Piloter la sécurité

Théories et pratiques sur les compromis et les arbitrages nécessaires

Springer

Paris
Berlin
Heidelberg
New York
Hong Kong
Londres
Milan
Tokyo

René Amalberti

Piloter la sécurité

Théorie et pratiques sur les compromis et les arbitrages nécessaires

Springer

René Amalberti

ISBN 978-2-8178-0368-5 Springer Paris Berlin Heidelberg New York

Springer-Verlag France est membre du groupe Springer Science + Business Media

Maquette de couverture : Nadia Oudanne
Images de couverture : © fkprojects - Fotolia.com
© M.studio - Fotolia.com

Mise en page : DESK – Saint-Berthevin

Avertissement de lecture

Le texte est organisé pour faciliter une lecture à trois vitesses

- des résumés proposés à chaque section, en gras ;
- le texte principal ;
- des encarts pour une lecture par l'exemple.

Sommaire

Avant-propos

Quinze ans se sont écoulés depuis la publication de « La conduite des systèmes à risques »[1]

La sécurité des systèmes complexes n'a pas perdu son actualité, bien au contraire. Pour prendre quelques exemples, citons la vingtaine de catastrophes aériennes mondiales survenant encore chaque année, les presque aussi fréquentes – mais plus retentissantes – catastrophes de la chimie (explosion de l'usine Total AZF à Toulouse en 2001, naufrage du tanker Prestige avec une marée noire sans précédent sur les côtes françaises et espagnoles en 2002, explosion de la raffinerie BP au Texas en 2005, explosion du terminal pétrolier de Buncefield en 2005, mauvais forage de la compagnie pétrolière indonésienne provoquant un volcan de boue ininterrompu à Sidoarjo depuis 2006, explosion de la plateforme BP dans le golfe du Mexique en 2009 avec une marée noire sur tout le sud des États-Unis), les rares mais dramatiques catastrophes du nucléaire (Tchernobyl en 1986 ; Fukushima en 2011), sans oublier les problèmes atteignant les Services publics : les milliers de morts au quotidien d'une médecine décidemment peu sûre, ou les milliers de jeux bancaires dangereux révélés par la crise internationale des subprimes en 2008 et le rebond de la crise de la dette européenne en 2011 (US$ 25,000 milliards évaporés ??). La liste serait trop longue pour prétendre être exhaustive. Mais plus encore que les morts – qui ont plutôt tendance à baisser en proportion – c'est la diversité des milieux concernés qui frappe l'imagination, et la gravité croissante des sinistres, avec leurs immenses répercussions économiques.

On voit là réunies toutes les racines d'un système en équilibre précaire à l'échelle planétaire : produire toujours plus, avec des outils plus complexes, dans des endroits plus difficiles, en générant forcément toujours plus de risques d'accompagnement ; puis

1. Amalberti R (2001) La conduite des systèmes à risques. Paris: PUF, 2e ed, traduit en espagnol : Amalberti R (2009) El control de los sistemas de alto riesgo, Madrid: Modus Laborandi.

convoquer la science pour contrôler ce risque croissant, en cherchant l'alchimie magique qui réglerait au mieux les multiples fonctions d'échanges entre risques contradictoires : accès à l'innovation et nouveaux risques, marchés concurrentiels, libre entreprise et limitation des contraintes légales, sécurité des biens et sécurité des personnes, sécurité immédiate et sécurité sur le long terme, déchets…

J'ai passé ma vie à étudier ces risques, à chercher cette alchimie mystérieuse qui écoperait l'eau d'un bateau qui fait exprès de prendre l'eau. Car la sécurité, c'est d'abord ce paradoxe : on la convoque quand on a déjà pris les risques.

Chemin faisant, je suis passé par plusieurs phases de réflexion pour répondre au problème de « comment améliorer la sécurité et la gestion des risques ». Ce livre est le dernier d'une trilogie qui reflète ce chemin personnel fait de trois aspects complémentaires :

- comprendre et améliorer la gestion individuelle des risques dans les postes de travail des industries à risque (la conduite des systèmes à risques[2]) ;
- changer de point de vue et améliorer la gestion systémique des risques dans l'entreprise (la série des livres coédités à la MSH-CNRS *Grenoble sur les séminaires Risques, erreurs et défaillances, 2001, 2002, 2003 et une série d'articles*[3]) ;
- et enfin, aider à la gouvernance des systèmes à risques avec un modèle intégré de gestion des compromis de sécurité (*ce livre*).

Ces trois aspects complémentaires ont émergé naturellement par la succession de trois époques assez bien séparées de ma vie professionnelle.

- Le premier temps est celui de la recherche universitaire. Bien que médecin de formation initiale, ce temps de vie universitaire a vraiment débuté avec ma deuxième formation en psychologie cognitive, et mon affectation en 1982 dans un poste permanent de chercheur d'un laboratoire militaire (l'Institut de médecine aérospatiale). Immédiatement confronté aux accidents aériens, j'ai orienté mon parcours vers l'erreur humaine. Ce parcours m'a servi à nourrir la théorie sur la gestion individuelle des erreurs et à établir les bases du compromis cognitif.
- Le second temps a été celui de l'action interdisciplinaire. À la fin des années 1980, j'ai eu la chance de travailler étroitement avec Airbus, Air France et l'OACI (Organisation de l'aviation civile internationale, ICAO en anglais) à l'élaboration et à la diffusion mondiale des premiers cours de CRM (*Crew-Resources Management*). Cette connaissance du milieu aéronautique a favorisé mon détachement aux autorités européennes de l'Aviation civile (*JAA Joint-Aviation Authorities*) comme responsable sécurité et facteurs humains jusqu'en 1999. Dans cette position, j'ai

2. Amalberti R (2001) La conduite des systèmes à risques. Paris: PUF, 2e ed.

3. Amalberti R, Fuchs C, Gilbert C (2001) Risques, erreurs et défaillances. Grenoble: MSH Vol. 1.

Amalberti R, Fuchs C, Gilbert C (2002) Conditions et mécanismes de production des défaillances, accidents, et crises (Vol. 2). Grenoble: MSH-CNRS.

Amalberti R, Fuchs C, Gilbert C (2003) La mesure des défaillances et du risque (Vol. 3). Grenoble : MSH-CNRS.

Amalberti R. (2001). The paradoxes of almost totally safe transportation systems. Safety Science 37: 109-26.

Gilbert C, Amalberti R, Laroche H, Pariès J (2007) Toward a new paradigm for error and failures. Journal of Risk Research 10: 959-75.

appris que la sécurité était un objet interdisciplinaire, mais compris de façon différente voire parfois antagoniste par chaque discipline. J'ai surtout constaté, et testé, qu'il était illusoire de prétendre réduire totalement ces différences qui reposent sur des modèles profondément ancrés, chacun avec une logique raisonnée, même si elle est en opposition avec d'autres logiques (économiques, politiques, humaines, techniques, et mêmes culturelles avec les différences États-Unis/Europe sur l'esprit des règlements). J'en ai tiré une façon de concevoir les règlements et les approches de sécurité, que j'ai pu tester et appliquer avec les partenaires américains sur l'élaboration de la plateforme commune de règlements facteurs humains en aéronautique civile.

- Le troisième temps est celui de l'action sur la gouvernance. En multipliant depuis la fin des années 1990 les postes de conseiller (risques environnementaux, énergie, sécurité des soins) et de direction de programmes de recherche sur la sécurité (énergie, transport), j'ai compris combien la sécurité est un objet brûlant de crise, paradoxalement placé dans un océan de vide théorique chez les politiciens et les dirigeants. Ces derniers, sous pression des médias et tournés vers le court terme, sont le plus souvent bien trop optimistes sur leurs résultats, convaincus que la seule application d'une politique de contrôle-sanction renforcée sur les acteurs de première ligne est LA solution aux problèmes, alors que les preuves se multiplient pour montrer que cette politique est justement génératrice des crises que ces mêmes politiciens et dirigeants redoutent. Ce paradoxe, ses conséquences, et les modèles de pilotage du risque sont le cœur de cet ouvrage.

