority, the Australian Bureau of Air Safety Investigation (BASI), and is acknowledged as a human factors training resource by the International Civil Aviation Organization (ICAO). It meets the JAR-FCL Human Performance and Limitations requirements for training ab-initio pilots, and is recommended training for all pilots who have no previous exposure to human factors. Topics include physiology, limits of human

performance, human error, motivation, stress, decision-making, communication, teamwork, personality, situation awareness, fatigue, and automation. This course is available in French, English and Spanish.

I.1.2.1.2. CREW RESOURCE MANAGEMENT

PILOTS

- *Dedale developed its first CRM course for pilots in 1993; Brent Hayward has been involved in the development and delivery of CRM training since 1990.*
- *Since then, we have developed courses for large and small airlines around the world.*
- *We've also developed courses for helicopter pilots.*
- *Our courses meet FAA and JAR-OPS mandatory requirements.*
- *Courses range from one to three day's duration*
- *Course topics include error management, automation, situation awareness, communication, decision-making, and procedures and practices*
- *We can customize the course in conjunction with company personnel*
- *We train the airline's instructors to use the material*
- *We also offer joint training with other company person I (e.g., cabin crew)*

CABIN CREW

- *We developed our first CRM course for cabin crew in 1996. Our courses meet FAA and JAR-OPS mandated requirements for, flight attendant training.*
- *Courses range from half a day to two day's duration.*
- *Course topics include error management, physical and psychological factors affecting performance, communication and co operation, and team performance*
- *We can customize the course in conjunction with company personnel*
- *We train the airline's instructors to use the material*
- *We also offer joint training with other company personnel (e.g., flights crew)*

MAINTENANCE

- *We developed our first Human Factors training course for maintenance personnel in 1996.*
- *Courses range from one to two day's duration.*

Course topics include flight safety statistics and maintenance, error management, factors affecting performance, Communication, Procedures and Practices in the maintenance environment, and factors affecting team performance
- *Courses meet JAR 66 requirements*
- *We can customize the course in conjunction with company personnel*
- *We train the airline's instructors to use the material*
- *We also offer joint training with other company personnel (e.g., flight crew)*

I.1. 2.1.3. AIR TRAFFIC MIANAGEMENT

- *Dedale developed the prototype "Team Resource Management" course for Eurocontrol, on the basis of the specifications of the EATCHIP TRM Task Force, in 1997.*
- *The training, developed in consultation with a group of controllers and experts, illustrates Human Factors concepts in the ATC environment.*
- *The TRM prototype course includes slides, videos, case studies, and role plays, and is currently being customized by each National CAA.*
- *Dedale also adapted the prototype for use by the French CAA. In conjunction with the French Air Traffic Management Research Center, this project was collaboratively developed with a group of ATCOs from different Control Centers throughout France.*

I.1.2.2.MARITIME

- *We developed our first "Bridge Resource Management" course for mariners in 1994.*
- *The course was developed in conjunction with the Danish Maritime Institute (DMI).*
- *There are no mandatory requirements for this type of training as yet. but we believe Human Factors is just as important at sea as in the air.*
- *The cours is three day's duration, but can be shortened.*
- *Course topics include human performance and limitations, decision making, stress, human error and reliability, communication, team performance, new technology on the bridge*
- *On request, we can also develop a "crisis and crowd panic management" course to meet Resolution 5 of the STCW Conference, 1995*

1.1.2.3. NUCLEAR INDUSTRY

- *EDF, the French Electricity and Power Authority, contracted Dedale to adapt CRM to the nuclear domain, for control operators and field workers working in long-lasting teams doing shift-work.*

The training focuses on everyday work and communication practices within the team, between teams (shift hand-over), and with other personnel.

- *Subjects include implicit communication, telecommunication practices, interruption management, work preparation, co-ordination and reporting, situation awareness, representation errors, error management, incident reporting and safety culture, time pressure management, use of procedures and written documents, team culture, and shift hand-over.*

1.2. INCIDENTS & ACCIDENTS

1.2.1. INCIDENT REPORTING SYSTEMS

Accidents are only the "tip of the safety iceberg" - many incidents, some more serious than others, occur on a regular basis. In an effort to understand these incidents and their organization's safety level more deeply, many companies around the world are now installing and maintaining confidential incident reporting systems. The BASIS system used by British Airways is just one example.

Dedale has been involved in two large scale projects in this area, one with Airbus Industrie and the French Civil Aviation Authority, the second with a major airline's Maintenance Department. We helped develop and/or implement the Incident Reporting Systems - the forms, the appropriate analytic tools and manageable data bases.

We can help you develop and implement a similar customized system of confidential reporting, analysis, investigation and remediation in your own safety-critical organization.

1.2.2. TRAINING IN ANALYSIS

To say an incident was caused by human error is almost a tautology - worse, it tells us, little about how the situation can be improved (short of removing the human from all aspects of design and operation).

Both Jean Paries and Brent Hayward have been active accident and incident investigators. Combining their academic and held experiences, Dedale offers education and training in "how to understand an incident". Participants learn how to extract the most organizational benefit from an incident by considering the underlying latent failures which predisposed the organization to a safety breach, as well as the immediate failure which precipitated the incident. Organizational, environmental, and regulatory

influences are explored, from the immediate present extending back into the company's history.

Dedale can provide training for operational personnel in incident and accident investigation techniques.

Brent Hayward has been involved in the development and delivery of Incident Investigation training courses for Air Traffic Controllers, flight crew and maintenance personnel in Australia and Singapore.

Incident Investigation training courses can be tailored to fit a variety of organisational and industry needs.

I.3. ORGANIZATIONAL

I.3.1. SAFETY CULTURE AUDITS

Safety is not a dichotomy - a company is not safe one day, and unsafe the next. So how safe is your company? Do you know its vulnerabilities, its weaknesses? How committed are people to increasing the level of safety in your company, are they encouraged in this area, and can it be done without sacrificing other organizational goals?

Using a systems approach, Dedale can evaluate the strengths and potential weaknesses of your company with regards the procedures, practices, leadership, communication and feedback, training and checking, organizational philosophy about error and correction, and interdepartmental conflicts. We offer diagnosis (using research, surveys, interviews, and/or observation), recommendations and actions (education, training, confidential reporting systems, and team building projects).

I.3.2. ORGANIZATIONAL SURVEYS

The psychologists in Dedale have a strong empirical and statistical background. Based on extensive experience in the design and development of workplace questionnaires, including the Flight Management Attitudes Questionnaire used by many airlines, we can design a questionnaire to assess employee satisfaction, attitudes and/or values about various aspects of your organization, e.g., management practices, safety procedures, training, current working conditions.

The results of these surveys, once analyzed and presented in a coherent summary, can

- help an organization diagnose its strengths and weaknesses*
- form the basis of an informed intervention such as new procedures or training*
- act as a baseline measure against which the success of future interventions can be measured (a pre-post design)*
- be used as a follow-up measure to track changes and the culture of the organization across time.*

1.4. CRITICAL INCIDENT STRESS MANAGEMENT PROGRAMS

Dedale can design and deliver Critical Incident Stress Management (CISM) Awareness and CISM Peer Support training programs for operational personnel and management. These programs are designed to ensure that organisations and their personnel are equipped to deal effectively with the trauma that can result from involvement in operational occurrences. CISM trauma that can result from involvement in operational occurrences. CISM Awareness training acts as a "stress and trauma inoculation" program for operational personnel, and aims to increase their awareness of issues related to the experience and management of traumatic events in the work place. The CISM Peer Support training program addresses the range of trauma management issues which Peer Support team members may be expected to encounter in their work environment.

II. PROJECTS

II.1. INSTRUCTOR GUIDE (AVIATION)

Improving instructors' or examiners' skills and knowledge is now required to meet the practical consequences of recent regulatory requirements (JAR-FCL and JAR-OPS). This project designed a written guide for instructors to help them track and assess the Human Factors skills of student-pilots. The following steps were considered:

- a list of key concepts was drawn from the BRIEFINGS courseware,*
- didactic principles were drawn from the literature*
- instructors were interviewed in the field*
- key concepts were associated with typical behaviors affecting flight safety.*
- a method for capturing and interpreting behavioral cues in training situations was developed.*
- the guide was designed to incorporate HF knowledge into a practical, operational tool.*

II.2. INCIDENT REPORTING SYSTEM

II.2.1. PILOTS

Working with Airbus Industrie, Dedale is developing an incident reporting and analysis system for the French Civil Aviation Authority. This system is premised on the following principles:

- *risk assessment and risk control strategies should be interpreted in a multi-layer structure which differentiates front-line operators, airlines, manufacturers, and civil aviation authorities*
- *the database should be more than just a bank of data, it should help decision-makers at the different levels of the system organize their responses*
- *the system should allow feedback which supports short-term and long-term adaptation*
- *there should be provision for more than one point of view in the reporting of an incident*

it should allow analysis in a way that promotes understanding of the precursors of a safety-threat.

II.2.2. MAINTENANCE

A major airline contracted Dedale to conduct a Human Factors audit of its Maintenance area. One outcome of the audit was the decision to implement a new incident reporting system, MEDA, the "Maintenance Error Decision Aid" method developed by Boeing.

Dedale's task was to identify the conditions needed to successfully implement MEDA in the airline, taking into account the various incident reporting and information systems already in use, as well as the company's structure and organizational culture.

It was decided that the system would be managed by a "Human Factors Correspondent" at the hangar level. These correspondents work in a network fed by the production teams, piloted by the initial working group, and managed by the security-safety manager. Future work includes more training for the HFC's, informing personnel about MEDA, and installing a new disciplinary policy (a 'no blame' philosophy).

II.3. CABIN EVACUATION STUDY

The introduction of very large aircraft such as the Airbus A3XX has alerted regulators to the need to study the effectiveness of cabin evacuations more closely. The French Civil Aviation Authority is sponsoring Dedale to conduct a research project, the aim of which is twofold: to perform a critical analysis of the current situation with regards the regulations, current training and practice, and to suggest relevant courses of improvement. Following a broad investigation of current activities, specific recommendations will be proposed within the following areas :

- *To increase flight attendants' awareness of evacuations (the reality of such an event and the physical and psychological phenomena they are likely to experience);*
- *To revise training syllabi to support such awareness (stress management, crowd control in a panic situation, the use of appropriate gestures and commands)*
- *To give greater consideration to training across the career-span of cabin attendants*

- *To improve evacuation simulations; and*
- *To improve the monitoring of training and activities on the line.*

III. - PROBLEMS/SOLUTIONS

The personnel of Dedale and Dedale Asia Pacific have extensive experience in the development and delivery of a broad range of safety management aids - diagnostic tools, education and training programs, and materials. With the goal of minimizing and managing human error in safety-critical industries, our work is relevant in all transport domains- road, rail, shipping and air - as well as nuclear, medical, off-shore, chemical and other industrial processes involving risk.

Depending on your needs, we can provide:

- *Crew Resource Management - initial and advanced training for Cockpit and cabin crew, maintenance, ramp, etc..)*
- *The "Briefings"© pilot training course in Human Factors*
- *Air safety investigation human factors aspects.*
- *Organizational safety audits*
- *Culturally customized training*
- *Design of documentation and procedures - human factors aspects*
- *Development and production of quality safety training*
- *Team Resource Management training for air traffic controllers*
- *Bridge Ressource Management programs*
- *Critical Incident Stress Management programs*
- *Development and implementation of safety reporting protocols*
- *Human factors awareness training for managers*
- *Safety education and training*
- *Situation awareness management training*

Dedale Asia Pacificis also able to provide consulting service int

- *selection of personnel, for safety critical operational roles*
- *Selection of key personnel for aviation management roles*
- *Psychological assessment and counselling for operational personnel*

ANNEXE 3

LE PROJET SCORE

<http://www.dcs.qmul.ac.uk/research/radar/Projects/SCORE/>

A Background

The majority of critical failures, such as the well-known incidents described in the Appendix, have been traced back to cultural issues relating to risk. At present there is no means to identify how organisational culture affects the risk of critical failures in an organisation. The objective of the SCORE programme of research is to investigate how culture affects risk. We will determine whether a *risk accounting system* can be produced to monitor an organisation's risk exposure over time by taking account of changes to their risk culture.

Although organisations *do* often learn from past incidents, degradation of the risk culture may lead to unnecessary risk exposure. The key research hypothesis is that it is possible to monitor such changes and provide quantified assessment of risk and its financial impact along with recommended remedial actions. The project will use a Bayesian approach to model both objective and subjective factors, and attitude survey techniques to inform the subjective measurements in the model. Following Reason's terminology it is possible to look at organisational accidents in terms of what are called active failures and latent conditions [Reason 1997]. Active failures are caused by unsafe acts performed by people committing errors or violations in the course of their duties. An example of an active failure would be a train driver passing a signal at red. Current thinking is that many active failures, caused by people operating within complex systems, are not necessarily the result of human fallibility alone but are supported by organisational features such as poor procedures, poor training, ineffective safety procedures, poor maintenance of equipment etc. These features are termed latent conditions and are present in all systems to a greater or less extent. When organisations identify major risks they should create defences aimed at averting the occurrence of the underlying hazard or at least reduce its severity should it occur. However, the effectiveness of these defences may be eroded over time making incidents more likely as a result of human error (slips, mistakes).

Based on this model the underlying problems exemplified in a number of well-known critical failures (e.g. The Piper Alpha accident [Cullen 1990] and more recently the Concorde accident) are that independent QA or audit processes fail to identify latent conditions, risk management responsibilities are unclear and there is no way of determining whether the overall risk exposure of an organisation is diminishing or increasing. There is also a further complicating factor in that managing risk requires a vigilant attitude towards dealing with non-events. Major accidents, whether they are safety related or business related, tend to be rare and thus preventing their occurrence requires dynamic behaviour (risk management activities) to create stable outcomes . the continuation of non-events. It is when the behaviour patterns change, for example when risk monitoring becomes slack, that latent conditions arise. This makes an accident more likely. However, where effective risk management is operated there is little feedback beyond the failure of the hazard to manifest itself to re-enforce the continued operation of the procedures. Maintaining focus in this environment requires a constant awareness of the likelihood of risks manifesting themselves and thus, it is contended, risk accounting will help maintain this focus.

The challenges faced by risk managers in industry and commerce may be summarised as follows:

- Lack of risk accounting system causes, at the extreme, critical and business failures. Organisations do not yet know how to effectively monitor risks and report them at Board level.
- Top-down regulation pressures increase demands on organisations of all types to monitor their risk exposure. New regulations (such as [Turnbull 1999]) will push plcs and financial institutions to provide audited assessments of organisational risks. Organisations do not yet know how to do this.
- There is no accepted way of quantifying risk in financial terms, and so, for example, banks may have to allocate inordinately large amounts for capital allocation to cover operational risks.
- Drastic organisational change, such as privatisation, impacts risk. At present organisations do not know how to manage risk in a distributed complex system with many stakeholders.

Figure 1 in the Appendix shows the relationship between the risk effects identified by Reason, in terms of active failures combining with latent conditions and breached defences to cause catastrophic accidents or bankruptcy, and the primary and secondary causes of these risk effects.

The primary and secondary causes identified in Figure 1 are well known. However organisations do not closely monitor them as a matter of routine for the following reasons (identified as root causes in Figure 1):

- quantifying the effects of secondary causes on risk effects is “hard” and cannot be done using conventional statistical methods;
- data collected has been sparse and data collection is non-trivial in complex organisations;
- the lack of common approaches that can be shared by organisations has led to a situation where risk measurement is at its worst in those areas where risks are often greatest . at the interfaces between organisations and departments;
- cultural values with respect to risk are prone to drift and change as large organisations change their focus, goals and role in the economy;
- lack of systems to monitor vigilance - there is no standard means of capturing risk/attitude culture;
- lack of financial measure of risk means that, risk exposure is not taken sufficiently seriously at Board level.