Une évolution… ou une révolution ? Compromis et suffisance

Pour différentes raisons géopolitiques, le monde change assez rapidement en ce début de XXIe siècle ; ce changement d'époque est très favorable aux porteurs d'idée de rupture en matière de sécurité, à l'échelon de l'individu comme à celui des organisations. Le temps des facteurs humains traditionnels fondés sur les limites et les performances humaines se termine en matière de sécurité. Place aux modèles de couplage dynamique (*Joint-Cognitive Systems*) et aux modèles systémiques. On commence seulement à lire les effets de cette rupture en matière de gouvernance du risque.

L'accident de demain, rare mais sans doute encore plus dramatique, sera un accident où les règlements existaient pour éviter le problème, où peut-être même personne n'aura fait une erreur caractérisée, où aucun système n'aura été vraiment en panne, mais où l'érosion aura affaibli toutes les composantes ; l'ampleur de variation des conditions de fonctionnement d'un jour aura suffi pour dépasser les seuils de couplage tolérables. Paradoxalement, la sécurité du système aura tout misé sur des procédures rassurantes, qui l'auront fait progresser, puis l'auront mis en confiance, puis se seront affaiblies au fil du temps à la fois par l'érosion des défenses, l'augmentation des tolérances, et la perte d'expertise à gérer des situations difficiles. La nouvelle idée de **résilience** est à comprendre

dans ce sens : l'augmentation de la **sécurité réglée**, imposée par les règlements, se fait forcément au prix d'une rigidité accrue, d'une volonté d'immense standardisation des techniques et des hommes, et finalement d'une adaptation moins grande des opérateurs aux surprises (impact négatif sur la **sécurité gérée**, basée sur l'expertise des opérateurs et que l'on peut associer à l'idée de résilience). L'art de l'intervention de sécurité réussie consiste à régler le compromis et les arbitrages entre le bénéfice de cette sécurité réglée et la perte qui va en résulter pour la sécurité gérée.

La notion de compromis soutient tout l'édifice théorique et pratique de ce livre. Le compromis est tout autant le nécessaire compromis cognitif ou intellectuel « microcentré » que le travailleur doit régler en permanence entre la demande extérieure, ses propres savoir-faire, les tâches et motivations concurrentes, son état physiologique de fatigue et de stress, que le compromis de réglage « macrocentré » qui modélise les arbitrages plus ou moins conscients entre performance et sécurité au niveau de la gouvernance des systèmes complexes.

- Le premier compromis, dit microcentré, se situe à l'échelle de l'opérateur. Il renvoie à un des derniers points particulièrement méconnus de la psychologie humaine car il mobilise l'ensemble du contrôle intellectuel et se trouve naturellement labile et révisable, de sorte qu'il échappe à la plupart des méthodologies d'étude de la psychologie traditionnelle qui postulent une certaine stabilité pour capturer et mesurer une capacité intellectuelle de base (mémoire, attention, vigilance…). Ceci dit, la psychologie a beaucoup progressé, et à défaut de caractériser le réglage du compromis cognitif à chaque instant, on sait aujourd'hui caractériser les variables qui le modulent en temps quasi réel. Tout l'ouvrage précédent sur la conduite des systèmes à risques était consacré à cette modélisation, et à ses conséquences très importantes en matière de conception d'assistance sûre à la conduite. On les reprendra dans ce livre sous forme de résumé.
- Le second compromis, dit macrocentré, est le cœur innovant de ce livre. Il porte sur les arbitrages entre performance et sécurité dans le pilotage du risque au niveau de la gouvernance de l'entreprise. On parle de décisions de sacrifice. Les polémiques sont quotidiennes sur ce type de compromis, et entretiennent la presse à scandale. Ce livre donne les clés de cet arbitrage et des sacrifices qu'il nécessite. Presque toutes ces clés de ce compromis sont surprenantes et souvent politiquement incorrectes en première analyse, mais finalement faciles à comprendre après réflexion. Parmi les résultats les plus paradoxaux, le lecteur découvrira notamment que l'institutionnalisation de la sécurité est une propriété émergente des systèmes déjà sûrs, et que les stratégies d'interventions doivent significativement varier dans les méthodes et les outils en fonction du niveau de sécurité de l'entreprise, et être de plus en plus lourdes au fur et à mesure que la sécurité s'améliore. Le niveau de sécurité possède en effet cette étonnante propriété de ne jamais être suffisant, et même d'engendrer une exigence sociétale qui augmente en parallèle des progrès réalisés. C'est une variable sans maximum, et toute amélioration rend le jugement d'autrui encore plus sévère sur les quelques cas d'insécurité persistants. Le lecteur découvrira aussi que choisir une stratégie de sécurité inadaptée, notamment trop ambitieuse, génère finalement de l'insécurité.

La continuité des modèles entre les deux types de compromis, micro et macro, individus et organisations, est étonnamment grande, comme si les mêmes modèles pouvaient se décliner dans une perspective fractale. La performance psychologique en condition réelle et journalière des opérateurs, le degré d'attention de ces derniers, leur pertinence de choix, apparaissent toujours à l'observateur comme imparfaits, presque décevants en regard de ce que l'on croit que les gens sont capables de faire, et même de ce qu'on a pu directement observer de leurs entraînements. La performance sécuritaire des entreprises est elle aussi presque toujours décevante, toujours inférieure à ce que le discours et les organisations laissent présager.

Dans les deux cas, ce jugement est hâtif et inexact. Les performances sont certes non maximales, mais restent suffisantes compte tenu des exigences des normes du travail.

Par exemple, on n'exige pas d'un automobiliste de conduire strictement au centre de sa chaussée (ce qui pourrait pourtant paraître idéal) ; on construit au contraire son environnement de sorte qu'il puisse conduire dans un espace élargi où il peut même utiliser des degrés de tolérance complémentaires s'il ne vient personne en face. Cette construction partagée, pensée et obtenue à la fois par consensus technique (choix d'une largeur de la chaussée, ergonomie de la route), et par consensus social (consigne de verbalisation donnée à la police sur ce qui est ou non à réprimander) permet de répondre raisonnablement à l'exigence de sécurité et renvoie à cette idée de « suffisance » : « le contrat social du conducteur est de rester sur sa moitié de chaussée », on n'exige pas plus de lui, cela « suffit », et on ne le verbalisera pas s'il atteint cet objectif. Cette vision s'applique partout dans le monde du travail, et paradoxalement sert la sécurité au lieu de la desservir, comme pourrait le laisser croire le laxisme qu'elle suggère : en effet, plus la chaussée est large, moins l'exigence de concentration de conduite pour le conducteur est grande, moins il se fatigue, et plus il dispose de marges pour récupérer un impondérable ou une surprise (*la construction de la suffisance construit aussi la sécurité).*

La sous-optimalité permet ainsi d'installer un compromis, de traiter en parallèle d'autres objectifs (pensées privées, autres pôles d'intérêts…), voire tout simplement de s'épargner et économiser des efforts inutiles en réservant son énergie pour accroître d'autres dimensions de sa performance, pour durer (être aussi efficace en début qu'en fin de vacation de travail), ou pouvoir répondre aux aléas et aux coups durs, bref de vivre en symbiose avec une demande plus globale de la société, qui ne peut jamais se résumer simplement à UN objectif qui serait unique, la sécurité immédiate par exemple.

D'ailleurs, la sécurité n'a jamais fait survivre les entreprises ; l'absence de sécurité peut les tuer, mais en aucun cas la sécurité peut apparaître comme le seul but à poursuivre.

Cette idée de SUFFISANCE vient comme un complément naturel de l'idée de COMPROMIS et sera souvent explicitée et débattue dans le livre pour en comprendre l'installation, et surtout les implications en matière de construction des règlements et d'audit des entreprises. Comment se construit cette alchimie de consensus technique et social sur ce qui est « suffisant » dans l'installation puis l'interprétation de la norme ?

Comme toujours un travail n'est jamais le fruit d'une seule personne. Les compagnons de route de longue date sont d'abord à citer pour leur continuelle contribution aux débats ; en France : Jean-Michel Hoc, Jean Pariès, Maurice de Montmollin et Jacques Leplat, et à l'international Jens Rasmussen, Jim Reason et Eric Hollnagel. Tous sont restés des

relations proches et des critiques et inspirateurs de mes travaux. Puis tous mes thésards qui ont fait une partie significative du travail de terrain (avec un hommage particulier à Gaël Morel et ses travaux sur la pêche professionnelle en haute mer). Je ne peux citer tous les autres amis internationaux dans tous les milieux académiques et industriels que j'ai fréquentés, et qui m'ont pénétré de leur expérience et de leurs propres modèles. Je mentionnerai particulièrement ma part d'aventure dans la montée en puissance de l'Institut puis de la Fondation pour la culture de sécurité industrielle (ICSI/FOCSI) qui m'a permis non seulement de mieux pénétrer encore les arcanes de la grande industrie et ses enjeux de sécurité, mais peut-être plus encore de côtoyer des personnes d'une immense expérience ; je pense particulièrement à René Deleuze et à Ivan Boissières.

Une des richesses de cette expérience réside indiscutablement dans la pluralité d'influences et de milieux, qui vont de la recherche de tradition francophone et anglo-saxonne à la gouvernance politique, et de l'aviation à la santé, en passant par la route, la pêche professionnelle et la grande industrie. Après tout, la science n'est souvent qu'une affaire de synthèse, et la plus grande contribution de cet ouvrage est peut-être justement de proposer un reflet qui intègre des approches et des milieux qui ne se côtoient pas, qui se caricaturent mutuellement, dont chacun pense que son cas est si particulier qu'il ne peut apprendre des autres, mais dont la somme vue par un œil extérieur peut faire émerger des théories et propriétés communes.

Effet d'âge encore, le lectorat potentiel s'est agrandi, et ce livre devrait exister rapidement en trois langues, français, anglais et espagnol.

Bref, ce livre tente de donner les clés de la sécurité des systèmes à risques au XXI^e^ siècle, en vulgarisant au maximum les modèles tout en conservant un niveau de précision scientifique suffisant, pour une cible de lecteurs enseignants, consultants ou industriels susceptibles d'appliquer les modèles.

Le chemin théorique, même s'il n'est jamais achevé, est bien balisé, de même que la vision transversale des liens existants entre les différents courants mondiaux. Le lecteur y trouvera aussi une liste et une lecture critique de très nombreuses références.

Le chemin pratique de l'intervention de sécurité est lui aussi tracé, mais volontairement limité aux principes généraux sans portfolio d'outils. Je laisse ces développements d'outils à charge d'autres collègues. Cette distance à des kits d'évaluation sur étagères n'est pas qu'une énième dérobade de scientifique pour les problèmes de terrain ; sans minimiser leur intérêt, ne pas mettre l'accent sur eux, c'est mettre l'accent ailleurs, et notamment sur la décision politique qui précède leur emploi. Or le succès en cette matière de gouvernance du risque est avant tout une affaire de choix de stratégie à haut niveau, et non d'outils de mesure et de questionnaires faciles à utiliser mais masquant souvent l'essentiel.

Lecteurs, accrochez-vous, le texte est rempli de contre-évidences, certaines dérangeantes, d'autres rassurantes, mais toutes centrales pour une gouvernance réussie du risque.

Bonne lecture. Les critiques et les débats sont toujours les bienvenus.

René Amalberti

1

La demande de sécurité et ses paradoxes

Le monde exige toujours plus de sécurité. Mais cette demande varie d'un système à l'autre en fonction de son cycle de vie. La pression sur la sécurité est souvent maximale en fin de cycle, paradoxalement au moment où le système atteint la quasi-apogée de son niveau de sécurité.

Un monde en demande de sécurité

Les problèmes de sécurité dans notre société n'ont jamais été autant à l'ordre du jour. Ce n'est pas tant le nombre des accidents que leur médiatisation mondiale, immédiate et intensive, qui fait peur aux citoyens des sociétés riches qui ont tout à perdre dans l'écroulement de leur confort, de leur santé, et de leurs valeurs.

Pire, il s'ajoute une multiplication d'apôtres de l'apocalypse (ou de *whitsleblowers*)[1], très médiatisés, qui jettent prédictions de malheur et confusion en considérant tous les accidents – et encore plus dans leur agrégation multiorigines – comme les symptômes d'une société ayant perdu tout contrôle de sa sagesse et de son droit à renoncement (périls d'origines industrielles, catastrophes naturelles, « suicides » sociétaux comme le tabac, l'alcool ou la route, séismes économiques). Sans surprise, cette situation a fait de ce thème une variable incontournable et croissante des politiques publiques… et des élections.

En réaction, les instances publiques nationales et internationales ont créé des agences, des nouvelles tutelles et des bureaux dédiés à la sécurité ; ces mêmes instances ont multiplié les lois et les décrets en lien avec la sécurité ; l'argent de la recherche a été fléché vers ce domaine avec rapidité (augmentation de près de 300 % des crédits recherches des états occidentaux sur ce thème depuis 1992). Les formations universitaires et continues suivent le même chemin inflationniste, les petites et moyennes entreprises et

1. Lire : de Kersasdoué J (2007) Les prêcheurs de l'apocalypse, pour en finir avec les délires écologiques et sanitaires. Paris : Plon.

les cabinets de consultances spécialisées sur ce créneau de l'intervention et du conseil en sécurité sont de plus en plus nombreuses (+ 72 % aux États-Unis entre 1985 et 2000) pour répondre à des demandes exponentielles d'audits et de rapports d'états sur les risques (+ 430 % depuis 10 ans).
C'est cette émergence du concept « sécurité » qui a finalement donné les vraies lettres de noblesse scientifique à ce sujet, longtemps traité comme une simple variable d'accompagnement des évolutions technologiques.
Mais l'éclairage public n'a pas que des avantages ; le marché créé est aussi polémique que juteux, et présente encore de nombreuses fragilités.
Les systèmes se mettent souvent à tourner à deux vitesses, avec d'un côté une approche vertueuse de qualité et de sécurité enkystée et drapée dans ses nouveaux bureaux, pleine de certitudes sur les contraintes à imposer au système, et de l'autre une production sous pression du marché, dont la règle du FBC (*Faster-Better-Cheaper*)[2] reste la seule solution de la survie commerciale et du succès. La modélisation des décisions de sacrifice et les interfaces de gouvernance nécessaires pour arbitrer entre les valeurs de sécurité et les valeurs de production sont parmi les points les moins connus de la gestion de la sécurité. Il faut bien reconnaître que mourir économiquement est aussi un accident ; et l'opposition entre sécurité formelle et survie économique n'est peut-être pas aussi grande qu'on l'imagine, mais on manque crucialement de regard scientifique, global ou systémique sur la question.
En bref, on a rapidement progressé sur le détail (les erreurs), encore plus rapidement progressé sur les idées simples et les préconisations locales de sécurité (qui se réglementent et se vendent), mais on reste presque totalement démuni de modèle cadre de gestion stratégique de la sécurité.
Est-on allé trop loin sans tenir assez compte des contraintes de terrain ? Trop vite ? La menace de sécurité impossible des industries à risques est-elle au niveau annoncé ? Est-ce un vrai péril de société ? Peut-on traiter la sécurité comme un problème générique, indépendamment de sa source ? Quels sont les fondements scientifiques disponibles ?
Et d'ailleurs pour finir, est-ce un champ scientifique relevant de connaissances d'abord techniques, ou un champ relevant d'abord du social ?