This project will tackle the root causes, and hence intends to reduce the likelihood of primary enabling conditions meaning that organisations will be less likely to suffer critical failures and more profitable as a result. It should also help improve their ability to collect, quantify and monitor the “soft” secondary causes of risk. We do not intend to research into industry specific latent conditions and their possible interaction to form accident trajectories. Rather, focus will be on the emergence of latent “unsafe” conditions, by modelling the contribution of “soft” factors like culture and attitudes and quantifying the changing level of risk these imply. The project aims to investigate the possibility of producing a single organisation-wide measure of operational risk that reflects the scale and complexity of the operating procedures in a way that also provides a meaningful indicator to the Board and other stakeholders.

B Research programme and methodology

The key research hypothesis is that it is possible to monitor changes in an organisation’s risk culture and provide a quantified assessment of the impact of such changes on risk, and its accompanying financial impact, along with recommended remedial actions.

The objective is to investigate whether a *risk accounting system* – the SCORE method and tool – can be developed to enable organisations to quantify risk in such a way as to provide an “account” of operating risks. This approach, which is analogous to the way a financial account is made publicly available to outside scrutiny and analysis, is the one advocated by the Turnbull guidelines [Turnbull 1999]. SCORE will be based on the techniques of BBNs [Lauritzen and Spiegelhalter, 1988], which are widely believed to be the best method for modelling and quantifying uncertainty where there are both objective and subjective factors. SCORE will predict and monitor operational risk using data collected from various forms of risk instrumentation, such as risk attitude and behaviour questionnaires, safety case evaluations, audit results and incident logs. Specifically, the project will

- Apply past research results in dependability argumentation using BBNs and decision analysis techniques (influence diagrams, utility theory, MCDA) to monitor and predict operational risk;
- Identify the cultural changes that may lead to a loss of vigilance, latent conditions and operational failures and develop measures of these changes that can be included within belief networks;
- Determine the strengths of relationships between the various primary and secondary causes of incidents in order to aid quantification and develop a generic approach;
- Design a model for combining diverse operational risks into one single “accounting” measure of the safety or financial impact such risks have on the organisation and society at large;
- Develop and test the means to instrument an organisation for the purpose of collecting data on risks, their identification, reduction or mitigation and the cultural and technical forces affecting the effectiveness of risk management processes.
- Test the research hypothesis (and provide feedback for improvement) by making available during the project a pre-commercial prototype of SCORE for use by the industrial partners (who will have initiated

internal projects to act as a testbed). This will also enable us to achieve awareness and special benefits of these new measurement techniques within mainstream risk analysis circles.

Seven main tasks have been identified that will achieve the project objectives (dissemination is covered in Section D). These tasks, their inputs, outputs and where appropriate the lead partner for that task are described below.

Task 1 — Developing risk accounting method and BBN models (SCORE approach) - lead partner RADAR

The methods and principles for quantitative analysis of risks, often called probabilistic risk analysis (PRA) are well known and widely accepted throughout industry, especially in the area of safety critical systems. It has been argued that this approach seems well suited to the problem of measuring risk in *any* context. However, it is by no means obvious that it can be meaningfully applied to *whole* organisations. RADAR's work on using BBNs for safety cases and dependability arguments has improved the PRA approach by helping measure the influence of subjective, often ambiguous and diverse information, on risk. A BBN is a directed graph where the nodes represent uncertain variables and the arcs represent causal or influential relationships between variables. Associated with each node is a probability table that represents the probabilities of the various node values conditional on the values of its parent nodes. Building a good BBN model involves two difficult steps:

1. Building the 'topology', that is, defining the “right” set of variables and arcs;
2. Defining the node probability tables (NPTs);

Task 1 will focus on the first of these steps. RADAR will develop “template” BBN models that can be tailored to any risk scenario that an organisation may face. The general idea is that defences against specific hazards will be identified. Then latent conditions likely to compromise these defences will be modelled in such a way that where evidence arises of the emergence of these conditions the risk associated with the hazards can be calculated and propagated into the broader risk model.

The key outputs from this task (which together with the outputs of tasks 2 and 3 will be called the SCORE method) will be a method and executable BBN models. The industrial collaborators will review the early models and comment on their validity and practicality as well as examine how their own approach to risk could be improved in line with research advances made.

Task 2 — Establishing empirical relations between risk culture and risk effects - lead partner SRU

The aim of this task is to help complete step 2 of the BBN model building described in Task 1 - to provide a framework for weighting and linking risk culture and risk effects *within* the BBN. The SRU was one of the first academic groups to establish the link between safety/risk culture and attitudes and other indicators of safety performance. Relationships have been established between culture and occupational accidents (eg. Donald, 1994; Donald and Canter, 1994) as well as other quantified risk assessment (QRA) measures (Hurst, Young, Donald, Gibson and Muyselaar, 1996). This research has shown that safety/risk culture measures improve risk prediction beyond that available from models assuming generic failure rates rather than incorporating specific culture indices.

Previous research establishing these links has, however, been limited, primarily by two main factors. The first of these is that development of measures and establishing of relationships has been industry specific, and in particular limited to major hazard sites in the process industries. The second limitation is that the studies have tended to generate relatively small data sets, compromising the statistical power and generalisability of the results. The two limitations of previous research will be addressed during the current project. This will initially be achieved using data previously collected by the SRU. The Safety Attitude, Behaviour, Culture (Safety-ABC) database currently held by the SRU includes data collected in over one hundred organizations and industrial sites. Using the database allows more powerful statistical procedures to be used. Structural Equation Modelling and Bayesian learning will be exploited to establish the causal links between risk performance and components of risk culture.

The resulting empirical relations will be compared and validated against the experience of the industrial collaborators.

Task 3 — Designing instrumentation for risk data collection - lead partner SRU

While Tasks 1 and 2 will provide complete BBN models for quantifying risk, these BBN models depend on users being able to enter sensible observations for variables. The aim of this task is to provide a means of

collecting data for the factors (especially the subjective ones) to be entered as observations. To date risk culture instruments have not been produced for inclusion in BBNs. Consequently, within the framework of existing models, the new or modified instrumentation will be developed to achieve this goal. WeThe project will draw directly on the expertise and the models and instruments previously developed by the SRU in industrial contexts. To allow exploitation of the Safety-ABC database and instrumentation compatibility, the designed risk culture measures will follow as closely as possible those previously developed by the SRU.

The risk culture instrumentation will measure a number of organizational facets of risk. Previous research has established these using Multidimensional Scaling (MDS) procedures (e.g. Donald and Canter, 1994). However, recent work has shown that a hierarchical three level factor model of risk appears more appropriate for use with BBNs than those previously established.

It is a project aim that organizations will be able to use the instrumentation and results to identify areas for culture change initiatives. The lower levels of the model will provide sufficient detail for organizations to monitor and develop actions to address particular culture issues. The instrumentation will therefore provide both an assessment and management diagnostics tool. Previous research by the SRU has shown the feasibility of successfully using culture measures in this way (Donald, 1995; Donald and Young, 1996).

Developing the instrument will follow three stages:

1. Examine existing measures and assess their suitability as a generic risk culture assessment tool and their appropriateness for use with BBNs.
2. Pilot the modified or new instrumentation within the collaborating organizations to ensure its generic relevance within different contexts.
3. A full application of the instrumentation to establish measures of reliability and validity. Data collected at this stage will also be used as input to the BBNs.

It is a project aim that tools will be produced that will allow organizations to monitor risk culture on a regular basis. As risk culture changes relatively slowly, it should be sufficient for organizations to monitor on a frequent basis; however this contention will be reviewed with the industrial partners and revised if necessary. To support the monitoring process, the risk culture measures will be available in two forms. The standard form will be a paper-based or web based measure that can be used for data collection. This is currently the norm for using such tools. For the second form of the instrumentation software will be developed within the context of the SCORE tool (Task 4). SRU will lead this task and will carry out the data collection for these stages of the project.

Task 4 — Developing prototype tool for risk prediction and monitoring - lead partner RADAR

The aim is to build a prototype SCORE tool to support application of the method as described by tasks 1-3. The tool will contain the BBN templates identified in Task 1 and the probability tables derived from Task 2. These will form tailorable components to model an organisation's particular risk set. In this way knowledge will be reused and the model constructed to fit the problem at hand. The tool will provide a software version of the risk instrumentation measures developed in Task 3 to help organizations use the risk culture measures (this part will be developed by SRU). The software will allow editing of the measures to ensure that organisation specific terminology is appropriate. It will also allow the data collected by the organization to be input and results, in the form of culture risk diagnostic profiles, using BBNs to be generated. The long-term aim is to allow online data collection and analysis by organisations. In this way organizations can monitor risk culture and its change over time. A dedicated Internet domain for this purpose has been agreed with associates of the project group.

The tool will have a high quality GUI and accompanying help files to ensure that it can effectively support the industrial collaborators in the validation task. The project will consult the industrial collaborators and identify the elements of BBN theory needed to support the modelling task to define the requirements for the tool. Critical to the success of the project will be the ability to summarise the key elements of the risk accounts made in a concise form. The project will build the tool in such a way that it can reveal the full model or cogently report critical and sensitive areas to high-level management, without the need to dig deeply into the models.

The outputs of this task will be a series of incremental prototypes of the tool and a requirements specification document. The industrial collaborators will provide feedback on these.

Task 5 — Trialing the approach in practice - coordinator RADAR

We intend to hold a number of workshops with the collaborating organisations to involve them throughout the life-cycle of SCORE. This will help ensure that we meet the requirements of users and incorporate their expert input into the method as it evolves. As a result this will increase the likelihood of the collaborators using the method and tool. This will determine whether the approach to risk accounting is likely to work and, just as importantly, to identify the barriers to exploitation within organisations. The validity and practicality of the research will be tested against current practice *and* current practice will be challenged to improve (this idea is called *reciprocal validation*).

The outputs of this task will be a candid validation report describing the failures and successes of SCORE, the barriers to its implementation and prescriptions on how these were or might be overcome.

Task 6 — Integration of method, tool and instrumentation - lead partner RADAR

The SCORE method and tool requires an integration stage where all elements of the system to be delivered come together and any faults and inconsistencies are removed. This task will therefore reduce the risk of the partners producing research ideas containing inconsistent nomenclatures, models and assumptions.

The outputs of this task will be the final version of the pre-commercial tool and the final report. This final report will provide a synopsis of the results from all of the other tasks and will be available for dissemination of the project results.

Task 7 — Management

Dr Martin Neil and Dr Ian Donald will jointly be responsible for overall management (including responsibility for interfacing to the industrial collaborators and EPSRC). One of the senior researchers at each site will be responsible for day-to-day management of the project. A project Technical Board involving one senior representative from each collaborator will be formed. This Board will meet every three months and decisions and actions will be recorded in a set of minutes.

The schedule assumptions and Gantt Chart for the SCORE schedule is contained in the Appendix.

C Relevance to Beneficiaries

All the industrial partners have expressed an interest in the following project objectives:

- The production of explicit risk assessment decision frameworks combining uncertain evidence which can then be systematically and consistently used by trained assessors.
- The ability to model corporate level risk management systems and instrument the model with evidence derived from human and organizational factors often described as “safety culture” or “risk culture”
- The ability to use tools produced within the project to track risk exposure over time and to determine whether exposure is rising or falling and why this is happening; where risk is moving adversely the method will give clear indications of why this is happening and what must be done to reverse the situation.
- The ability to associate financial costs with risk elements and to produce an itemized financial risk exposure account alongside the model thus associating overall risk exposure with the costs associated with that exposure.

The proponents of this project use the term “risk auditing” to describe the results that will arise from this project and all of the partners are concerned with risk auditing.

References

DATUM: Dependability Assessment Through the Unification of Measurable evidence, funded by EPSRC under the Safety Critical Systems Research Programme, 1992-1996 with collaborators: Lloyd's Register of Shipping, Royal Holloway College, and Centre for Human Computer Interaction and Design (City University).

- Donald, I. & Canter, D.. Employee Attitudes and Safety in the Chemical Industry. *Journal of Loss Prevention in the Process Industries*, 7, 203-208, 1994.
- Donald, I. Measuring Psychological Factors in Safety. *Safety and Health Practitioner*, March, 26-29, 1994.
- Donald, I. Psychological Insights into Managerial Responsibility for Public and Employee Safety. In R. Bull and D. Carson (Eds.) *Handbook of Psychology in Legal Contexts*. Chichester: Wiley. (pp 625-642.), 1995.
- Donald, I., & Young, S. Managing Safety: An Attitudinal Based Approach to Improving Safety in Organizations. *Leadership and Organization Development Journal*, 17, 13-20, 1996.
- Fenton and Neil, 1999 b. Predicting Software Defects Using Bayesian Belief Nets. Agena Ltd, Document identifier: Agena/Philips/D02-v1.0. Version 1.0, 30 June 1999 (b).
- Fenton N and Neil M. Software Metrics and Risk, FESMA 99, 2nd European Software Measurement Conference, 8 October, 1999.
- Fenton N. and Neil M. Making Decisions: Bayesian Nets and MCDA. To appear in Journal of Knowledge Based Systems, 2000.
- Fenton N. and Neil M. The “Jury Fallacy” and the use of Bayesian Networks to present Probabilistic Legal Arguments. Accepted for publication in the bulletin of the IMA, 2000.
- Fenton N., Littlewood B., Neil M., Strigini L., Sutcliffe A. and Wright D. Assessing dependability of safety critical systems using diverse evidence. IEE Proceedings on Software Engineering, Vol. 145, No.1, February 1998.
- Fenton N.E., and Neil M. A Strategy for Improving Safety Related Software Engineering Standards. IEEE Transactions on Software Engineering Vol. 24, No. 11, November 1998
- Fenton NE and Pfleeger SL, 'Software Metrics: A Rigorous and Practical Approach', PWS, 1998
- Fenton NE, How effective are software engineering methods?, Journal of Systems and Software Vol 20, 93-100, 1993.
- Hurst, N., Young, S., Donald, I., Gibson, H., & Muyselaar, A. (1996) Measures of Safety Management Performance and Attitudes to Safety at Major Hazard Sites. *Journal of Loss Prevention in the Process Industries*, 9, 161-172.
- IMPRESS: (IMproving the software PRocESS using bayesian nets) funded by EPSRC, 1996-2000 with collaborators: Hugin Expert A.S. (Denmark).
- Neil and Fenton 2000. Risk Assessment of ATM Architectures (ATM-RAM). Agena Ltd, Document identifier: Agena/NATS/Risk_Assessment_STCA_deliv3_ver1_0, Version 1.0, 22 April 2000 (b).
- Neil and Fenton 2000. TRACS: Transport Reliability Assessment & Calculation System. TRACS Version 4.3 (Professional) User Manual. Defence Evaluation and Research Agency (DERA), Data Analysis and Reliability Section (DARS) Fighting Vehicles Department, Land Systems Sector. Agena Ltd, Document identifier: Agena/DERA/user manual v2.2, 20 July 2000 (a).
- Neil M, Fenton N. and Nielsen L. Building Large-Scale Bayesian Networks. To appear in Knowledge ; Engineering Review, 2000.
- Neil M. and Fenton N.E. A Critique of Software Defect Prediction Research. IEEE Transactions on Software Engineering, 25, No. 5, 1999. (a)
- Neil M. Littlewood B. and Fenton N. Applying Bayesian Belief Networks to Systems Dependability Assessment. Proceedings of Safety Critical Systems Club Symposium, Leeds, Published by Springer-Verlag, 6-8 February 1996.

Pfleeger SL, Fenton NE, Page P, Evaluating software engineering standards, IEEE Computer, 27(9), 71-79, Sept, 1994.

Reason J. *Managing the Risks of Organisational Accidents*. Ashgate Press, 1997.

S.L. Lauritzen and D.J. Spiegelhalter, "Local Computations with Probabilities on Graphical Structures and their Application to Expert Systems (with discussion)". *Journal of the Royal Statistical Society Series B*, Vol. 50, No 2, pp.157-224, 1988.

SCULLY: Scaling up Bayesian Nets for Software Risk Assessment. 1 July 2000 - 30 June 2003, EPSRC Project GR/N00258, Partners: Philips and Hugin A/S (Denmark).Funding to QMW: £203,501.

SERENE: SafEty and Risk Evaluation using bayesian Nets, funded by CEC Framework IV 22187 Partners: ERA Technology (UK), HUGIN Expert A/S (Denmark), TÜV Nord (Germany) Electricité de France, Objectif Technologie (France).

SHIP: Assessment of the Safety of Hazardous Industrial Processes in the Presence of Design Faults, funded by the CEC Environment programme, 1993-1995 with collaborators: Adelard (UK), IEI-CNR (Pisa, Italy), VTT (Finland), Corelis Technology (France), ENEA (Rome, Italy).

SIMP: Systems Integration for Major Projects. 1 July 2000 - 30 June 2003, EPSRC Systems Integration Initiative Programme, Project GR/N39234 Partners: BAe, Intellectual Capital Services (ICS). Kennedy Carter, UMIST, City University (CHCID). Funding to QMW: £194,873.

SMARTIE: Standards and Methods Assessed using Rigorous Techniques in Industrial Environments, funded by the UK Systems Engineering Programme supported by the EPSRC and DTI, 1990-1995 with collaborators: British Rail, Brameur Ltd, Secure Information Systems Ltd, Praxis, and Programming Research Ltd;

The Hon Lord Cullen. *The Public Enquiry into the Piper Alpha Disaster. Volume 2*. London HMSO, 1990.

Turnbull 1999. *Internal Control - Guidance for directors of listed companies incorporated in the United Kingdom*. Published by ICAEW on 20 April 1999.

ANNEXE 4

Synthèse de « *Prévention du risque de dommages liés aux inondations* »

La Commission Internationale pour la Protection du Rhin, 2002

http://www.iksr.org/pdf/RZ_iksr_franz.pdf

„Seule la volonté des différents acteurs de coopérer permet de limiter les dommages dans l'intérêt commun. La prévention des dommages nous concerne tous.“

Le présent rapport s'efforce de présenter de manière générale et d'évaluer les mesures envisageables pour réduire le risque de dommages liés aux inondations dans diverses situations. Il met ainsi en avant les moyens de réduire, dans les conditions actuelles, les dommages potentiels en cas de crue, mais ne saurait se substituer à des études détaillées d'analyse des risques encourus, seules à même de dire s'il y a lieu de prendre des mesures complémentaires et le cas échéant d'en définir la nature précise.

■ Conditions préalables à la prise de mesures de prévention des dommages liés aux inondations

Connaître l'aléa et ses paramètres essentiels tels que la probabilité, la nature et l'intensité de l'impact est une condition préalable à la prévention des dommages. Ces connaissances doivent être transmises à tous les acteurs avec la crédibilité requise.

Les **cartes de l'aléa d'inondation** font ressortir les surfaces exposées au risque. Elles sont un outil de planification indispensable. Des éléments de rappel bien visibles dans le paysage entretiennent la conscience du risque auprès des populations. Cette conscience du risque doit être maintenue éveillée par **l'information et la formation**.

Le **niveau des dommages potentiels** détermine la priorité et l'étendue des mesures. Pas de mesures sans dommages potentiels.

■ Prévisions

Des prévisions de bonne qualité permettent une occupation des sols de valeur économique plus élevée dans les zones exposées au risque. Elles sont particulièrement efficaces pour la protection des personnes, même lorsque le temps d'avertissement est court.

Elles ne montrent toute leur efficacité que si elles sont mises en relation avec des mesures prévues et expérimentées au préalable.

■ Protection des personnes

Les **pertes en vies humaines** sont souvent imputables à un mauvais comportement. Des refuges sûrs doivent être accessibles rapidement. La prise de conscience de l'aléa et la connaissance de l'accès aux refuges sont indispensables.

Lorsque l'on dispose de suffisamment de temps, le **sauvetage de personnes** est possible avec les moyens techniques actuels, même dans des situations très difficiles.

■ Mesures de préservation de surfaces

Préserver les surfaces de toute construction par le biais de dispositions d'aménagement du territoire pour éviter à long terme la croissance des dommages potentiels et donner au fleuve l'espace nécessaire pour atténuer voire empêcher l'inondation de zones d'habitat. Ce type de mesures ne fait pas baisser les dommages potentiels actuels.

Réglementer la construction et les usages par le biais de documents de planification appropriés pour amener les propriétaires à adapter le type de construction au risque. Des mesures de ce type sont nécessaires pour la protection des personnes et pour éviter les dégradations environnementales ou les préjudices à tierces personnes. Elles ont un effet à long terme.

Le risque de dommages

Le risque de dommages est généralement compris comme le croisement de la probabilité de dommage et de la somme des dommages potentiels

Possibilités d'agir sur le risque de dommages

Depuis le 19^{ème} siècle, on s'emploie à agir sur le risque en faisant quasi exclusivement appel à des mesures de protection fondées sur le génie hydraulique pour réduire l'occurrence des crues.

Le savoir sur les moyens de limiter l'étendue des dommages par une adaptation des usages ou du mode de construction s'est perdu ou a été supplanté parce que jugé superflu. Le présent rapport entend mettre en avant les moyens de réduire, dans les conditions actuelles, les dommages potentiels en cas de crue.

Choix des mesures

Le type de mesures à adopter est essentiellement déterminé par l'impact de eaux, c'est-à-dire leur profondeur. La justification économique d'une mesure dépend de l'occurrence de l'inondation, des coûts de la mesure et des dommages que cette dernière est censée prévenir.

■ Mesures de construction préventive

L'**adaptation des ouvrages au risque en présence**, combinée à différentes mesures temporaires de protection des bâtiments, est la seule mesure qui permette de réduire les dommages potentiels existants dans les zones d'habitat sans modifier fondamentalement les usages.

La **protection des bâtiments** vise à réduire ou à éviter les dommages sur un bâtiment donné. Le degré d'efficacité peut atteindre 100 % lorsque l'eau peut être retenue par un rehaussement des bâtiments menacés ou des dispositifs de protection locaux, 50 à 75 % lorsque le bâtiment est étanché et 10 à 30 % lorsque l'aménagement intérieur résiste à l'impact des eaux. Ces mesures sont réalisables en cas de remise en état suite à une inondation, lors d'aménagements importants ou dans les nouveaux bâtiments.

Les **chauffages au mazout** représentent un risque particulier. Si ces équipements sont protégés, les dommages occasionnés aux bâtiments peuvent baisser de 50 à 65 %. Les dommages occasionnés aux **entreprises industrielles et commerciales** sont à peu près deux fois plus élevés que ceux subis par les habitations. L'étanchement et la mise hors d'atteinte sont des mesures particulièrement efficaces car elles permettent de réduire la durée de l'interruption d'exploitation. Les dommages dus à une interruption de l'exploitation peuvent dépasser les dommages directs. Lorsque les **profondeurs d'eau dépassent deux mètres**, les mesures de protection des bâtiments ne font plus effet que dans quelques cas isolés.

■ Mesures de comportement préventif

Une des conditions permettant d'adopter le comportement approprié en situation d'inondation consiste à **planifier les actions éventuelles** à engager en les ajustant au temps de préalerte.

L'**évacuation ou le déplacement de biens mobiliers** dans les habitations peut permettre de réduire les dommages sur ces biens de 20 à 80 % selon le temps de préalerte. Celui-ci devrait être d'au moins 4 heures. Dans les entreprises industrielles et commerciales, l'évacuation requiert une bonne organisation en regard des grandes quantités de biens. Cette mesure est ici particulièrement efficace puisqu'elle permet de protéger des biens de grande valeur, de raccourcir la durée de l'interruption d'exploitation et d'éviter les difficultés de livraison.

■ Mesures de prévention des risques

Si l'on réussit à éviter une inondation en prenant des **mesures d'urgence**, on a alors un rapport coûts/efficacité très avantageux. En cas d'événement extrême, les **surfaces de décharge de secours**, qui présentent des dommages potentiels moindres, peuvent être inondées. Les surfaces de décharge d'urgence doivent être partie intégrante des plans de lutte contre les risques majeurs.

La **prévention financière** individuelle doit figurer en première place, les contributions publiques visant à garantir le minimum vital devant arriver en dernier lieu. A mi-chemin de ces deux positions, l'Etat peut mettre en place un système d'assurance. Les assurances permettent de répartir les dommages sur la communauté, les rendant ainsi supportables pour le particulier. Elles peuvent inciter l'assuré à prévenir les dommages par le biais de recommandations et de clauses d'assurance adaptées au risque. Cependant, les conditions générales du régime d'assurance doivent être conçues de manière à rendre la prime d'assurance financièrement abordable et à favoriser l'application des mesures de prévention des dommages.

Promouvoir la mise en oeuvre

Information et recommandations: elles ne posent juridiquement aucun problème. Leur succès est fonction de l'expérience ou, lorsqu'elle fait défaut, de la force de persuasion des arguments utilisés. Que l'expérience soit personnelle ou qu'elle subsiste dans les zones avoisinantes, elle ne doit en aucun cas disparaître.

Des **incitations financières** telles que des prestations d'assurance adaptées ou des subventions peuvent être mises en place.

Les **dispositions réglementaires** sont indispensables en cas de vulnérabilité des personnes et de danger pour l'environnement ou des tiers. Les dispositions réglementaires mal justifiées restent souvent sans effet.

Mesures de prévention des dommages inondations

Réduire la vulnérabilité des personnes

Dans des locaux, éviter : personnes âgées ou handicapées dans locaux vulnérables, locaux sans issue vers des étages supérieurs, présence dans les sous sols et parking, utilisation des ascenseurs.

A l'extérieur : se tenir sous les ponts ou les digues, camper sur le tracé d'équipement, rouler en voiture sur les routes inondées (risques d'être emporté dès que la hauteur d'eau sur les routes est supérieure à 50 cm)

En ce qui concerne les secours, le retour d'expérience des Pays-Bas montre qu'il est indispensable d'avoir une politique d'information claire et uniforme, à ajuster entre les différents services décisionnels et les médias pour convaincre les populations de la nécessité d'évacuer. Cela demande des mesures préparatoires engageant les organisations locales, toutes les personnes doivent être évacuées et la protection contre le vol et le vandalisme doit être clairement démontrée. Les temps d'alerte doivent au moins être de 4 h, des temps plus importants permettent d'évacuer de nombreux biens des habitations et des entreprises (locaux de sécurité à prévoir).

Répartition des coûts des dommages

L'évolution des dommages est exponentielle traduisant l'accroissement de la densification de l'habitat et du coût des biens inondés dans les zones inondables.

L'analyse des dommages s'appuie sur des constats à l'étranger (absence de chiffres provenant des assureurs français). En l'absence de mesure préventive, les dommages en zones résidentielles affectent pour une part égale les biens mobiliers et les bâtiments :

biens mobiliers	
meubles	40 %
autres équipements	40 %
portes et gros appareils électriques	20 %.
bâtiments	
murs, plafonds, revêtements	36 %
sols et revêtements	27 %
installations de chauffage	27 %
électricité, fenêtres.	10%

Mode d'équipement des habitations

La prévention minimise les dommages en adaptant l'usage et l'équipement des bâtiments :

- renoncer à une cave ou au sous-sol, abaisse les dommages de 3000 à 6000 € ;
- rendre la cuve à mazout résistante aux eaux ou opter pour un chauffage au gaz, évite 50 % des dommages correspondants ou plus ;
- placer les principaux interrupteurs et distributeurs au-dessus du niveau d'inondation, permet d'utiliser les étages supérieurs même pendant la crue.

Étanchement

L'étanchement complet d'ouvrages permet de protéger l'intérieur du bâtiment de l'impact des eaux. Les dommages se limitent alors à une façade extérieure salie et humide.

Pour les ouvrages existants, si la façade et la cave sont étanches, l'étanchement se limite aux ouvertures du bâtiment. Il est ainsi possible d'installer des portes et des fenêtres étanches ou, si la période d'avertissement est suffisante, d'ériger des batardeaux ou de mettre en œuvre d'autres mesures de fortune (sacs de sable et bâches etc.)

Si la façade du bâtiment n'est pas étanche, on peut la recouvrir de batardeaux ou d'une bâche pour la rendre étanche. Étancher durablement a posteriori des bâtiments équipés de caves non étanches entraîne un travail et des frais importants, car il faut mettre à nu la construction dans son ensemble.

Si la cave n'est pas étanche mais que les quantités d'eau infiltrées dans la cave sont faibles, on les évacue par pompage permanent, de sorte qu'il reste seulement à nettoyer et à faire sécher les murs et le sol de la cave. Si la cave ne résiste pas systématiquement à la poussée des eaux, il faut alors la remplir d'eau propre, en tout ou en partie, pour assurer sa stabilité. Il convient en tout cas d'accorder suffisamment d'importance au risque de poussée des eaux et de reflux des eaux d'égout lorsque l'on étanche un bâtiment.

Une cave étanche réduit les dommages de l'ordre de 75 % à 85 %. On parvient à réduire les dommages de 50 à 60 % en évacuant l'eau par pompage lorsque seule la cave est touchée. Ces mesures ne concernent pas les zones exposées à des profondeurs d'inondation importantes.

Le rehaussement est une option très efficace et financièrement avantageuse pour protéger les nouvelles constructions :

- la construction sur piliers offre une grande liberté de conception ; l'espace gagné sous le bâtiment peut servir de parking ;
- la construction sur murs agrandit les possibilités d'utilisation du bâtiment ;
- la construction sur remblai constitue une mesure financièrement très avantageuse (notamment si le terrain avoisinant est en pente) et judicieuse quand le niveau des eaux souterraines est élevé.

Dispositifs permanents ou parois mobiles

Les mesures de mise hors d'atteinte (digues, parois mobiles) peuvent réduire l'étendue des dommages de 60 à 80%. Les dommages restants dépendent fortement de la cave. Si celle-ci est étanche, l'efficacité peut atteindre pratiquement 100 %. La mise en œuvre de cette mesure est nettement restreinte dans les zones exposées à de grandes profondeurs d'inondation.

La mise hors d'atteinte à l'aide de parois ne prévient pas les dommages imputables aux eaux souterraines.

Au moyen d'un système des parois mobiles de protection composées de supports d'aluminium, de palettes et de bâches, on a pu éviter l'inondation du quartier de Rodenkirchen, à Cologne, lors de la crue de 1999. Ce système a été mis en place par 18 personnes en 5 heures sur une longueur de 500 mètres. Du fait de sa souplesse d'utilisation, de sa maniabilité et de son poids faible, ce système est également opérationnel dans les zones d'habitat.

ANNEXE 5

Internal Control

Guidance for Directors on the Combined Code

(Le rapport Turnbull)

ISBN 1 84152 010 1

Published by

The Institute of Chartered Accountants
in England & Wales
Chartered Accountants' Hall
PO Box 433
Moorgate Place
London EC2P 2BJ
Internet: www.icaew.co.uk/internalcontrol

Copyright © The Institute of Chartered
Accountants in England & Wales

Further copies can be obtained from:

Accountancy Books
PO Box 21375
London WC1N 1QP

Telephone 020 7920 8991
Fax 020 7920 8992
www.accountancybooks.co.uk

September 1999

Contents

	Paragraph number(s)
Introduction	
Internal control requirements of the Combined Code	1-7
Objectives of the guidance	8-9
The importance of internal control and risk management	10-13
Groups of companies	14
The Appendix	15
Maintaining a sound system of internal control	
Responsibilities	16-19
Elements of a sound system of internal control	20-24
Reviewing the effectiveness of internal control	
Responsibilities	25-26
The process for reviewing effectiveness	27-34
The board's statement on internal control	35-41
Internal audit	42-47
Appendix	
Assessing the effectiveness of the company's risk and control processes	
Membership of the Internal Control Working Party.	