Question de périmètre : quels systèmes concernés, pour quelle démarche de sécurité

Ce livre traite de l'(in)sécurité des grands systèmes sociotechniques (pôles énergétiques, transports publics, services : banques, médecine). La sécurité de ces systèmes n'a pas perdu son actualité, bien au contraire.

2. *(*FBC : *Faster-Better-Cheaper),* expression venue de la NASA qui en avait fait sa devise avant le deuxième accident de la navette.

La liste des catastrophes serait trop longue pour prétendre être restituable dans cet ouvrage. Mais plus encore que les morts (qui ont plutôt tendance à baisser en proportion), c'est la diversité des milieux concernés qui frappe l'imagination, et la gravité croissante des sinistres.
Ces « grands systèmes sociotechniques » présentent tous trois caractéristiques :
- les processus à contrôler sont dynamiques, ils évoluent pour eux-mêmes mais peuvent être infléchis par l'intervention humaine ;
- ils restent sous le contrôle d'hommes « au contact du processus » et dans la boucle de « management » ; en anglais, on emploie le terme de *sharp end* pour les premiers, et de *blunt end* pour les seconds[3]. Cette propriété de contrôle humain horizontal et vertical ne disparaît pas quel que soit le niveau de technologie employé, même si le nombre d'opérateurs tend à se réduire avec les solutions innovantes ;
- ils sont à risques ; le risque est la mort physique des acteurs et/ou du système lui-même (notamment mort économique). Cette mort peut être isolée mais s'accompagne le plus souvent d'effets collatéraux.

Les solutions « de sens commun » pour sécuriser les systèmes complexes ne manquent pas

La prise de risque génère la sécurité, tout comme l'eau envahissant le bateau exige d'écoper. Le discours de la fiabilité est à cet égard limpide : le monde comporte des ***dangers*** pour l'activité des êtres humains (énergies, matières, objets, produits). Le ***risque*** correspond à la fréquence d'exposition des humains à ces dangers, et aux conséquences de cette exposition ; le risque est négligeable et peut sans doute être accepté pour un danger très grave mais très exceptionnel (être blessé par une météorite) ou un danger fréquent dont les conséquences sont mineures (une crise de foie pour avoir mangé trop de chocolat). Il est au contraire inacceptable pour un danger fréquent avec des conséquences sévères (doigt coupé pour un menuisier) ou un danger plus rare mais dont les conséquences sont majeures (accident nucléaire).
Pour ces cas jugés inacceptables, la sécurité consiste d'abord à diminuer l'exposition au risque chaque fois que c'est possible, puis à protéger les opérateurs et les citoyens contre ce risque chaque fois que l'exposition à ce risque est jugée inévitable pour des raisons commerciales ou publiques. Les systèmes à risques entrent dans cette seconde catégorie où l'on a accepté de s'exposer au risque (pour d'autres bénéfices) et où l'objet de la sécurité consiste à trouver des solutions d'évitement – non pas du risque – mais des accidents.
Depuis des millénaires, l'espoir d'amélioration continue de la sécurité repose sur une série de fondamentaux qui ont peu varié, tant ils apparaissent comme des évidences de bon sens ; on peut en repérer cinq récurrents dans nos pensées et nos agissements.

3. Reason J (1990) Human error. Cambride University Press.

1re idée : pour le responsable (l'entreprise, le secteur industriel), la sécurisation doit répondre à quatre buts, certains publics et avouables (les deux premiers), d'autres plus personnels (les deux derniers) :
- réduire les accidents (attente de progrès mesurables) ;
- montrer au(x) client(s), et plus globalement à la société, que la volonté de faire mieux est présente, et s'affiche à travers des efforts continus ;
- adoucir les postures et attitudes critiques des observateurs, citoyens, clients, riverains, en espérant une reconnaissance des efforts consentis et du bilan obtenu ;
- réduire le spectre de survenue de grandes crises socioéconomiques postaccidents (on pense par exemple à la crise politique du sang contaminé en France, à la vache folle au Royaume-Uni, à la remise en cause de la NASA après les accidents de la navette, à la très forte instabilité politique ayant suivi l'ouragan Katrina aux États-Unis ou la catastrophe de Fukushima au Japon).

2e idée : le chemin de la sécurité passe par des actions bien connues, démontrées dans des industries et secteurs devenus sûrs (les « bons élèves », par exemple le nucléaire et l'aviation). Nous vivons avec la notion d'un système de solutions et d'une voie finale unique de sécurité qui serait commune à toutes les industries : la meilleure sécurité serait obtenue pour tous par la mise en route des mêmes outils réputés performants dans les différentes entreprises à succès.

3e idée (raffinement de la précédente) : la conformité à une marche « idéale » procédurale fait partie de la voie obligée de sécurisation. La réduction de la dispersion des pratiques professionnelles par l'introduction de procédures conduit naturellement à une meilleure sécurité. Le retour d'expérience, la participation active des acteurs et du management dans la surveillance des écarts et plus globalement la démarche qualité sont les outils habituellement retenus pour cette mise en conformité.

4e idée (qui doit un grand merci à Reason) : les erreurs – par définition involontaires – sont tolérables et de toute façon peu ou prou inéluctables, même si le débat n'est pas purgé sur le fait qu'elles soient accessibles, ou pas, à des interventions de sécurité et leur réduction de fréquence. Le système doit accepter les erreurs comme le verso indissociable de l'intelligence humaine, et développer des stratégies pour gérer ces erreurs tout en évitant leurs conséquences. Les barrières s'organisent en trois secteurs complémentaires : *Prévention* (éviter le risque), *Récupération* (gérer le risque et éviter l'accident), et *Atténuation* (accepter l'accident mais ne pas en mourir, réduire l'impact). La distinction entre erreurs patentes (des acteurs de première ligne) et erreurs latentes (de la gouvernance du système) est un autre point essentiel proposé par Reason, soulignant l'importance de cibler une partie des actions sur le management et pas simplement sur les acteurs de première ligne.

5e idée (un effet de nos sociétés juridiques ?) : les erreurs sont éventuellement tolérables, mais les écarts volontaires à la norme et les violations restent considérés comme des actes délibérés et injustifiables.

Hélas, le caractère de « bon sens » de ces cinq idées est semé d'embûches dans leur déploiement et le bénéfice que l'on en tire. Le bénéfice de chacune de ces idées se vérifie, mais il est souvent limité à un domaine relativement restreint d'application.
Pour bien comprendre ce phénomène paradoxal, ce premier chapitre propose une macroanalyse de la gouvernance du risque, en étudiant les modèles décrivant les changements de sécurité dans les cycles industriels et leur progression vers leur apogée de sécurité. Plusieurs conséquences importantes sont suggérées en termes de macrogouvernance du risque. Ces conséquences guident la suite du livre.