Introduction

Internal control requirements of the Combined Code

1. When the Combined Code of the Committee on Corporate Governance (the Code) was published, the Institute of Chartered Accountants in England & Wales agreed with the London Stock Exchange that it would provide guidance to assist listed companies to implement the requirements in the Code relating to internal control.
2. Principle D.2 of the Code states that 'The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets'.
3. Provision D.2.1 states that 'The directors should, at least annually, conduct a review of the effectiveness of the group's system of internal control and should report to shareholders that they have done so. The review should cover all controls, including financial, operational and compliance controls and risk management'.
4. Provision D.2.2 states that 'Companies which do not have an internal audit function should from time to time review the need for one'.
5. Paragraph 12.43A of the London Stock Exchange Listing Rules states that 'in the case of a company incorporated in the United Kingdom, the following additional items must be included in its annual report and accounts:
 - a. a narrative statement of how it has applied the principles set out in Section 1 of the Combined Code, providing explanation which enables its shareholders to evaluate how the principles have been applied;
 - b. a statement as to whether or not it has complied throughout the accounting period with the Code provisions set out in Section 1 of the Combined Code. A company that has not complied with the Code provisions, or complied with only some of the Code provisions or (in the case of provisions whose requirements are of a continuing nature) complied for only part of an accounting period, must specify the Code provisions with which it has not complied, and (where relevant) for what part of the period such non-compliance continued, and give reasons for any non-compliance'.
6. The Preamble to the Code, which is appended to the Listing Rules, makes it clear that there is no prescribed form or content for the statement setting out how the various principles in the Code have been applied. The intention is that companies should have a free hand to explain their governance policies in the light of the principles, including any special circumstances which have led to them adopting a particular approach..
7. The guidance in this document should be followed by boards of listed companies in: assessing how the company has applied Code principle D.2; implementing the requirements of Code provisions D.2.1 and D.2.2; and reporting on these matters to shareholders in the annual report and accounts.

Objectives of the guidance

8. This guidance is intended to: reflect sound business practice whereby internal control is embedded in the business processes by which a company pursues its objectives; remain relevant over time in the continually evolving business environment; and enable each company to apply it in a manner which takes account of its particular circumstances. The guidance requires directors to exercise judgement in reviewing how the company has implemented the requirements of the Code relating to internal control and reporting to shareholders thereon.
9. The guidance is based on the adoption by a company's board of a risk-based approach to establishing a sound system of internal control and reviewing its effectiveness. This should be incorporated by the company within its normal management and governance processes. It should not be treated as a separate exercise undertaken to meet regulatory requirements.

The importance of internal control and risk management

10. A company's system of internal control has a key role in the management of risks that are significant to the fulfilment of its business objectives. A sound system of internal control contributes to safeguarding the shareholders' investment and the company's assets.
11. Internal control (as referred to in paragraph 20) facilitates the effectiveness and efficiency of operations, helps ensure the reliability of internal and external reporting and assists compliance with laws and regulations.
12. Effective financial controls, including the maintenance of proper accounting records, are an important element of internal control. They help ensure that the company is not unnecessarily exposed to avoidable financial risks and that financial information used within the business and for publication is reliable. They also contribute to the safeguarding of assets, including the prevention and detection of fraud.
13. A company's objectives, its internal organisation and the environment in which it operates are continually evolving and, as a result, the risks it faces are continually changing. A sound system of internal control therefore depends on a thorough and regular evaluation of the nature and extent of the risks to which the company is exposed. Since profits are, in part, the reward for successful risk-taking in business, the purpose of internal control is to help manage and control risk appropriately rather than to eliminate it.

Groups of companies

14. Throughout this guidance, where reference is made to 'company' it should be taken, where applicable, as referring to the group of which the reporting company is the parent company. For groups of companies, the review of effectiveness of internal control and the report to the shareholders should be from the perspective of the group as a whole.

The Appendix

15. The Appendix to this document contains questions which boards may wish to consider in applying this guidance.

Maintaining a sound system of internal control

Responsibilities

16. The board of directors is responsible for the company's system of internal control. It should set appropriate policies on internal control and seek regular assurance that will enable it to satisfy itself that the system is functioning effectively. The board must further ensure that the system of internal control is effective in managing risks in the manner which it has approved.
17. In determining its policies with regard to internal control, and thereby assessing what constitutes a sound system of internal control in the particular circumstances of the company, the board's deliberations should include consideration of the following factors:
 - I the nature and extent of the risks facing the company;
 - I the extent and categories of risk which it regards as acceptable for the company to bear;
 - I the likelihood of the risks concerned materialising;
 - I the company's ability to reduce the incidence and impact on the business of risks that do materialise; and
 - I the costs of operating particular controls relative to the benefit thereby obtained in managing the related risks.
18. It is the role of management to implement board policies on risk and control. In fulfilling its responsibilities, management should identify and evaluate the risks faced by the company for consideration by the board and design, operate and monitor a suitable system of internal control which implements the policies adopted by the board.
19. All employees have some responsibility for internal control as part of their accountability for achieving objectives. They, collectively, should have the necessary knowledge, skills, information and authority to establish, operate and monitor the system of internal control. This will require an understanding of the company, its objectives, the industries and markets in which it operates, and the risks it faces.

Elements of a sound system of internal control

20. An internal control system encompasses the policies, processes, tasks, behaviours and other aspects of a company that, taken together:
- I facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial, compliance and other risks to achieving the company's objectives. This includes the safeguarding of assets from inappropriate use or from loss and fraud, and ensuring that liabilities are identified and managed;
 - I help ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate a flow of timely, relevant and reliable information from within and outside the organisation;
 - I help ensure compliance with applicable laws and regulations, and also with internal policies with respect to the conduct of business.
21. A company's system of internal control will reflect its control environment which encompasses its organisational structure. The system will include:
- I control activities;
 - I information and communications processes; and
 - I processes for monitoring the continuing effectiveness of the system of internal control.
22. The system of internal control should:
- I be embedded in the operations of the company and form part of its culture;
 - I be capable of responding quickly to evolving risks to the business arising from factors within the company and to changes in the business environment; and
 - I include procedures for reporting immediately to appropriate levels of management any significant control failings or weaknesses that are identified together with details of corrective action being undertaken.
23. A sound system of internal control reduces, but cannot eliminate, the possibility of poor judgement in decision-making; human error; control processes being deliberately circumvented by employees and others; management overriding controls; and the occurrence of unforeseeable circumstances.
24. A sound system of internal control therefore provides reasonable, but not absolute, assurance that a company will not be hindered in achieving its business objectives, or in the orderly and legitimate conduct of its business, by circumstances which may reasonably be foreseen. A system of internal control cannot, however, provide protection with certainty against a company failing to meet its business objectives or all material errors, losses, fraud, or breaches of laws or regulations.

Reviewing the effectiveness of internal control

Responsibilities

25. Reviewing the effectiveness of internal control is an essential part of the board's responsibilities. The board will need to form its own view on effectiveness after due and careful enquiry based on the information and assurances provided to it. Management is accountable to the board for monitoring the system of internal control and for providing assurance to the board that it has done so.
26. The role of board committees in the review process, including that of the audit committee, is for the board to decide and will depend upon factors such as the size and composition of the board; the scale, diversity and complexity of the company's operations; and the nature of the significant risks that the company faces. To the extent that designated board committees carry out, on behalf of the board, tasks that are attributed in this guidance document to the board, the results of the relevant committees' work should be reported to, and considered by, the board. The board takes responsibility for the disclosures on internal control in the annual report and accounts.

The process for reviewing effectiveness

27. Effective monitoring on a continuous basis is an essential component of a sound system of internal control. The board cannot, however, rely solely on the embedded monitoring processes within the company to discharge its responsibilities. It should regularly receive and review reports on internal control. In addition, the board should undertake an annual assessment for the purposes of making its public statement on internal control to ensure that it has considered all significant aspects of internal control for the company for the year under review and up to the date of approval of the annual report and accounts.
28. The reference to 'all controls' in Code Provision D.2.1 should not be taken to mean that the effectiveness of every internal control (including controls designed to manage immaterial risks) should be subject to review by the board. Rather it means that, for the purposes of this guidance, internal controls considered by the board should include all types of controls including those of an operational and compliance nature, as well as internal financial controls.
29. The board should define the process to be adopted for its review of the effectiveness of internal control. This should encompass both the scope and frequency of the reports it receives and reviews during the year, and also the process for its annual assessment, such that it will be provided with sound, appropriately documented, support for its statement on internal control in the company's annual report and accounts.
30. The reports from management to the board should, in relation to the areas covered by them, provide a balanced assessment of the significant risks and the effectiveness of the system of internal control in managing those risks. Any significant control failings or weaknesses identified should be discussed in the reports, including the impact that they have had, could have had, or may have, on the company and the actions being taken to rectify them. It is essential that there be openness of communication by management with the board on matters relating to risk and control.

31. When reviewing reports during the year, the board should:
- I consider what are the significant risks and assess how they have been identified, evaluated and managed;
 - I assess the effectiveness of the related system of internal control in managing the significant risks, having regard, in particular, to any significant failings or weaknesses in internal control that have been reported;
 - I consider whether necessary actions are being taken promptly to remedy any significant failings or weaknesses; and
 - I consider whether the findings indicate a need for more extensive monitoring of the system of internal control.
32. Additionally, the board should undertake an annual assessment for the purpose of making its public statement on internal control. The assessment should consider issues dealt with in reports reviewed by it during the year together with any additional information necessary to ensure that the board has taken account of all significant aspects of internal control for the company for the year under review and up to the date of approval of the annual report and accounts.
33. The board's annual assessment should, in particular, consider:
- I the changes since the last annual assessment in the nature and extent of significant risks, and the company's ability to respond to changes in its business and the external environment;
 - I the scope and quality of management's ongoing monitoring of risks and of the system of internal control, and, where applicable, the work of its internal audit function and other providers of assurance;
 - I the extent and frequency of the communication of the results of the monitoring to the board (or board committee(s)) which enables it to build up a cumulative assessment of the state of control in the company and the effectiveness with which risk is being managed;
 - I the incidence of significant control failings or weaknesses that have been identified at any time during the period and the extent to which they have resulted in unforeseen outcomes or contingencies that have had, could have had, or may in the future have, a material impact on the company's financial performance or condition; and
 - I the effectiveness of the company's public reporting processes.
34. Should the board become aware at any time of a significant failing or weakness in internal control, it should determine how the failing or weakness arose and re-assess the effectiveness of management's ongoing processes for designing, operating and monitoring the system of internal control.

The board's statement on internal control

35. In its narrative statement of how the company has applied Code principle D.2, the board should, as a minimum, disclose that there is an ongoing process for identifying, evaluating and managing the significant risks faced by the company, that it has been in place for the year under review and up to the date of approval of the annual report and accounts, that it is regularly reviewed by the board and accords with the guidance in this document.
36. The board may wish to provide additional information in the annual report and accounts to assist understanding of the company's risk management processes and system of internal control.
37. The disclosures relating to the application of principle D.2 should include an acknowledgement by the board that it is responsible for the company's system of internal control and for reviewing its effectiveness. It should also explain that such a system is designed to manage rather than eliminate the risk of failure to achieve business objectives, and can only provide reasonable and not absolute assurance against material misstatement or loss.
38. In relation to Code provision D.2.1, the board should summarise the process it (where applicable, through its committees) has applied in reviewing the effectiveness of the system of internal control. It should also disclose the process it has applied to deal with material internal control aspects of any significant problems disclosed in the annual report and accounts.
39. Where a board cannot make one or more of the disclosures in paragraphs 35 and 38, it should state this fact and provide an explanation. The Listing Rules require the board to disclose if it has failed to conduct a review of the effectiveness of the company's system of internal control.
40. The board should ensure that its disclosures provide meaningful, high-level information and do not give a misleading impression.
41. Where material joint ventures and associates have not been dealt with as part of the group for the purposes of applying this guidance, this should be disclosed.

Internal audit

42. Provision D.2.2 of the Code states that companies which do not have an internal audit function should from time to time review the need for one.
43. The need for an internal audit function will vary depending on company-specific factors including the scale, diversity and complexity of the company's activities and the number of employees, as well as cost/benefit considerations. Senior management and the board may desire objective assurance and advice on risk and control. An adequately resourced internal audit function (or its equivalent where, for example, a third party is contracted to perform some or all of the work concerned) may provide such assurance and advice. There may be other functions within the company that also provide assurance and advice covering specialist areas such as health and safety, regulatory and legal compliance and environmental issues.
44. In the absence of an internal audit function, management needs to apply other monitoring processes in order to assure itself and the board that the system of internal control is functioning as intended. In these

circumstances, the board will need to assess whether such processes provide sufficient and objective assurance.

45. When undertaking its assessment of the need for an internal audit function, the board should also consider whether there are any trends or current factors relevant to the company's activities, markets or other aspects of its external environment, that have increased, or are expected to increase, the risks faced by the company. Such an increase in risk may also arise from internal factors such as organisational restructuring or from changes in reporting processes or underlying information systems. Other matters to be taken into account may include adverse trends evident from the monitoring of internal control systems or an increased incidence of unexpected occurrences.
46. The board of a company that does not have an internal audit function should assess the need for such a function annually having regard to the factors referred to in paragraphs 43 and 45 above. Where there is an internal audit function, the board should annually review its scope of work, authority and resources, again having regard to those factors.
47. If the company does not have an internal audit function and the board has not reviewed the need for one, the Listing Rules require the board to disclose these facts.

Appendix

Assessing the effectiveness of the company's risk and control processes

Some questions which the board may wish to consider and discuss with management when regularly reviewing reports on internal control and carrying out its annual assessment are set out below. The questions are not intended to be exhaustive and will need to be tailored to the particular circumstances of the company.

This Appendix should be read in conjunction with the guidance set out in this document.

1. Risk assessment

- I Does the company have clear objectives and have they been communicated so as to provide effective direction to employees on risk assessment and control issues? For example, do objectives and related plans include measurable performance targets and indicators?
- I Are the significant internal and external operational, financial, compliance and other risks identified and assessed on an ongoing basis? (Significant risks may, for example, include those related to market, credit, liquidity, technological, legal, health, safety and environmental, reputation, and business probity issues.)
- I Is there a clear understanding by management and others within the company of what risks are acceptable to the board?

2. Control environment and control activities

- I Does the board have clear strategies for dealing with the significant risks that have been identified? Is there a policy on how to manage these risks?

- I Do the company's culture, code of conduct, human resource policies and performance reward systems support the business objectives and risk management and internal control system?
- I Does senior management demonstrate, through its actions as well as its policies, the necessary commitment to competence, integrity and fostering a climate of trust within the company?
- I Are authority, responsibility and accountability defined clearly such that decisions are made and actions taken by the appropriate people? Are the decisions and actions of different parts of the company appropriately co-ordinated?
- I Does the company communicate to its employees what is expected of them and the scope of their freedom to act? This may apply to areas such as customer relations; service levels for both internal and outsourced activities; health, safety and environmental protection; security of tangible and intangible assets; business continuity issues; expenditure matters; accounting; and financial and other reporting.
- I Do people in the company (and in its providers of outsourced services) have the knowledge, skills and tools to support the achievement of the company's objectives and to manage effectively risks to their achievement?
- I How are processes/controls adjusted to reflect new or changing risks, or operational deficiencies?

3. Information and communication

- I Do management and the board receive timely, relevant and reliable reports on progress against business objectives and the related risks that provide them with the information, from inside and outside the company, needed for decision-making and management review purposes? This could include performance reports and indicators of change, together with qualitative information such as on customer satisfaction, employee attitudes etc.
- I Are information needs and related information systems reassessed as objectives and related risks change or as reporting deficiencies are identified?
- I Are periodic reporting procedures, including half-yearly and annual reporting, effective in communicating a balanced and understandable account of the company's position and prospects?
- I Are there established channels of communication for individuals to report suspected breaches of laws or regulations or other improprieties?

4. Monitoring

- I Are there ongoing processes embedded within the company's overall business operations, and addressed by senior management, which monitor the effective application of the policies, processes and activities related to internal control and risk management? (Such processes may include control self-assessment, confirmation by personnel of compliance with policies and codes of conduct, internal audit reviews or other management reviews).
- I Do these processes monitor the company's ability to re-evaluate risks and adjust controls effectively in response to changes in its objectives, its business, and its external environment?
- I Are there effective follow-up procedures to ensure that appropriate change or action occurs in response to changes in risk and control assessments?
- I Is there appropriate communication to the board (or board committees) on the effectiveness of the ongoing monitoring processes on risk and control matters? This should include reporting any significant failings or weaknesses on a timely basis.
- I Are there specific arrangements for management monitoring and reporting to the board on risk and control matters of particular importance? These could include, for example, actual or suspected fraud and other illegal or irregular acts, or matters that could adversely affect the company's reputation or financial position?

Membership of the Internal Control Working Party

Nigel Turnbull (Chairman)	Executive Director Rank Group Plc
Roger Davis (Deputy Chairman)	Head of Professional Affairs PricewaterhouseCoopers
Douglas Flint	Group Finance Director HSBC Holdings plc
Huw Jones	Director of Corporate Finance Prudential Portfolio Managers
David Lindsell	Partner Ernst & Young
Tim Rowbury	Internal Audit Consultant
Jonathan Southern	Director of Accounting and Reporting Diageo plc
David Wilson	Company Secretary and General Counsel Debenhams plc
Staff	
Anthony Carey	Project Director, ICAEW
Jonathan Hunt	Project Manager, ICAEW

ANNEXE 6

« *Plutôt prévenir que guérir* » de Carey et Turnbull

Article de Carey et Turnbull, *Plutôt prévenir que guérir*, paru dans le supplément risques des Echos, 28 septembre 2000.

Plutôt prévenir que guérir

Le conseil d'administration est responsable de la stratégie à long terme de l'entreprise. Dans cette optique, le rapport Turnbull présente les meilleures pratiques de conception, d'application et de maintenance d'un système efficace de contrôle interne des risques.



Anthony Carey

Anthony Carey était directeur de projet du groupe de travail sur le contrôle interne de l'Institute of Chartered Accountants en Angleterre et au pays de Galles. Il est actuellement directeur de l'Institute's Center for Business Performance et secrétaire du Corporate Governance Group.

La gestion des risques (« risk management ») doit faire partie intégrante de l'activité de l'entreprise et non pas être considérée comme un simple exercice permettant de satisfaire aux exigences réglementaires. En procédant à l'évaluation et au contrôle des risques, les sociétés s'assurent de saisir toutes les opportunités existantes, de renforcer leur avantage concurrentiel et de passer moins de temps à « éteindre les incendies ».

La réduction des événements imprévus et la capacité à atteindre les objectifs sont deux facteurs qui renforcent la confiance des actionnaires dans l'entreprise. Le climat qui en résulte contribue à augmenter le cours de l'action et à diminuer le coût du capital.

A cet égard, le rapport Turnbull, préparé par un groupe de travail de l'Institute of Chartered Accountants en Angleterre et au pays de Galles et avalisé par la Bourse de Londres, cherche, en partant d'une approche fondée sur les risques, à définir les méthodes adaptées à l'entreprise pour concevoir, mettre en œuvre et maintenir un système solide de contrôle interne.

Il propose davantage une infrastructure générale qu'une série de règles, et sa conception permet aux sociétés de moduler son application en fonction de circonstances spécifiques. Plutôt que de spécifier des contrôles définis pour l'ensemble des entreprises, ce rapport invite donc les conseils d'administration des sociétés cotées en Bourse à identifier les risques importants liés à la réalisation des objectifs et à mettre en place un système de contrôle interne fiable pour gérer efficacement ces risques. Tout cela exige du conseil une vision précise des objectifs de la

ANTHONY CAREY ET NIGEL TURNBULL

d'une décision mal évaluée, d'une erreur humaine, d'une mise en échec délibérée des contrôles ou de circonstances imprévues.

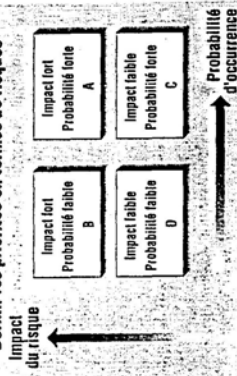
Identifier la problématique

Quand il détermine le profil de risque de la société, le conseil doit analyser l'information fournie par l'équipe de direction sur les risques importants courus par le groupe. Il lui faut aussi décider des types de risques qu'il juge acceptables, de la probabilité qu'ils se concrétisent et de la possibilité de réduire leurs répercussions en cas d'occurrence. Enfin, il ne devra pas oublier d'envisager les coûts et les bénéfices des contrôles spécifiques.

Le meilleur moyen d'identifier et d'évaluer les risques est de créer d'un système de contrôle efficace. Les entreprises doivent considérer tous les types de risques auxquels elles sont confrontées : stratégiques, opérationnels, financiers ou liés aux règles de conformité. Une étude récente montre que, dans cette évaluation, les directeurs financiers ont tendance à privilégier les risques stratégiques et opérationnels. On peut citer à titre d'exemples : l'incapacité à gérer avec succès des projets majeurs, principalement technologiques ; le manque d'innovation ; les problèmes liés à une mauvaise réputation ou à une gestion peu brillante de la marque ; et les difficultés dues au manque de motivation du personnel.

Dans leur identification des risques, les administrateurs ne se contenteront pas de sélectionner certains risques potentiels sur une base générique. Ils devront s'attacher uniquement aux risques spécifiques à leur secteur et aux circonstances sociales à un moment précis. Quels sont les obstacles susceptibles d'empê-

Définir les priorités en termes de risques



société, de son activité présente ainsi que de ses buts stratégiques à long terme.

Les principes énoncés dans ce rapport encouragent la gestion et non la suppression des risques. Dans une économie de marché concurrentielle, une société qui ne manifeste qu'un faible appétit pour le risque a peu de chances de générer des rendements élevés. En effet, dans certains cas, le conseil d'administration peut être amené à conclure, après analyse, que la société a intérêt à saisir davantage d'opportunités et à prendre plus de risques pour réussir à long terme. Cependant, les administrateurs et les parties prenantes doivent être conscients qu'un système de gestion des risques n'assure pas à 100 % la réalisation des objectifs. Il est impossible d'écartier la possibilité

L'Art de la Gestion des Risques

Les Echos - jeudi 28 septembre 2000

cher l'entreprise d'atteindre ses objectifs ? Il sera utile d'examiner comment le changement, au sein du groupe ou dans l'environnement économique et commercial externe, joue sur son profil de risque, car ce facteur est de nature à accroître les risques ou à en introduire de nouveaux.

Il est capital non seulement d'envisager les problèmes récents subis ou évités par la société et ses concurrents, mais aussi de tenir compte des types de risques qui peuvent encore se greffer par la suite. Les questions de probité seront également prises en compte, notamment celles liées à la fraude - un point sur lequel l'entreprise risque d'être particulièrement vulnérable. Enfin, avec le développement des marchés mondiaux et des marques internationales, auquel s'ajoute la puissance accrue des groupes de pression internationaux, nombreux sont les sociétés qui consistent un défaut d'image de marque comme une préoccupation majeure. Dans ce contexte, les risques liés à l'environnement sont importants et ne cessent d'augmenter dans de multiples secteurs d'activité. Ceux-ci peuvent générer des coûts directs significatifs, qu'il s'agisse d'amendes ou de dommages-intérêts, et nuire sérieusement à la réputation de l'entreprise.

Certains risques importants seront plus facilement décelés par une vision d'ensemble au niveau de la direction, et d'autres par les connaissances opérationnelles plus approfondies des exécutants. Le défi est de réunir ces deux approches. Les sociétés qui développent des systèmes de gestion des risques doivent avoir un langage commun à toute l'organisation pour décrire les risques similaires et les classer par catégories. Cela permet d'évaluer le risque cumulé dans un secteur donné.

Définir les priorités

Après avoir identifié les risques, il faut encore définir leur ordre de priorité. Ceci peut se faire initialement en analysant les risques bruts spécifiques à un événement ou à une situation. Par risque brut, on entend la probabilité qu'un événement ou une situation se produise, associée à l'évaluation de son impact - avant de prendre en compte l'application des stratégies de contrôle. Les conséquences potentielles seront analysées non seulement en termes financiers, mais aussi sous l'angle plus large de la réalisation des objectifs de l'entreprise.

Le rapport Turnbull souligne que ce contrôle doit être adapté à la culture et aux méthodes de l'entreprise. Il est donc préférable d'intégrer les mécanismes appropriés aux systèmes de gestion des informations existants, plutôt que de développer des modèles de signal de risques totalement séparés. Des bases de données lourdes sur les risques sont susceptibles d'éloigner l'entreprise de son objectif premier : amener son personnel à prendre conscience des risques cruciaux liés aux tâches qu'il accomplit, et à les gérer. Tous les employés ont un rôle à jouer dans le contrôle interne. Ils doivent en effet posséder collectivement les connaissances, les compétences, les informations et l'autorité suffisantes pour exercer et maîtriser le système de contrôle interne.

La communication entre les différents niveaux hiérarchiques de même qu'entre les services est l'un des secrets d'un système de gestion des risques efficace.



Nigel Turnbull

Nigel Turnbull a été président du groupe de travail sur le contrôle interne de l'Institute of Chartered Accountants en Grande-Bretagne et au pays de Galles. Il préside le groupe de travail sur l'entreprise de cet institut et fait partie des directeurs de Lasmo.

L'administration d'entreprise britannique

Quand la Bourse de Londres a publié en été 1998 son « Combined Code on Corporate Governance » (Code général de l'administration institutionnelle), l'accent mis sur les différents types de contrôles dévolus à la direction est passé de la notion de contrôle financier interne au concept plus global de contrôle interne. Le principe D2 de ce Code stipule que « le Conseil devra maintenir un système solide de contrôle interne afin de protéger l'investissement des actionnaires et les actifs de la société ». Une autre disposition de ce Code indique que les administrateurs devraient procéder au moins une fois par an à un examen de l'efficacité du système de contrôle interne du groupe et en informer les actionnaires.

Le rapport Turnbull complète la conception de ce principe d'administration d'entreprise en Grande-Bre-

tagne, grâce à des conseils sur l'application des mesures du Code relatives au contrôle et à l'audit internes. Ceci sera applicable aux exercices clos à partir du 23 décembre 2000, mais certaines dispositions transitoires sont déjà valables pour les clôtures préalables.

Ce guide invite les sociétés cotées en Grande-Bretagne à indiquer si leur système de contrôle des risques est conforme au Code. Toutefois, il revient au marché de décider des mesures à prendre dans le cas contraire. Le « Combined Code » remplace le « Cadbury Code » de 1992 qui stipulait que les administrateurs devaient rendre compte de l'efficacité du système de contrôle interne de leur société. Bien que, par la suite, le rapport Rutterman, avec ses conseils d'application sur ce dernier point, ait continué à se focaliser sur le contrôle financier interne.

La surveillance continue est un élément clef d'un bon système de contrôle. Mais, comme le souligne le rapport Turnbull, le conseil d'administration ne peut s'en contenter pour se décharger de sa responsabilité, à savoir vérifier l'efficacité du système de contrôle interne du groupe. Il doit aussi recevoir et étudier régulièrement les rapports fournis par les directeurs opérationnels et, le cas échéant, par les spécialistes de certains secteurs, tel l'audit interne, l'hygiène ou la sécurité. Si le conseil souhaite se concentrer sur les secteurs susceptibles d'offrir les meilleurs résultats, il aura intérêt à se focaliser sur un nombre limité de risques résiduels significatifs pour le groupe.

Lors de l'examen des possibilités de contrôle, les administrateurs vérifient qu'ils possèdent en temps voulu suffisamment d'informations pertinentes sur les risques encourus par l'entreprise. Ont-ils, par exemple, les données nécessaires sur la position de la société dans le marché ou sur les compétences et l'attitude de ses employés ? Les principaux indicateurs de risque et les résultats de la surveillance intégrée doivent être transmis régulièrement au conseil ou aux comités désignés. Le président aura intérêt à encourager des discussions régulières de bilan lors des réunions du conseil. Lors d'une proposition d'acquisition, par exemple, les administrateurs voudront probablement savoir si une analyse des risques complète et fiable a été effectuée. De même, un projet d'investissement important de capital devra inclure une estimation des risques.

Les rapports remis au conseil par le comité de direction doivent comporter une évaluation objective par secteurs du système de contrôle dédié à la gestion des principaux risques. Tout échec ou faille du contrôle sera discuté en termes de conséquences réelles ou potentielles et des mesures correctives. A tout moment, le conseil doit avoir la certitude d'avoir une vision des facteurs importants tenue à jour.

Le rapport Turnbull n'invite nullement les administrateurs à discuter des principaux risques dans leur rapport annuel, mais plutôt à indiquer, le cas échéant, l'existence d'un processus permanent d'identification, d'évaluation et de gestion des principaux risques pour l'entreprise, et à confirmer que celui-ci est conforme aux règles et fait l'objet d'une révision constante. Pour donner un aperçu de son niveau d'implication effective, le conseil d'administration pourra également récapituler son mode d'examen de l'efficacité du contrôle interne.

Le rapport Turnbull invite à une approche « sur mesure » de la gestion des risques, plutôt qu'un système « prêt à appliquer ». Dans cette optique, la situation unique et en constante évolution de chaque société cotée en Bourse sera fidèlement reflétée. Ces entreprises seront alors prêtes à affronter les défis du marché du XXI^e siècle. ●

Résumé

L'importance de la gestion des risques et du contrôle interne dans l'ordre du jour du conseil d'administration a changé. Dans cet article, Anthony Carey et Nigel Turnbull affirment que ces questions doivent désormais faire partie intégrante de l'activité de l'entreprise. Au Royaume-Uni, le rapport Turnbull sur le contrôle interne propose aux sociétés une structure de mise en place de systèmes de gestion des risques. Les administrateurs doivent savoir identifier et évaluer les risques intervenant dans la réalisation des objectifs de l'entreprise. Ce faisant, ils intégreront les nouveaux types de risques émergents – tels que l'image de marque. La prise de risque va de pair avec une économie concurrentielle. Il existe plusieurs stratégies pour les gérer : l'acceptation, le transfert, l'élimination ou le contrôle.

ANNEXE 7

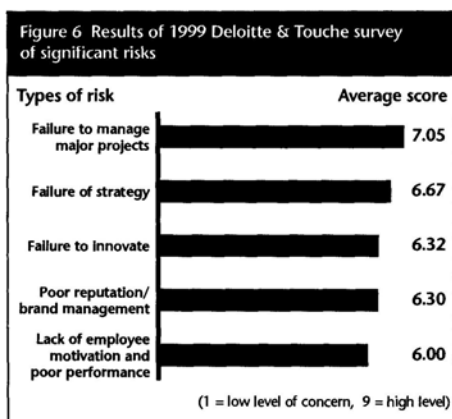
Implementing Turnbull, Risks

Risks, chapitre 4 de *Implementing Turnbull : A Boardroom meeting*, publication de The Institute of Chartered Accountants, Septembre 1999, disponible sur http://www.icaew.co.uk/viewer/index.cfm?AUB=TB2I_26539&tb5=1

4. Risks

4.1 What are the significant types of risks which could be addressed?

A recent survey revealed which types of risk were normally of most concern.