Cycles de vie des systèmes sociotechniques et place paradoxale du temps de la sécurité

Tout système, biologique ou technique, finit par mourir. Le besoin ou la fonction continuent à être assurés, mais les moyens de réalisation de ces besoins et fonctions changent régulièrement.
Par exemple, la mobilité et les échanges sont une clé du commerce et un besoin constant des sociétés depuis l'Antiquité. Une de ces plus récentes modalités est d'être transporté dans les airs. Les ballons dirigeables ont représenté une façon de faire ; les avions pilotés une seconde façon ; les drones ou avions automatiques en sont déjà une troisième façon. Chaque façon satisfait le même besoin et correspond à un système sociotechnique particulier, un couplage organisationnel spécifique, et subit un cycle de vie particulier. On peut aisément montrer que ces cycles de vie sont aujourd'hui sensiblement de la même durée que le cycle de la vie humaine : entre 30 ans pour les morts précoces et un peu plus de 100 ans pour les systèmes les plus robustes. Ces cycles de vie ont été plus longs dans le passé, atteignant parfois plusieurs siècles, mais l'accélération de l'innovation dans notre société a définitivement emballé le système.
Chaque cycle fait passer le système considéré d'une phase de naissance à une phase de vieillissement. Le modèle de cycle présenté dans cette section s'inspire de nombreux travaux, notamment de ceux du sociologue Hughes[4] dont le terrain d'étude privilégié a été pendant longtemps le développement de l'industrie de l'énergie électrique.
Le modèle décrit trois phases[5].

4. Hughes T (1983) Networks of power-electrification in Western countries. Baltimore: John Hopkins Univ Press.

5. Amalberti R (2006) Optimum system safety and optimum system resilience: agonist or antagonists concepts? In: Hollnagel E, Woods D, Levison N. Resilience engineering: concepts and precepts, Aldershot, England: Ashgate: 238-56.

Une phase de créativité initiale souvent silencieuse pour le grand public

Les nouveaux systèmes naissent avec quelques individus portant l'innovation ; la sécurité n'est pas une priorité à ce stade, même si les accidents sont hautement probables dans ces phases initiales de réglage de l'invention (immaturité). Mais il faut dire que ces accidents tuent surtout leurs inventeurs, avec des effets collatéraux limités alors que le nombre de prototypes est forcément réduit voire confidentiel.

La découverte de la transfusion sanguine et l'ouverture d'un cycle de vie industriel. La transfusion sanguine devient possible après 1900 à la suite de la découverte du système ABO et de la compatibilité des groupes sanguins par Karl Landsteiner (étape d'innovation). La période de 1910 à 1930 voit suivre la première étape d'optimisation : les progrès qui se concentrent sur les conditions de la commercialisation à grande échelle, l'organisation du réseau de collecte du sang, la conservation du sang, et le développement d'applications cliniques.

Une phase d'optimisation et de profits économiques, de loin la plus longue, dit « temps de la qualité »

Elle s'étend sur plusieurs dizaines d'années. C'est le cœur de la vie utile du système, entre naissance de l'invention et sclérose du vieillissement. À ce stade, l'industrie absorbe l'innovation, la standardise, l'optimise, et la généralise pour un objectif de rentabilité (économique, éthique, bien-être). Cette phase procède en deux temps. Le premier temps règle les problèmes les plus importants de l'innovation, en la rendant utilisable commercialement. À ce stade, la sécurité évolue très rapidement, en parallèle de chaque amélioration technique.

L'exemple des cycles dans le transport aérien
Après les travaux pionniers de la fin du XIX^e^ siècle sur les ballons, et une mise au point difficile d'une version civile développable à grande échelle (1899-1906), les ballons dirigeables, particulièrement avec l'industriel allemand Zeppelin, vont représenter pendant près de 30 ans la top technologie pour faire voler fret et passagers. Mais cette solution va très vite manquer de futur, en ne trouvant pas les ressorts d'une technologie alternative à l'usage de l'hydrogène particulièrement inflammable. La pression médiatique et politique aidant, l'accident du Zeppelin Hindenburg en 1936 va sonner brutalement le glas de cette technologie au profit des avions, une technologie alternative pour transporter les passagers à grande échelle. Pendant 20 ans (1935-1955), les avions de ligne s'avéreront objectivement plus dangereux que les derniers Zeppelin, mais ils auront pour eux la croissance mondiale, et un incroyable rythme d'innovation (arrivée des jets, des automatismes…) qui leur donnera une

crédibilité sur leur potentiel (valeur positive d'espoir) et permettra une tolérance aux (nombreux) accidents résiduels de cette période (ce qui n'était plus le cas pour une technologie usée prématurément comme celle du Zeppelin).
Paradoxalement, ce cycle ouvert dans les années 1935 est à nouveau en train de se terminer. L'aéronautique civile classique avec des pilotes aux commandes approche de sa fin, et devrait subir une rupture technologique de très grande envergure vers les années 2030/2040 avec l'arrivée annoncée d'un guidage satellitaire complet du système. Les professions changeront, de même que toute l'économie du système, mais on continuera à prendre des avions pour aller de A à B (continuité de la fonction).

Un modèle général décrivant les étapes du cycle de vie des grands systèmes industriels. Les grands systèmes, à leur échelle, naissent et meurent – on parle de cycle industriel – en connaissant un cours de vie largement reproductible d'un système à l'autre (Hughes, 1983). Mais la mort du système n'est pas la mort de la fonction du système ; la fonction renaît de ses cendres dans une nouvelle technologie issue d'une rupture technologique : le cycle reprend, souvent sous une forme différente de couplage.

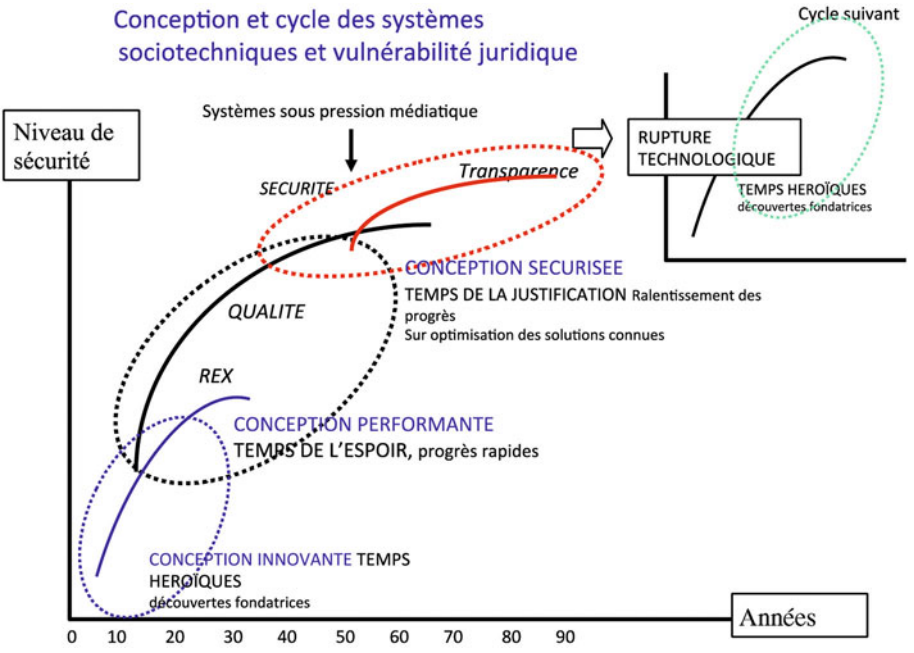


Fig. 1

À ce stade de commercialisation de l'innovation, la recherche très amont est freinée, les inventeurs sont gentiment mis dans des positions honorifiques, de fait écartés de l'entreprise pour laisser la place à des ingénieurs et des commerciaux capables de transformer l'idée de départ en produit commercial efficace et fiable. On évite ainsi les interventions trop

défensives des inventeurs qui protègent leur « bébé », et une activité trop brownienne d'inventions alternatives qui pourrait disperser les efforts, consommer les ressources, et jeter la confusion dans l'image commerciale du produit que l'on veut lancer.
Le second temps correspond au temps de la qualité ; la démarche qualité optimise de plus en plus le produit, introduit le retour d'expérience, la rigueur dans les procédés ou protocoles pour satisfaire le client ; elle efface progressivement les défauts initiaux pour satisfaire au mieux le client. La contrainte réglementaire augmente en parallèle. Hale et Swuste[6] distinguent trois niveaux de règles représentant aussi trois caractéristiques des politiques de gestion des risques à ce stade :

- introduction de règles sur le produit définissant des objectifs à atteindre ou ne pas dépasser selon la matière considérée, par exemple une concentration maximale de toxique admissible, ou le respect de la règle ALARA (*As Low As Reasonably Practible*), ou encore le fait que de multiples règlements aéronautiques mentionnent que la situation ne doit *pas exiger* des *compétences exceptionnelles de la part des pilotes* ;
- introduction de règles sur le processus imposant une organisation de contrôle à mettre en place et à faire respecter (qui, sur quoi, quand, où). Par exemple, une compagnie aérienne doit se doter d'un système de retour d'expérience, administré par une cellule indépendante ;
- et introduction de règles sur le processus imposant un résultat : par exemple un port de lunettes obligatoire par les opérateurs, ou la possession d'une licence avec un examen médical pour le personnel.

Les accidents sont de moins en moins nombreux. La sécurité continue à évoluer en parallèle des optimisations mais elle ne fait pas l'objet d'un bureau ou d'une direction spécifique ; elle est un simple produit de l'optimisation continue. La raison en est simple : pendant toute cette phase, la justice est encore relativement clémente. C'est un temps privilégié de symbiose entre résultats économiques, satisfaction du public, progrès de sécurité et tolérance aux accidents. Les procès sont rares, et quand ils ont lieu, les condamnations et indemnisations restent modérées. La défense (de l'industrie) à beau jeu en plaidant que l'accident est survenu faute de connaissances suffisantes. Souvent d'ailleurs, la situation accidentogène ne pourrait plus se reproduire au moment du procès, par le seul fait des découvertes et des progrès réalisés entre le temps de l'accident et le temps de la justice (plusieurs années en général).

Une phase d'optimisation finale, dite « temps de la sécurité »

Les progrès se ralentissent et le système devient balistique (*Hugues parle de « momentum incontrôlé »*) en tombant souvent dans des sur-optimisations locales au détriment d'une vision stratégique globale. Le nombre de règlements augmente rapidement, et la nature de ces règlements est de plus en plus réactive aux évènements. La sanction d'un tel accroissement est généralement une augmentation des contradictions légales et des règlements faiblement utiles.

6. Hale A, Swuste A (1998) Safety rules: procedural freedom or action constraint? Safety science 29: 63-177.

La fabrique du droit est de plus en plus lourde et complexe (*Le Monde*, 27 janvier 2007), et les règles de droit enflent démesurément dans les sociétés occidentales, en écho d'une demande publique de plus en plus exigeante. Le « recueil annuel de l'assemblée » (française) faisait 1 300 pages en 1990 ; il en comptait 2 500 en 2006.

À ce stade, les accidents sont devenus rares, voire très rares, mais sont beaucoup plus insupportables pour l'opinion publique. Le poids du management grossit ; les directions de la sécurité remplacent ou viennent compléter les directions de la qualité. Des cellules de crises apparaissent, parce que les crises elles-mêmes se font plus fréquentes et dévastatrices. Cette situation génère deux paradoxes difficiles à gérer et qui vont causer à terme la mort du système :

- les pires problèmes de sécurité (en termes d'image de l'entreprise) sont ressentis alors que les efforts n'ont jamais été aussi grands pour la sécurité et que les accidents n'ont jamais été aussi peu nombreux. Les systèmes ainsi devenus très sûrs deviennent en même temps plus fragiles ;
- la société demande plus de transparence sur le risque réel, mais ne sait pas gérer cette transparence ; la possession de l'information rend en retour cette société civile plus intolérante à tous les problèmes résiduels ; plus le public dispose de l'information, plus il est pris de doute sur ce qu'on lui cache derrière cette information. Cette posture de défiance rend difficile le déploiement des systèmes d'informations trop transparents, et freine en retour la sécurisation réelle des pratiques.

Un bon exemple de ces réactions paradoxales de fin de cycle

Pendant le mois d'août 2005, la télévision française renvoie, à seulement quelques semaines d'intervalle, l'image de plusieurs accidents aériens majeurs : la série commence le 2 août avec l'accident d'un Airbus A340 d'Air France à Toronto, miraculeusement sans victimes grâce à une évacuation réussie au sol ; le compte se poursuit avec un accident de charter qui amerrit au large de Palerme avec les deux moteurs coupés (ATR-72 de Tuninter), heureusement à nouveau avec survivants (23 sur 39) ; on suspecte un plein fait avec du mauvais carburant, ce qui n'est guère rassurant pour la confiance dans ces compagnies charters. À peine une semaine plus tard, un autre accident charter survient le 14 août, avec un Boeing 737 d'Helios Airways qui percute une montagne près d'Athènes ; les pilotes ont apparemment suffoqué à un manque d'oxygène totalement incompréhensible ; et, à peine quelques jours plus tard, le 16 août 2005, survient le dernier et plus émotionnel des accidents de cette série. Il s'agit de l'accident du vol charter 708 de la West Caribbean Airlines transportant des Français de la Martinique, tous quasiment du même village. L'avion s'écrase dans la jungle vénézuélienne par le fait de conditions météorologiques déplorables et d'une gestion d'équipage très déficiente. L'émotion est immense dans le grand public, déjà sensibilisé l'année d'avant avec l'accident du charter touristique de Flash Airlines au départ de Charm-el-Cheick, qui avait tué 135 passagers français en retour de vacances.

La polémique enfle rapidement à la suite de révélations sur l'entretien des avions charters, l'autorisation de voler, sur le manque d'information sur les compagnies dangereuses. La DGAC (Direction générale de l'aviation civile, *French CAA*) annonce rapidement des dispositions plus sévères de contrôle des compagnies charters, et la mise à disposition d'une liste de compagnies charters « à éviter » (liste noire).
Dans les mois qui suivent, les passagers des compagnies charters montrent des attitudes extrêmes ; à plusieurs reprises, ayant été informés d'un dysfonctionnement causant un retard, ils refusent d'embarquer ou demandent à débarquer, créant à chaque fois des polémiques sur le vol et le remboursement des billets. Paradoxalement, l'analyse technique de ces cas montre que les compagnies appliquent en fait strictement le règlement (ce qu'elles ne faisaient pas avant) ; au lieu de prendre le moindre risque les équipages suivent toute la procédure, informent les autorités et les passagers dans une transparence totale.
Deux ans plus tard, les compagnies sur la sellette qui avaient fait des efforts, particulièrement les charters, irritées de subir ces incompréhensions, sont parfois retombées dans leur travers d'en dire le moins possible aux passagers et aux autorités.

On assiste aussi dans cette dernière phase à l'intensification des outils et méthodes qui se sont avérés jusque-là porteurs des améliorations (démarche qualité, suppression des risques, contraintes diverses sur le processus, protocoles, règlements). Les effets négatifs de ces suroptimisations se traduisent par un déplacement des dangers. Les erreurs d'action sont remplacées par des erreurs par défaut d'action. Le système consomme de plus en plus de ressources à se contrôler. Cette consommation, peu perceptible au départ, devient significative quand le système se déploie, particulièrement dans un climat de gestion tendue de personnel. Le déploiement et souvent les dérives des outils de la qualité continue sont un bon exemple de ce paradoxe. Les contraintes réglementaires créent aussi des ordres de priorité dans les problèmes traités, en laissant dans l'ombre des secteurs objectivement plus dangereux mais moins émotionnels, moins soumis à la pression réglementaire et aux contrôles techniques, et *de facto* moins médiatiques.