The survey indicated that the most significant risks were frequently operational or strategic in nature. The major projects which were identified frequently had a technology element.

How do you go about identifying risks?

- Understand the business's services and products
- Know the market place
- Consider the business process risks
- Also consider how people might behave in different situations
- Consider the quality of the local management team
- Think about the changing external environment

The matrix in figure 7 over the page, sets out various risks to consider but should not be regarded as comprehensive. There are, of course, various ways of setting out matrices, but it is particularly useful to include items which might immediately trigger a response from the board. Bland risk descriptions should be avoided. In the financial and some other sectors, it will be difficult to categorise between business, financial, operational and compliance risks. Also, some risks can be included under more than one heading.

A pitfall to avoid is merely selecting risks from a generic matrix. The risks need to be specific to the industry sector and the circumstances of the company. It is particularly

useful to relate them to the likely obstacles facing the critical success factors which underpin the achievement of the company's objectives. Useful questions to ask include:

- How is change affecting the risks we face and the risks we have chosen to take (this is because change areas are often the biggest areas of risk for a business)?
- What would we hate to see reported in the press?
- What problems or near misses have already happened to us or our competitors in recent years?
- What are the types of fraud and business probity issues to which the business could be particularly susceptible?
- What are the major regulatory and legal risks to which the business is exposed?
- What risks arise from the business processes?

4.2 How much risk could you take and in which areas?

Directors need to consider formally which risks are 'significant'. It is for the board to decide on their significance, according to the nature, extent and timing of events and the amount of 'headroom' available to the company should major problems occur.

Risk-return relationships and therefore the company's risk exposure are determined, not only by the external business environment, but also by the actions of its managers.

4.3 Should you quantify risks?

The detailed quantification of risk can be useful but in a smaller listed company it is perhaps enough to quantify risk as high, moderate or low. What matters most is that the board and management develop a clear, shared understanding of what risks are unacceptable or likely to become unacceptable, and then decide on how they are going to manage the risks using different control strategies.

Figure 7 Risk matrix

Business

Wrong business strategy
 Competitive pressure on price/market share
 General economic problems
 Regional economic problems
 Political risks
 Obsolescence of technology
 Substitute products
 Adverse government policy
 Industry sector in decline
 Take-over target
 Inability to obtain further capital
 Bad acquisition
 Too slow to innovate

Financial

Liquidity risk
 Market risk
 Going concern problems
 Overtrading
 Credit risk
 Interest risk
 Currency risk
 High cost of capital
 Treasury risk
 Misuse of financial resources
 Occurrence of types of fraud to which the business is susceptible
 Misstatement risk related to published financial information
 Breakdown of accounting system
 Unrecorded liabilities
 Unreliable accounting records
 Penetration and attack of IT systems by hackers
 Decisions based on incomplete or faulty information
 Too much data and not enough analysis
 Unfulfilled promises to investors

Compliance

Breach of Listing Rules
 Breach of financial regulations
 Breach of Companies Act requirements
 Litigation risk
 Breach of competition laws
 VAT problems
 Breach of other regulations and laws
 Tax penalties
 Health and safety risks
 Environmental problems

Operational and other

Business processes not aligned to strategic goals
 Failure of major change initiative
 Loss of entrepreneurial spirit
 Stock-out of raw materials
 Skills shortage
 Physical disasters (including fire and explosion)
 Failure to create and exploit intangible assets
 Loss of intangible assets
 Breach of confidentiality
 Loss of physical assets
 Lack of business continuity
 Succession problems
 Year 2000 problems
 Loss of key people
 Inability to reduce cost base
 Major customers impose tough contract obligations
 Over-reliance on key suppliers or customers
 Failure of new products or services
 Poor service levels
 Failure to satisfy customers
 Quality problems
 Lack of orders
 Failure of major project
 Loss of key contracts
 Inability to make use of the Internet
 Failure of outsource provider to deliver
 Industrial action
 Failure of big technology related project
 Lack of employee motivation or efficiency
 Inability to implement change
 Inefficient/ineffective processing of documents
 Poor brand management
 Product liability
 Inefficient/ineffective management process
 Problems arising from exploiting employees in developing countries
 Other business probity issues
 Other issues giving rise to reputational problems
 Missed business opportunities

Case Study No. 3

Green plc introduced control self-assessment techniques for some of its key operating units several years ago. This mainly involved using workshops to identify risks. The results were initially well received by the board but each year its enthusiasm and that of the staff waned a little more. The non-executive directors were concerned that the board was doing nothing to address many of the risks identified.

Turnbull has re-invigorated the workshops. A highly successful workshop has been held by senior operational management with the emphasis on avoiding major operational disasters and on identifying and responding to the potential obstacles to achieving the critical success factors for the next three years. The risks previously identified in the staff workshops were reviewed so that senior management were aware of the key issues highlighted in the past. Precise quantification of risk was avoided as it was felt that it would complicate and slow down the process.

An ongoing programme is being arranged for the staff but much more emphasis is being placed on:

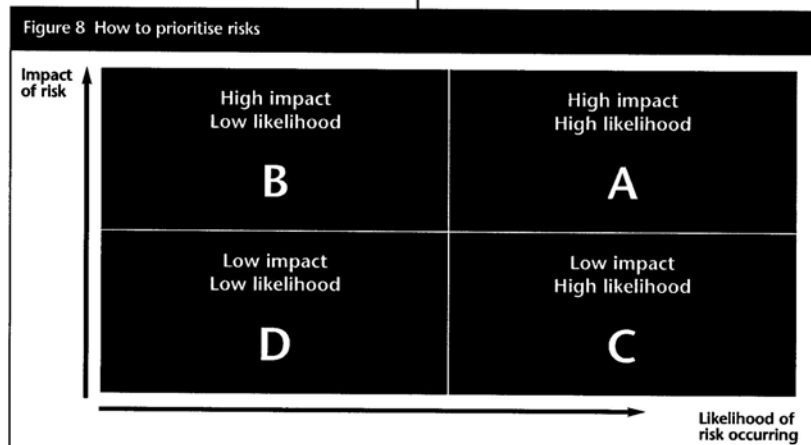
- awareness of the company's business objectives;
- risk awareness and the fundamentals of good risk management and internal control;
- the alignment of business objectives, risks and control;
- the identification and maintenance of early warning mechanisms;
- quicker responsiveness to changes within the company and to the external environment; and
- the sharing of good practices for improving the business.

The general feeling is that the new workshop programme will be much more relevant to the needs of the business.

4.4 Prioritisation of risks

How could risks be prioritised?

The following 'two by two' diagram in figure 8 is widely used. First you need to assess the gross risk associated with an event, that is the probability and impact of the event on the assumption that control processes are very weak or non-existent.



As can be seen, risks are prioritised according to their impact and likelihood. Generally an A,B,C or D rating will suffice, which can be interpreted as:

- A Immediate action
- B Consider action and have a contingency plan
- C Consider action
- D Keep under periodic review

The impact should be considered not merely in financial terms, but more importantly in terms of potential effect on the achievement of the company's objectives. Not all risks will be identified as significant. Non-significant risks would be reviewed regularly, particularly in the light of changing external events, to check that they remain non-significant.

Some boards prefer to use a 'three by three' alternative which offers more analysis than a simple 'two by two'. Some companies go as far as using a 'six by six'.

What do you do after the gross risks have been prioritised?

Having identified and then prioritised the significant risks in gross terms, it is then helpful to determine for each of these, (1) do the directors wish to accept this risk, (2) what is the control strategy to avoid or mitigate the gross risk, (3) who is accountable for managing the risk and maintaining and monitoring the controls, (4) what is the residual risk, that is the risk remaining after the application of the control processes, and (5) what is the early warning mechanism?

Taking each of these points in turn:

1. Each gross risk is considered in the context of the company's objectives. The board decides whether the identified risks exceed the benefits which will be obtained by achieving the objectives i.e., is it worthwhile to continue with a particular objective if the risks outweigh the reward? If the decision is to carry on, the board must decide how to respond to the risk by adopting specific control strategies.

The board need to determine their risk appetite i.e. the amount of risk which they are willing to take.

This involves considering, for significant risks, whether the risk/reward ratio is appropriate.

2. Control strategies include:

- accepting the risk;
- transferring the risk (e.g. passing it to another party by changing contractual terms);
- elimination (by adopting an exit strategy);
- control (by building control into the operational process, additional quality control, involving your best people in managing it);
- sharing the risk with another party;
- insuring against some or all of the risk;
- avoiding the risk in other ways.

3. Delegation of responsibility for managing risk in totality would not be allocated to a single individual. Ideally, it would be spread across those responsible for managing different business activities.

4. Consideration could be given to determining the level of risk remaining after the application of the control strategy. A key point to note is that it is not possible to eliminate risk entirely. Risk management policies need to be aligned with the company's objectives – there is no use in trying to eliminate all risks in the company, since some risk will always be undertaken in order to make profit. You need to know your risk profile and how to manage it. Where there are risks, they need to be sensible risks and not reckless or ill-considered ones. The company's business objectives need to be appropriate to the risk appetite of the board.

The number of risks identified as significant should preferably be limited. As a rough guide, a company could face as few as fifteen to twenty-five residual risks which require group management attention and which are significant to the group as a whole.

5. Early warning mechanisms are reporting processes which enable the board and senior management to be alerted before a problem becomes a disaster, and at a stage when action can be taken to mitigate or overcome the situation. The idea behind 'Key Risk Indicators' (as a form of early warning mechanism) is to give early indication of potential problems in order that corrective action may be taken promptly.

Business objectives and related plans need to include measurable performance targets and indicators. 'Key Performance Indicators' can be very useful early warning mechanisms. However, management's usual 'Key Performance Indicators' may not be sufficient on their own for this purpose as they are generally designed to report past results. By the time the Key Performance Indicators have shown a significant deterioration it may be too late to prevent losses or other adverse effects. Therefore, consider also the use of 'Key Risk Indicators'.

Case Study No. 4

Purple plc's sales and other figures looked good but the monthly management information gave no indication to the board that there had been a significant level of change in the sales force in the key regions. As a result, the sudden slump in sales took the directors totally by surprise and also precipitated a severe cash flow crisis.

Therefore, in determining their early warning mechanisms, Purple plc's management introduced people turnover into their reports from operating units as one of their key risk indicators.

Key questions which could be asked in this area include:

- Does the current management information provided to the board and senior management give them sufficient early warning of potential problems?
- Is there awareness of trigger events, or frequency of events, for each significant business risk which should alert management to a potentially significant issue?
- Does potential board news travel quick enough to the top of the company and is action taken quickly enough?

It should be borne in mind that under the Combined Code on Corporate Governance, the company chairman has a specific responsibility to ensure that all directors are properly briefed on issues arising at board meetings.

ANNEXE 8

Implementing Turnbull, Embedding the Process

Embedding the Process, chapitre 5 de *Implementing Turnbull : a Boardroom Meeting*,
publication de The Institute of Chartered Accountants, September 1999, voir
http://www.icaew.co.uk/viewer/index.cfm?AUB=TB21_26539&tb5=1

5. Embedding the process

After performing the high-level steps described above, should the process of introducing Turnbull be 'embedded'?

The answer is emphatically yes, as the Turnbull guidance expects the system of internal control to be embedded in the operations and form part of the culture. Also, the guidance expects risk management and internal control to be ongoing, and it is difficult, perhaps impossible, to achieve this unless the process is deepened. The key to achieving this is consultation throughout the business.

Useful steps you can take in this area include:

- a memo from the Managing Director to all members of management and staff to 'kick off' the deepening of risk management and internal control;
- dissemination of a risk management policy document and codes of conduct;
- 'round tables' and workshops at different levels of the company on risk management and internal control;
- re-allocation of some of the training budget to specific business risk training;
- dissemination of the key business objectives and significant risks;
- clear communication of policy on how significant risks are to be managed;
- involvement of staff in identifying and responding to change and in 'operating early warning mechanisms; and
- channels of communication for people to report suspected breaches or other improprieties.

Turnbull suggests that policies may be communicated on such things as customer relations, service levels for both internal and outsourced activities, health, safety and environmental protection, security of tangible and intangible assets including business continuity, expenditure, and accounting and financial and other reporting.

The aim should be to improve the culture at all levels of the company so that management and staff become more focused on meeting company objectives and managing properly the significant risks.

By changing behaviour at all levels of the company and embedding better business practices within day-to-day activities, there is less need for a multitude of control procedures to be laid on top of the business.

People issues which need to be considered include:

- whether the remuneration policies and working practices encourage good risk management and actually discourage taking reckless or bad risks;
- how to instill an attitude of 'doing things right first time';
- whether accountability for fulfilling business objectives and managing related risk is sufficiently clear;
- how to create an environment in which people are willing to report problems rather than to 'sit on them';
- whether the actions of different parts of the company are appropriately co-ordinated;
- whether the people in the company and in outsource providers have sufficient knowledge, skills and tools to support the achievement of the company's objectives and to manage the significant risks effectively;
- how to introduce a common risk management vocabulary across the company; and
- the adoption of work practices and training which result in improved performance.

Employee understanding of the purpose of controls and a sense of 'ownership' are critical to success.

Tumbull says that all employees have some responsibility for internal control as part of their accountability for achieving objectives. They, collectively, need to have the necessary knowledge, skills, information and authority to establish, operate and monitor the system of internal control. This will require an understanding of the company, its objectives, the industries and markets in which it operates and the risks it faces.

A major point which Tumbull stresses is that control should be embedded within the business processes by which a company pursues its objectives. It follows that, rather than developing separate risk reporting systems, it is best to build early warning mechanisms into existing management information systems. Cumbersome risk management databases can be a distraction from the key point which is that each person in the organisation becomes more focused on meeting the business objectives and in managing significant risks which relate to the tasks which he or she performs.

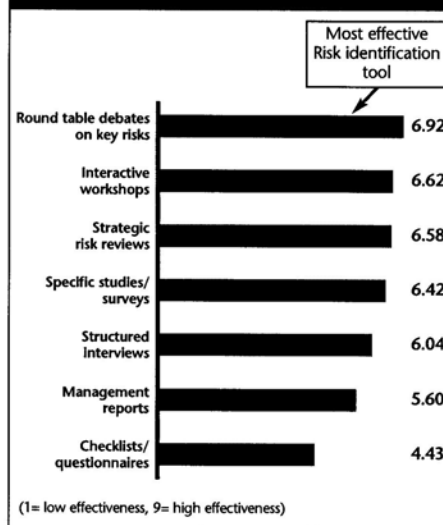
A key issue which can be addressed is the extent to which executive committees put significant risk management issues on their agenda. Where there is a risk committee, it should avoid usurping the role of the executive committee. It can encourage and foster good risk management and awareness, but it should not take over the role of the executive management.

Opportunities exist through embedding risk management to remove duplicate or unnecessary controls and to create an environment where, subject to sound risk management practices, there is more empowerment for people within the company to work to satisfy the needs of customers.

Senior management and the board need to ask whether they have enough timely, relevant and reliable reports on progress against business objectives and the significant risks. For instance, do they have enough qualitative information on customer satisfaction and employee attitudes? Also, as risks change, do they have the necessary business information to respond effectively?

You cannot rely only on an initial workshop. Changing external factors and internal problems result in new or significantly changing risks arising. There is a need to find out whether the employees believe that risk management is really mitigating significant risk. Unless other steps are taken, the board or senior management can be blissfully unaware of an impending disaster until it is too late. Set out in figure 9 opposite, are the results of a recent survey indicating which are the better techniques for identifying risk.