Pression des médias et investissements irrationnels en fin de cycle. La France a investi de l'ordre de 50 Meuros dans les suites (très médiatiques) de l'accident survenu dans le tunnel du Mont-Blanc[7] (39 victimes, 24 mars 1999) pour la sécurisation des quelques grands tunnels alpins, qui au total, n'ont causé que bien peu de victimes depuis 20 ans. À la même époque, cette somme était significativement supérieure au total des sommes investies par l'état français pour toute la sécurité routière [la route tuait pourtant plus de 8 000 personnes par an[8]]. De même, on a assisté au début des années 2000 à une inflation de contraintes anti-incendie sur les maisons de retraite françaises faisant suite à quelques accidents dramatiques fortement

7. Summary an analysis of the accident available on http://www.mace.manchester.ac.uk/project/research/structures/strucfire/CaseStudy/HistoricFires/InfrastructuralFires/mont.htm.

8. http://www.fiafoundation.org/publications/Documents/road_safety_in_france.pdf.
Ce décalage, vrai pour la période citée, a heureusement été atténué quand la sécurité routière est devenue une grande cause présidentielle à la suite de la seconde élection du président Chirac.

médiatisés. Ce budget de mise en conformité toujours plus important a pioché dans l'enveloppe commune des autres budgets de sécurité de ces établissements, et les a réduits d'autant, alors que les questions de sécurité des soins, survenant le plus souvent sans médiatisation, étaient estimées causer bien plus de victimes que ces (rares) feux d'établissements.

Cette intolérance croissante de fin de cycle abaisse le seuil de déclenchement des situations de crises. Les crises sont plus nombreuses, plus imprévisibles, et toujours plus ardues à contrôler. Le déclencheur des crises de sécurité d'une entreprise est particulièrement sensible au regroupement des plaintes et au phénomène de résonance émotionnelle par les médias.

Enfin les affaires en justice montrent un glissement sensible de la perception des juges vis-à-vis de la responsabilité des industries et systèmes publics. Les marges de progression technologique spectaculaire sont moindres. Le public, et la justice dans son écho à la société civile, tendent à considérer que le risque perçu n'est plus lié à une technologie innovante ou un savoir insuffisant, mais à un arbitrage incorrect donnant la priorité à d'autres dimensions que la sécurité.

Dans ce contexte progressivement défavorable, les seuls à minimiser et percevoir tardivement l'intégrité de la menace sont ceux qui travaillent dans le secteur considéré. Les mécanismes de défenses biaisent leurs perceptions et enferment industriels et partenaires sociaux dans un double piège : corporatisme et protectionnisme. Les acteurs se refusent à miser sur la fin de cycle et à investir sur le cycle suivant ; dans ces conditions, les acteurs industriels qui ont animé tout le cycle vont souvent s'effondrer au profit de nouveaux acteurs industriels qui vont animer le cycle suivant. Sans qu'il s'agisse d'un cycle de sécurité au sens propre, l'exemple de la fin de la photographie argentique et de Kodak, menacé de faillite, est presque une caricature de ce comportement d'enfermement[9].

La fin du cycle et la mort

La fin du cycle s'annonce par des investissements financiers croissants associés à la pression prioritaire des politiques de sécurité (il peut s'agir de coûts directs – personnels, moyens –, ou de coûts indirects – baisse de l'activité, indisponibilité de sécurité). Les profits baissent, et le système cherche des échappatoires en réouvrant largement la recherche amont.

Dès que les conditions d'une alternative sont raisonnablement disponibles, il suffit d'un dernier accident bien médiatisé (un « big-one ») pour que le système précédent s'écroule et laisse la place au système suivant. En ce sens, le « big-one » n'est pas un accident simplement exploité pour ce qu'il représente objectivement du point de vue de sa cause technique, organisationnelle ou humaine, mais un accident exploité symboliquement pour sa valeur systémique.

9. Kodak Teeters on the Brink, Wall street Journal, January 2012, 4, access on http://online.wsj.com/article/SB10001424052970203471004577140841495542810.html.

Ainsi vont les cycles de l'industrie. Et les exemples ne manquent pas.

La fin annoncée de la transfusion sanguine[10]**.** Le sang est devenu très sûr, si sûr que ses quantités tendent maintenant à manquer et que le coût des produits sanguins est devenu explosif. La recherche amont a été réouverte il y a déjà 10 ans pour trouver des substituts du sang (hémoglobine de synthèse) ou des solutions palliatives quasi naturelles (culture de cellules souches produisant des globules rouges). Le potentiel innovant disponible laisse penser que le cycle du sang naturel dans la transfusion sanguine est sur sa fin, et qu'un nouveau cycle se prépare très prochainement. Le cycle de vie de la transfusion de sang humain aura vécu à peine plus de 100 ans.

Les accidents sont souvent plus sévères en fin de cycle, plus insupportables et plus chers à réparer juridiquement

En phase finale d'évolution, la situation de paradoxe est souvent aggravée par les progrès de performance qui majorent considérablement les risques liés aux très rares accidents restants.

Le bénéfice proposé au consommateur est en progrès constants ; les gains concernent, selon les technologies, la baisse du coût à la vente (énergie, voiture, agroalimentaire), un service plus efficace (plus rapide, plus confortable, transports publics), ou une innovation qui ouvre des perspectives jusque-là interdites (chimie, médicaments, techniques chirurgicales).

Le progrès technologique permet d'exploiter des marges jusque-là inaccessibles ou négligées : on va plus vite, on produit plus, on augmente les flux de trafic, on entreprend des thérapies complexes sur des personnes jusque-là condamnées et exclues du système médical. Mais premier paradoxe, ce processus de progrès est forcément porteur de nouveaux risques.

Le déploiement de sécurité sur ces systèmes est significatif, et pondère le nouveau risque accepté pour le maintenir à un niveau stable et très résiduel.

Si faible soit le risque résiduel, il ne supprime pas l'hypothèse de l'accident. Or, second paradoxe, chaque accident résiduel tend à être plus sévère du fait de l'augmentation des performances des systèmes ; il est souvent incroyablement plus coûteux en termes de réparation aux victimes, au point de provoquer dans beaucoup de secteurs une crise publique de l'assurance.

10. Amalberti R (2009) Quel futur et quelle stratégie de sécurité pour un système devenu ultrasûr ? Transfusion Clinique et Biologique 16: 80-5.

Le coût de compensation d'un accident de la route chez un jeune handicapé à vie a atteint en 2007 la somme de 7 Meuros (source MACSF, 2007). Elle était en moyenne 10 à 20 fois inférieure il y a seulement 10 ans, alors que les accidents de la route étaient deux fois plus nombreux.
La provision pour un possible accident aux États-Unis d'un Boeing 747 (source March, 2001) est passée d'environ 500 M$ en 1995 à 750 M$ en 2001, et frôle 1 000 M$ de nos jours. Elle est encore plus élevée pour un Airbus A380. À noter que dans les catastrophes aériennes, deux types de préjudices doivent être indemnisés : les préjudices aux victimes et les préjudices économiques. L'attentat du World Trade Center (11 novembre 2001) a été la démonstration parfaite que les préjudices économiques d'un seul accident pouvaient être si élevés (immobilisation de Wall Street pendant plusieurs semaines) qu'ils pouvaient ruiner assureurs et réassureurs (plusieurs centaines de milliards de US$) ; les assureurs aériens n'ont finalement pas payé ; ils ont négocié (pendant la crise) de limiter très sévèrement leur seuil de réparation des dégâts collatéraux et économiques. En clair, les états sont redevenus – comme dans l'ancien temps – les assureurs de leur risque majeur car le marché privé ne peut plus couvrir ces risques.
Ces chiffres sont presque anecdotiques comparés aux 25,000 milliards de US$ que la crise des *subprimes* et la dette européenne pourraient coûter aux systèmes occidentaux. Là encore, les états ont été massivement obligés d'intervenir pour assurer le risque supposé être géré par un marché de libre concurrence.