Figure 9 Deloitte & Touche 1999 survey of useful techniques for identifying business risk



Case Study No. 5

Red plc had a 'bottleneck' in that most key decisions had to go through a central department which, although it contained talented people, was overloaded with work. This overload had the effect of slowing down the responsiveness of the company and the danger of problems arising from the situation was perceived, by senior management, as a risk to the business.

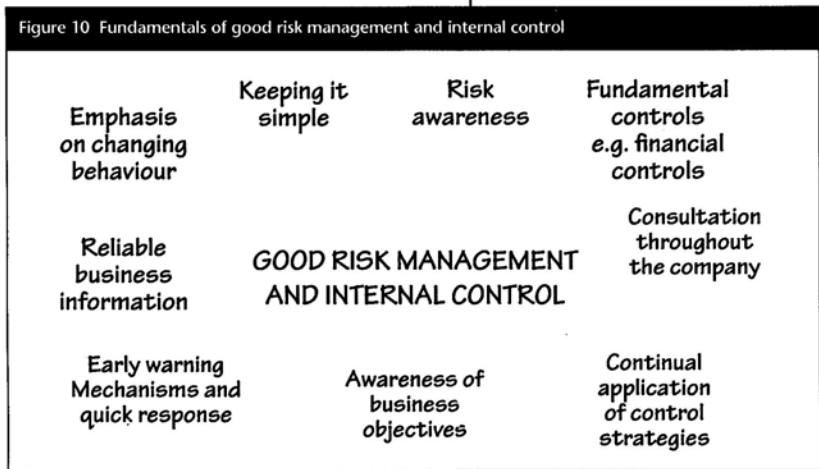
The department head took decisive action as part of a risk management initiative. This involved a departmental round table discussion on business objectives and risks, a 'change initiative' and follow up.

The initiative has been a success. The bottleneck has been removed, the department is much more highly regarded and the risk has been considerably reduced.

Identifying risks, good communication and addressing people issues are, however, not enough. There is also a need to ensure that the fundamentals of good risk management and internal control are maintained.

A high level of management and employee involvement in improving risk management and internal control is usually needed in order to turn around a problem unit or department.

What are the fundamentals of good risk management and internal control?
 These are illustrated in figure 10 below.



Management should ensure that in designing risk management and internal control procedures, they do not limit opportunities for innovation, emerging good practices and potential company benefits. However, it is useful to set out the scope for the freedom within which people are allowed to act.

What about internal financial control?

Internal financial control remains vitally important and is needed to provide the board and senior management with information of sufficient quality to make good decisions.

Key areas to consider include the need for:

- good accounting records;
- regular reconciliations;
- clearance of suspense accounts and review of unusual items;
- 'true and fair' year end reporting and reliable interim reporting;
- combating the risk of fraud;
- the safeguarding of assets from inappropriate use or loss;
- the avoidance of losses from derivatives and financial instruments;
- reliable management information from within and outside the company; and
- liabilities to be identified and managed.

Internal financial control is a key part of the fundamentals of good risk management which should underpin the wider aspects of business risk.

Frequently, many fundamentals of good risk management and internal control are already in place. Do not replace what is already working well.

Key questions which directors of smaller listed companies could ask in this area are:

- Does the workforce have sufficient understanding of the business objectives and risks relevant to the tasks which they perform?
- How can the speed of reporting of potential problems be improved?
- Are key financial, operational and compliance controls, e.g. reconciliations, sufficiently up to date?
- Are there any areas of the business which could give rise to public embarrassment, and, if so, how can they be improved?

Case Study No. 6

Black plc is a manufacturer. The company has turnover of £55 million and three manufacturing locations. Due to its size, management did not believe a full time internal audit function was necessary. The company has a small number of customers and has been losing market share as competitors move manufacturing facilities overseas to take advantage of lower production costs. Management decided to commence a risk identification and awareness programme with senior and middle management. The programme was managed by external advisers to remove internal bias and provide resource to drive through the exercise.

The major concern of management at the start of the programme was how to ensure that the project added value to the organisation. They were anxious that the project should not be seen as purely form filling or compliant in nature. Therefore, it was split into three phases.

Phase One – an initial meeting with the board, including non-executives, to clarify the company's strategy and identify strategic risks;

Phase Two – time spent one-on-one with middle management to explore operational, financial and IT risks and business opportunities;

Phase Three – testing of key procedures including stock ordering and usage, stock recording and preparation of management information.

Results

The board discussion generated significant debate concerning the company's strategy. This led to clarification of the strategy and presentation of this strategy to employees. The discussion formalised approaches to a number of risks. None of the risks in isolation were new to the company, but a formal approach to managing them had not been previously developed. Two specific examples being the creation of a role to explore sourcing and manufacturing opportunities overseas and formal reporting to the board of key customer relationships including the involvement of the marketing department to assess them.

Phase Two identified a number of new operational risks including a lack of appropriate non-financial management information, such as the reporting of waste levels, inflexible pay rates not matching workloads and supplier unreliability leading to production disruptions.

Phase Three has become an ongoing process with periodic checks on key financial and non-financial systems and procedures, with results being presented to, and well received by, the board.

ANNEXE 9

Time magazine “ **Chainsaw AI Gets The Chop**”

Chainsaw Al Gets The Chop

Sunbeam's tumbling stock price and the problems behind it spur the company's board to "Dunlap" the man whose name means to lay off

By DANIEL KADLEC

When Stetson law professor Charles Elson joined the board at Sunbeam Corp. two years ago, the company's pugnacious CEO, Albert J. Dunlap, wanted him to think like an owner. So he insisted that Elson dig deep into his own pockets and buy \$100,000 worth of Sunbeam stock. Two weeks ago, with the value of that stake fast eroding, Elson said, "You bet I looked at the company as an owner." So he and his similarly staked board mates moved fast to "Dunlap" Dunlap, sacking the job slasher whose name had become a Wall Street verb.

It was a startling turnabout. Just last February, "Chainsaw Al" was so highly prized by this same board that he was given a rich new employment contract that included options on a staggering 3.75 million shares of stock--one of the 10 biggest options grants ever at any company. Now the precise terms of that contract are in dispute as the board attempts to deny severance to Dunlap and his No. 2, Russell Kersh.

The whole mess is certain to devolve into a nasty court battle that until very recently only Dunlap's fiercest critics could have imagined. Along with perhaps half a dozen shareholder suits stemming from the stock collapse, and litigation with the American Medical Association over a botched endorsement deal, Sunbeam expects a lawsuit from Dunlap seeking a going-away package.

For Dunlap, 60, recent events at Sunbeam are a true Armageddon. He remains undeniably rich. But he has lost more than \$200 million on paper with his stock and stock options since Sunbeam shares began to slide last March, and his once vaunted reputation as a turnaround phenomenon is in tatters. That reputation is what landed him lucrative assignments, including previous stints as CEO at Scott Paper and Crown-Zellerbach, plus a high profile that he reveled in. It also put his book, *Mean Business*, on the best-seller list in 1996. That tome became a bible for those who followed Al's dictum that "the most important person in any company is the shareholder."

But he came up demonstrably short at Sunbeam. The appliance maker lost \$44.6 million in the first quarter, and may post another loss this quarter. Analysts who thought the company would earn \$2 a share in 1999 put the figure today just north of \$1. Sunbeam suffers from an inventory glut that will take months to assess and longer to fix. It appears Dunlap had been "stuffing the channel," persuading retailers through discounts to buy more gas grills than they would normally need. This practice helped swell Sunbeam earnings in 1997 but led to this year's crash. Even Dunlap's huge success at Scott Paper is now under a cloud. Kimberly-

Clark, which bought Scott for top dollar in 1995, is struggling to make the merger pay off. Profits tumbled 19% last quarter.

Dunlap's role as self-appointed messiah for shareholder value, meanwhile, is up for another casting call. Sunbeam shares were as high as \$53 early this year and have fallen 79%--to \$11.25, which is lower than the level at which the stock traded (\$12.50) when Dunlap was hired. The collapse has crushed morale at Sunbeam, where workers who survived Dunlap's initial slashing and burning (he cut half the company's 12,000 jobs) were rewarded with a company-wide stock-option plan that for a painfully brief period was gratifying but now represents lost dreams. Said an employee on lunch break last week at Sunbeam headquarters in Delray Beach, Fla.: "I popped open a bottle of champagne when I heard the news [about Chainsaw]."

Dunlap appears to have given up on himself even before the board did. Members insist that firing Dunlap never crossed their minds until the man also known as "Rambo in pinstripes" raised the issue himself. At a fateful meeting on June 9, Dunlap said half a dozen times that he would go away quietly if the board were to buy him out of his contract. That was when the board lost confidence. "I was shocked," recalls board member Howard Kristol, a New York lawyer who represented Dunlap in his initial contract negotiation with Sunbeam. "We felt he had already left."

The board moved swiftly. Within days it discovered that business was much worse than Dunlap had let on just weeks before. What he had termed an aberration--the inventory glut--was in fact a continuing problem. Dunlap was fired June 13.

I tried repeatedly to get Dunlap or his lawyer on the phone but was unsuccessful. And I should note for the record that in the past I have written favorably of Dunlap, whose policy of fast and deep cost cutting at troubled companies, I believe, makes sense. Clearly, though, I was wrong about how far he could take Sunbeam.

It falls to another turnaround pro, Jerry Levin, 54, to pick up the pieces, and few expect fast answers. "The business is in lousy shape," says Andrew Shore, an analyst at Paine Webber. Shore, a Dunlap critic who recently baited Chainsaw Al by publicly asking him to work for \$1 a year until the stock recovered, pegs any turnaround at two years.

By most accounts, Levin is the person for the job. He fixed cosmetics company Revlon in the early 1990s, and most recently was doing the same for outdoor-equipment company Coleman--both efforts on behalf of controlling shareholder Ronald Perelman. Levin's selection is no accident. On March 2, Perelman sold Coleman to Sunbeam in a stock swap, and he is now Sunbeam's second-largest investor, with a 13% stake. The largest is activist money manager Michael Price, who controls 17%. As a measure of how quickly Dunlap's career unraveled, Price only two weeks earlier had publicly, emphatically supported Dunlap. But he became as willing as anyone for the ax to fall.

In hindsight, there were warnings. A Barron's article in the June 8 edition questioned Dunlap's accounting methods, and a FORTUNE article with the same date suggested that his job was in jeopardy. Another bell ringer might have been massive selling by insiders at Coleman in March, beginning only days after the company agreed to be bought by Sunbeam. The Coleman folks had to sell, or lose, their stock options. But by moving so quickly, they bolstered the view that Dunlap had grossly overpaid. Indeed, nine Coleman insiders, including Levin, cashed out 581,000 shares, according to CDA Investnet--near the post-merger peak and just ahead of the stock's collapse along with Sunbeam.

It wasn't supposed to end like this. Coleman and two smaller deals were part of Dunlap's plan to build and to prove he was more than a one-trick pony. But the circus left town without

him, and he perhaps learned that restructuring a company and restructuring consumer demand are two very different tasks.

OTHER JOB CUTTERS

Robert E. Allen

COMPANY AT&T

CUTS 40,000 announced in 1996

CURRENT STATUS Splitting Ma Bell into three pieces to boost value didn't solve all his problems. In 1997 he retired under pressure; he now plays more golf

Louis V. Gerstner Jr.

COMPANY IBM

CUTS 35,000 from '93 to '95

CURRENT STATUS He's highly regarded for restoring growth at Big Blue. He remains CEO, and this year was given a new employment contract granting him 2 million stock options

Stanley C. Gault

COMPANY Goodyear Tire & Rubber

CUTS 12,000 from '91 to '96

CURRENT STATUS Turned around company after its first yearly loss since the Great Depression. Retired in '96 on good terms, and heads Gault Development in Louisville, Ky.

ANNEXE 10

Articles de presse sur Toyota

La Tribune, 31 octobre 2002 : Le dynamisme insolent des voitures japonaises

Le Journal du Dimanche, 1^{er} décembre 2002 : Toyota, les secrets de fabrication

La Tribune, 18 novembre 2002 : La palme de la qualité pour les voitures japonaises

La Tribune, 31 octobre 2002 : Toyota reste fidèle à ses fournisseurs

► AUTOMOBILE Le dynamisme insolent des voitures japonaises

- Toyota, Nissan et Honda enregistrent des bénéfices semestriels en forte hausse.
- Ils profitent d'une dépréciation du yen, de la réduction des coûts et du lancement de produits séduisants.

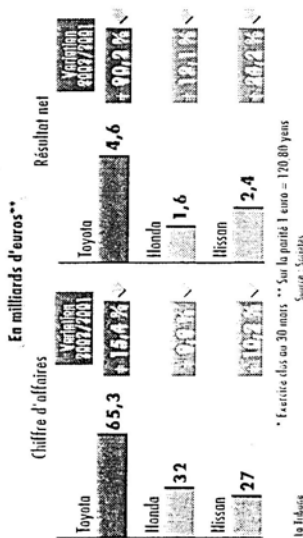
Les américains affichent des pertes abyssales et le numéro un européen, Volkswagen, accuse un net recul de sa profitabilité. Mais les japonais arborent toujours une insolente santé. Les trois grands constructeurs de l'archipel ont engrangé de nouveaux bénéfices record sur le premier semestre fiscal (avril-septembre) 2002-2003.

Et ce malgré la morosité de leur marché intérieur. Toyota double ainsi quasiment son profit net à 553,7 milliards de yens (4,6 milliards d'euros). Nissan et Honda voient leur résultat progresser respectivement de 24,2 % et de 12,1 %.

Les constructeurs nippons tirent profit de plusieurs facteurs, dont un purement extérieur : la

CROISSANCE ET RENTABILITÉ RECORD

Résultats des trois grands constructeurs automobiles japonais au premier semestre 2002 (avril-sept.)*



* Écriture du ou 30 mois. ** Sur la parité 1 euro = 170,80 yens

mené de 9,2 % à 1,4 million de véhicules, mais aussi de 37,8 % pour les motos à 3,87 millions. Nissan réalise de son côté des ventes en croissance de 7,5 % à 1,38 million. Le partenaire de Renault croît en particulier dans l'archipel (+ 12 % à 383.000) et aux États-Unis (+ 8,3 % à 378.000). Globalement, les japonais bénéficient de la rentabilité traditionnellement plus élevée des ventes d'automobiles au Japon et aux États-Unis par rapport à l'Europe où ils sont moins présents.

Les constructeurs nippons ont aussi réduit leurs coûts, ce qui a également un impact sur les résultats. Toyota affirme avoir économisé de la sorte 150 milliards (1,25 milliard d'euros) sur le semestre. Nissan annonce un gain de 102 milliards (880 millions d'euros) provenant de la réduction du coût des achats.

Pour l'année, Honda table sur un bénéfice net record de 410 milliards de yens (3,4 milliards d'euros), en hausse de 13 % mais en forte baisse par rapport aux projections initiales. Nissan escompte 490 milliards (4,2 milliards d'euros), en hausse de près d'un tiers sur 2001-2002.

Alain-Gabriel Verlaque

le groupe cartonne à l'étranger, où il bondit de 23,5 % à 1,99 million. Toyota progresse de 16,8 % en Amérique du Nord à un million d'unités et de 8 % à 392.027 en Europe. La firme bénéficie de la qualité reconnue de ses véhicules, de l'adaptation des modèles aux goûts locaux, comme les gros 4x4 et pick-up qui font un malheur outre-Atlantique ou les diesels performants sur le Vieux Continent.

Les livraisons mondiales de Honda ont pour leur part aug-

ment, la dépréciation du yen. Toyota reconnaît que l'érosion de la devise nipponne lui a rapporté 90 milliards (750 millions d'euros). Cet affaiblissement a notamment contribué à la compétitivité des produits japonais sur les marchés extérieurs, et donc à la hausse des ventes.

Ventes à l'étranger. Si Toyota a maintenu sa part de marché au Japon à 42 % (fino et Daihatsu compris) avec des ventes en léger retrait à 1,02 million de véhicules,

Toyota, les secrets de fabrication

Tolyo, Nagoya

Envoyé spécial

Florentin Collomp

« WELCOME to Toyota City ! » Ce n'est pas un surnom mais bien le nom officiel de cette ville, à 30 km de Nagoya, au centre du Japon. Une cité pas comme les autres. Parmi ses 250.000 habitants (c'est plus qu'à Montpellier), 60 % travaillent dans l'une des 18 usines de Toyota ou de ses sous-traitants. Dans les rues, sept voitures sur dix sont des Toyota. Le musée Toyota reçoit 320.000 visiteurs par an, dont un tiers d'écoliers, futurs consommateurs du géant japonais qui, en classe, étudient l'industrie automobile. A l'usine Takaoka, un véhicule sort des chaînes toutes les 57 secondes (2.700 par jour). De jeunes ouvriers aux cheveux teints en blond s'activent, visent, serrent, agrangent sans relâche. De savues méthodes électroniques attirent l'attention des chefs sur les problèmes éventuels. En cas de gros pépin, chaque ouvrier peut prendre l'initiative d'arrêter la chaîne afin de ne pas laisser un défaut non traité. C'est l'un des principes clés du « Toyota Production System ».

Dans ce qui n'était alors qu'une bourgade rurale où l'on cultivait la soie, Kiichiro Toyoda transforma en 1937 l'entreprise paternelle de métiers à tisser en constructeur automobile. Avec plus de trente ans de retard sur les Américains et les Européens, « C'est parce que l'on voulait rattraper ce retard que nous sommes parits très tôt à l'assaut du marché mondial », explique Shin Kanada, directeur des relations internatio-

Aujourd'hui, le constructeur, au troisième rang mondial derrière General Motors et Ford, vend 6 millions de véhicules dans le monde et réalise 130 milliards d'euros de chiffre d'affaires. Il sort un nouveau modèle (plus de 60 au total composent sa gamme) pratiquement tous les mois. Sa capitalisation boursière est la première au monde (parmi les constructeurs) et sa rentabilité la plus élevée du secteur. Un succès fondé sur le « Toyota Production System » (automatisation à visage humain, travail en équipes, production en flux tendus, amélioration continue...). Un modèle à l'efficacité redoutable (tout copié, jamais égalé). Pourtant, le géant ne se repose pas sur ses lauriers. Et trouve dans la remise en cause permanente un moteur de développement.

« Quand il n'y a pas de problème, c'est un problème », aime-t-on à répéter chez Toyota. Depuis dix ans, l'entreprise est servie : confrontée à un marasme économique qui ne cesse de se prolonger, ses ventes au Japon ont chuté de 30 %. Les experts ne prévoient pas de reprise avant

trois à cinq ans. Hémusement, Toyota vend aujourd'hui les deux tiers de sa production à l'étranger. La mondialisation du numéro un nippon est en marche. « L'international nous a apporté un second souffle, c'est une reformulation », affirme Shin Kanada.

Les résultats sont là. La marque taille des croupières aux constructeurs américains sur leur propre territoire : elle a déjà rallié 10 % de leur marché. En Europe, l'objectif de 5 % des ventes sera atteint en 2004 avec un an d'avance. En France, sa croissance atteint 27%. In octobre par rapport à l'année précédente, quand l'ensemble du marché recule. « D'ici deux à trois ans, la perception de Toyota en Europe aura considérablement progressé », pronostique Noriaki Hirakata, analyste financier chez Morgan Stanley à Tokyo.

A petits pas, le groupe fraye son chemin. « Le secret de Toyota, ce n'est pas son système de production, mais un mélange de puissance et d'humilité », pige Thierry Dombrevail, nouveau directeur des ventes et du marketing en Europe, recruté chez

Renault et ancien de Ford. Une (fausse ?) modestie incarnée à merveille par un petit homme trapu de 78 ans, Soichiro Toyoda, petit-fils du fondateur, président honoraire : « Vente des voitures en Europe, berceau de l'automobile, était un rêve qui nous a longtemps semblé inaccessible. Nous avons écouté les conseils de ceux qui nous ont recommandé de nous y installer pour être reconnus comme une entreprise européenne. Le rêve est devenu réalité ». Dernière est anglaise, la méthode est bien pensée : produire au plus près des zones de chalandise.

Depuis vingt ans, Toyota mène cette offensive de séduction sur tous les continents : elle produit aujourd'hui dans 26 pays. En France, son usine de Valenciennes, inaugurée voici deux ans, ne cesse d'augmenter sa capacité de production (*lire ci-dessous*). Le groupe va construire en République tchèque une petite voiture partenariale avec PSA pour renforcer son offre européenne à partir de 2005. Nagnère champion des exportations, Toyota devient même importateur : les modèles

Avenis vendus au Japon l'an prochain seront fabriqués en Grande-Bretagne !

« Nous avons encore beaucoup d'efforts à faire pour mondialiser notre gestion et accélérer les changements à tous les stades : production, organisation, distribution », relativise Hirochi Okada, président du conseil d'administration. Modeste, peut-être, la firme n'en a pas moins de grandes ambitions. En 2010, elle vise 15 % des ventes dans le monde. Après l'Amérique et l'Europe, marchés matures, Toyota mise gros sur la Chine, l'Inde et la Russie. « Il y a six milliards d'habitants sur terre et le parc automobile n'est que de 700 millions de véhicules », calcule Hirochi Okada. En Chine, il souhaite conquérir 10 % du marché d'ici à 2007.

Officiellement, Toyota n'a pas dans sa ligne de mire Ford ou General Motors. « Si nous devenions un jour numéro deux mondial, cela viendrait en plus de notre stratégie. Ce n'est nullement un objectif pour nous », prétend Soichiro Toyoda. Dans les faits, l'entreprise se prépare

sérieusement à prendre le dessus. « Les constructeurs américains, mal en point, réduisent leurs investissements tandis que Toyota ou Nissan les maintiennent. Cela portera ses fruits dans les années à venir », estime Noriaki Hirakata de Morgan Stanley.

Parmi les priorités de Toyota : les recherches sur la voiture propre. De la même manière qu'elle désamorce les préventions protectionnistes en s'installant dans les pays qu'elle convoite, Toyota embrasse les préoccupations écologiques croissantes pour mieux répondre. Après le premier véhicule hybride (essence-électricité), la Prius, vendue à 120.000 exemplaires depuis trois ans, le constructeur livre demain au ministère de l'Environnement japonais les premières voitures à pile à combustible (hydrogène) du monde. Une énergie appelée, selon l'entreprise, à remplacer à terme le pétrole. Le gouvernement américain a lui aussi passé commande de véhicules expérimentaux à Toyota. Un avertissement de plus aux constructeurs US.

► AUTO La palme de la qualité pour les voitures japonaises

Toyota arrive en tête de l'enquête du consultant JD Power, en Allemagne, sur la satisfaction des clients. Mazda, Honda, mais aussi BMW et Porsche, sont bien placés.

Considérés habituellement comme plutôt nationalistes en matière automobile, les consommateurs allemands n'en plébiscitent pas moins les belles japonaises. L'enquête effectuée outre-Rhin par le consultant américain JD Power sur la satisfaction des clients place en effet Toyota en tête, devant son compatriote Mazda. Aux onze premières places, on trouve pas moins de sept nippons. Certes, BMW et Porsche sauvent l'honneur des firmes germaniques avec, respectivement, la troisième et la cinquième place. Mais Mercedes n'arrive qu'à la huitième, Audi à la douzième. Et Volkswagen tombe dans la catégorie peu flatteuse des marques en dessous de la moyenne avec Fiat, Peugeot, Renault, Opel, Chrysler ou Smart. Sur les sept segments de marché étudiés, triomphent six Toyota et une Nissan. L'enquête, qui porte sur plus de 15.000 clients

Toyota plébiscité

(Indice de satisfaction des clients)
(En points)

1 - Toyota (Japon) :	831
2 - Mazda (Japon) :	805
3 - BMW (Allemagne) :	802
4 - Honda (Japon) :	797
5 - Porsche (Allemagne) :	796
6 - Daihatsu* (Japon) :	788
7 - Subaru (Japon) :	787
8 - Mercedes-Benz (Allemagne) :	781

(*) Groupe Toyota
Source : J. D. Power



Une ouvrière de l'usine Toyota à Miyazaki (Japon).

de 132 modèles âgés de deux à trois ans, analyse la fiabilité des véhicules, mais aussi la qualité de l'après-vente, le coût d'entretien et l'agrément général de la voiture. Ces résultats corroborent *grosso modo* ceux du récent sondage de JD Power en Grande-Bretagne, qui récompensait déjà Toyota.

Rigueur. « Il y a au Japon une très grande rigueur dans les process », explique-t-on chez Nissan, tout en précisant *in petto* : « Nos coûts de garantie sont sensiblement inférieurs à ceux de Renault. » La méthode, le sérieux dans la phase de conception, se retrouvent dans les usines. Par ailleurs, un constructeur

comme Toyota a établi de longue date une relation étroite et suivie avec ses fournisseurs japonais. Pas de baisse des coûts brutale exigée, pas de chantage, mais au contraire une fidélité réciproque à tout crin. Par ailleurs, Toyota reste attaché à son approche d'assembleur de composants. Il ne délègue pas la fabrication de modules complets. Nissan vient, toutefois, de faire le choix inverse. Du coup, que deviendra sa qualité ? Par ailleurs, les japonais sont moins technologiquement innovants que les français et prennent donc moins de risques. D'où une bien meilleure qualité sur les premières séries d'un nouveau modèle.

Alain-Gabriel Verdevoye

Toyota reste fidèle à ses fournisseurs

Alors que la plupart des constructeurs mondialisent leur réseau de fournisseurs, Toyota fait le choix inverse. Contrairement à Nissan, qui a démantelé son « keiretsu » (réseau de fournisseurs), le numéro un nippon renforce ses liens avec ses fournisseurs traditionnels. Le groupe compte en effet sur la fidélité des dizaines de PME qui fabriquent pour lui des composants, avec qui il a l'habitude de travailler.

Certes, il exige aussi des réductions de coûts et a lancé en juillet 2000 un plan à cet effet, baptisé CCC21 (pour « Construction of Cost Competitiveness ») ; mais, pour atteindre ses objectifs, il envoie ses cadres aider les équipementiers à les atteindre. Et quand il parle de délocaliser, en Chine ou en Europe, il essaie d'amener ses partenaires traditionnels dans ses valises.

Toyota a par ailleurs fait preuve de solidarité ces dernières années, en rachetant plusieurs fois à bon prix les participations mises en vente par les actionnaires de ses fournisseurs. Aujourd'hui encore, il n'utilise les concurrents des groupes qui composent son



Usine Toyota à Valenciennes. Le groupe a fait le choix de renforcer ses liens avec les sous-traitants.

« keiretsu » que pour établir des prix de référence. « Si vous travaillez avec Toyota, vous ne deviendrez jamais riche ; mais Toyota ne vous laissera jamais tomber », résume James Treece, directeur en Asie de la revue *Automotive News*.

Autre aspect sur lequel la stratégie de Toyota diffère totalement de celle de ses concurrents : la « modularisation ». De plus en plus, des constructeurs regroupent leurs fournisseurs dans une structure commune pour en exiger des modules complets (toit, système de transmission) et non plus des pièces.

Or Toyota reste viscéralement attaché à l'approche habituelle d'« une pièce par fournisseur ». Officiellement, parce qu'il pense qu'il faut connaître tous les éléments d'une voiture pour qu'elle soit assemblée correctement. Officieusement, il maintient ainsi un meilleur contrôle sur les prix de chaque composant.

Ce modèle semble porter ses fruits : la fiabilité des Toyota est mondialement reconnue.

Régis Arnaud, à Tokyo

ANNEXE 11

Inspections et défaillances critiques

CRITICAL FAILURES

Union Carbide's accident at Bhopal in India in December 1984 is well known. What is less known is that the same company experienced an accident at a similar plant at Institute in West Virginia, USA some eight months later. Following the Bhopal incident Union Carbide inspected this plant and found exemplary safety standards in operation. The Company stated that a similar accident could not happen there. However, it did institute some changes including the introduction of a gas leak detection system and increasing the height of the venting tower. The Company's positive view was underwritten by the Occupational Safety and Health Administration's (OSHA) following a positive review of the plant. On the 11th August 1985 the plant experienced a similar accident to that at Bhopal but involving aldicarboxime a less dangerous chemical than metyhl isocanate gas (MIC), which was involved at Bhopal. Following the incident OSHA attended the plant and this time came to the conclusion that this accident was "an accident waiting to happen". Union Carbide was fined \$1.4 million for the "constant, willful, violations" detected. The question that immediately arises is how can two investigations conducted by the same organisation (OSHA) and in such close proximity in time come up with such different conclusions?

This is not an isolated case. During the year preceding the Piper Alpha explosion the Department of Energy's Safety Directorate made three visits to the platform. The last visit was made ten days before the accident and commented that the operator, Occidental, had addressed problems that had previously been identified in the permit to work scheme and shift hand over procedures. As the Cullen report subsequently noted it was failures in these work practices which contributed to the disaster. The Cullen report cites many areas where the Inspector's knowledge of working practices fell short of what was desirable and these factors were implicated in the subsequent disastrous events. Lord Cullen stated "Even after making allowances for the fact that the inspections were based on sampling, it was clear to me that they were superficial to the point of being of little use as a test of safety on the platform." Once again one may ask how this state of affairs came about?

Turning away from the safety arena to the world of finance the collapse of Barings Bank is illustrative. In February 1995 Barings Plc was placed under administration by the High Court following the discovery that Barings Futures (Singapore) Pte had incurred losses of £869 million through the activities of Nick Leason, one of their settlement clerks/dealers. The subsequent investigations conducted by the UK's Board of Banking Supervision and the Singapore Ministry of Finance identified a catalogue of failures within Barings that inexorably led to the disaster. Among these were the fact that Leason was able to operate both as a dealer and a settlement clerk, that there was confusion over who Leason reported to, failures of Barings' management to react to various warning

indicators raised by their own internal audit process and external financial organisations. Collectively these led to the final financial disaster that overcame the bank. Why, one may ask, were the warning signs so systematically ignored?

Many other major accidents reveal similar situations where warnings are ignored, where inspections and audits are incomplete or uninformed, where lethargy within the organisation neglects to address warning indicators. Among these we may include the Challenger disaster, the Southall accident, the King's Cross Underground Fire and others.

Following the Ladbroke Grove railway crash on October 5th 1999 the UK's Health and Safety Executive was asked to review Railtrack's safety management arrangements. Among the many observations made in this report some common themes arose:

- While Train Operating Company's (TOC) produce Safety Cases that are assessed when they are produced the monitoring of performance against commitment is poor.
- There is confusion within the organisation over who is responsible for ensuring TOC compliance.
- Audits often identify poor performance which day to day monitoring fails to identify. These exhibit failures in the Safety Management System.
- Deficiencies identified in earlier audits are often not dealt with.
- Although data is widely collected it is fragmented and can not be combined in such a way as to provide an overall picture and determine whether safety performance is improving or deteriorating.
- The use of risk assessment and prioritisation tools was not well developed thus making it difficult to focus resources where most needed.
- Performance indicators were not structured so they could identify whether performance was improving or not.
- Where incidents arose root causes have tended to be ignored. There was a focus on the severity of the actual accident rather than on the severity of the potential incident.

Pour en savoir plus : http://www.dcs.qmul.ac.uk/research/radar/Projects/Score_Proposal.pdf