Quand le cycle se termine, l'accident devient insupportable plus par ses conséquences que par sa fréquence. Les politiques réglementaires doivent s'infléchir en conséquence. Mais ce n'est pas simple car ces politiques doivent passer :

- d'une *culture de comptabilité (de fréquence) des accidents et presque accidents* (encore dominante), facile à comprendre, à instrumentaliser et à communiquer au grand public, et surtout bornée par le mythe du zéro accident (on compte les accidents et incidents et on montre leur réduction dans le temps) ;
- vers une *culture de justification de la limite des investissements opérés sur la sécurité*, un domaine sans limite haute (toujours plus d'investissements qui en retour n'ont pas d'autres lectures pour le public et les entreprises en l'absence d'accident qu'une envolée des coûts), et nettement moins propice au jeu de la communication grand public.

On conçoit que le glissement imposé aux politiques par le jeu du progrès technique et de l'intolérance croissante aux risques résiduels soit difficile : d'un côté plus de bénéfices et une meilleure sécurité objective, et de l'autre des accidents rares mais graves entraînant une sur-réaction de l'opinion publique, capable de balayer les politiques et parfois même l'industrie avec une totale irrationalité technique et économique (fuite à l'étranger de l'industrie, perte des emplois, mise en cause de personnes publiques qui n'ont pas vraiment le contrôle réel du système).
Aujourd'hui cette bascule n'est pas réalisée sur la plupart des secteurs, et les politiques des pays occidentaux continuent à développer une réglementation réactive aux

événements, fonctionnant par poussées et par secteurs ; dans le fond, cette politique agit comme un frein appliqué de loin en loin sur l'échappement technologique, et ne peut donc prétendre à une sortie contrôlée du piège sociétal dans lequel les pays occidentaux se sont installés pour la gestion de leur(s) industrie/pratiques à risques.
En résumé, une transformation sociétale commune à tous les pays européens induit des problèmes communs dans la gestion des risques.

À côté des lieux communs, nombreux en matière de sécurité, quelques macrodifférences culturelles et stratégiques subsistent sur les interventions de sécurité

Tous les constats précédents convergent vers un modèle commun, mondial, de gestion de la sécurité des grands systèmes à risques.
Il demeure cependant quelques différences régionales dans les macrostratégies de sécurité, pour la plupart liées aux modèles culturels et juridiques. Une des plus évidentes oppose les pays dont la justice et l'administration s'inspirent du Code romain (France, Italie, Grèce, Espagne) et les pays qui s'inspirent d'un Code anglo-saxon (typiquement États-Unis et Royaume-Uni). Les différences s'expriment surtout dans le périmètre et l'intensité prescriptive des actions de sécurité[11]. Le Code romain, introduit par l'empereur Justinien, a entre autres particularités celle de reposer sur des spécifications écrites. La France à travers son code napoléonien s'inscrit totalement dans cet héritage de *pays de droit écrit*, avec une inflation de textes spécifiant jusqu'au détail de la prescription légale y compris pour les aspects relevant de la culture[12], *land of written laws*, alors que le Code anglo-saxon fait une place plus large au Code coutumier (*customary laws*). Bien sûr les déclinaisons intermédiaires ont progressivement lissé les différences[13], mais sans les effacer totalement.
Les deux exemples suivants, tirés de l'aéronautique, donnent le ton des différences.

Code romain *versus* Code anglo-saxon : des sensibilités différentes. Exemple de la réglementation nationale des examens médicaux pour les pilotes de ligne avant harmonisation européenne
Jusqu'en 2009, les règlements étaient nationaux.
En Suède ces examens sont confiés à des médecins certifiés, installés en ville en profession libérale. Ces médecins renvoient leurs résultats à une agence nationale. La réglementation est réduite mais sans tolérance : guide de bonnes pratiques,

11. http://www.answers.com/topic/roman-law.
12. Written reason of the ***Corpus Juris Civilis.***
13. Lire par exemple: MacQueen H (2000) Scots law on the road to the new IUS commune, http://www.ejcl.org/44/art44-1.html COMPARATIVE LAW, <http://www.ejcl.org/ejcl/44/art44-1.html>.

évaluation continue des médecins agréés réputée sévère, et agréments donnés pour une période de temps limitée (chaque accident d'un pilote renvoie à un examen minutieux des dossiers d'aptitudes ; tout manquement d'un médecin dans la détection d'une cause directe ou indirecte de l'accident peut constituer une cause de perte de son agrément ou de non-renouvellement).
En France, l'exclusivité des examens médicaux professionnels en aéronautique a longtemps été totalement réservée aux centres d'expertise militaires. Une timide ouverture s'est faite vers des centres civils à la fin des années 1980. Aucun médecin libéral installé en ville n'a pu obtenir d'agrément jusqu'à un temps récent. Ce système centralisé, public, possède une réglementation beaucoup plus étendue et plus sévère (en théorie) que la réglementation suédoise (contenu des visites plus important, et parfois normes d'aptitude plus restrictives) ; cette sévérité est compensée par un fonctionnement pragmatique et des dérogations multiples. L'évaluation continue des médecins agréés est quasi absente. Les agréments sont obtenus à vie, et les sanctions contre les erreurs sont extrêmement marginales.
Ces différences se sont certes estompées avec l'arrivée des règlements européens en 2000, mais, en y regardant bien, la différence de culture ne s'est pas encore gommée.

Code romain* versus *Code anglo-saxon : sensibilités différentes : la réglementation de formation des personnels navigants à la gestion des ressources dans le poste d'équipage (CRM* – Crew Resource Management*)

Les travaux conduits notamment aux États-Unis dans les années 1980 ont montré l'importance des formations aux compétences dites « non techniques » souvent regroupées sous l'acronyme CRM pour entraîner les pilotes au travail en équipage.
En 1993, l'Organisation de l'Aviation civile internationale modifie son règlement et introduit dans son annexe 6 (relative aux opérations aériennes) le paragraphe 9.3 exigeant une formation continue des équipages aux compétences non techniques.
Dès 1993, la Direction générale de l'Aviation civile française (DGAC) se dote d'un texte obligeant les compagnies aériennes à développer des formations CRM (arrêté de mars 1993). Ce texte est ambitieux, très prescriptif, avec un délai de mise en conformité assez court. La supervision administrative est confiée aux directions régionales de l'Aviation civile (DRAC). Seule la compagnie Air France est à cette époque dotée d'un outil de formation conforme (depuis 1992). La formation des personnels des directions régionales de l'Aviation civile, l'accompagnement et la mise en conformité reposent sur quelques fonctionnaires. Une étude effectuée en 2006[14] *montre que cette mise en conformité des compagnies françaises est erratique, particulièrement hétérogène d'une compagnie à l'autre, et le suivi par les agences régionales de l'administration particulièrement tolérant.*

14. Deharvengt S (2006) Barriers to regulating resilience: example of pilots'crew resource management training. Consulté sur http://www.ep.liu.se/ecp/023/002/ecp2307002.pdf.

*Inversement, depuis 1988, la FAA (*Federal Aviation Administration US*) dispose d'une AC (*advisory circular*) recommandant (et non exigeant) à ses compagnies la pratique des CRM. La première compagnie au monde à être dotée d'un tel outil a été United Airlines en 1982. En 1993, plus de 70 % des compagnies américaines disposaient déjà d'un CRM avec une certaine homogénéité nationale. Aucun règlement formel n'avait pourtant été édicté jusqu'en 2001.*
*De même au Royaume-Uni, il n'y a pas eu de demande réglementaire formelle jusqu'en 1999, date de bascule dans le règlement harmonisé européen JAA. En revanche, le bureau recherche de la CAA UK (*Civil-Aviation Authority UK*) a encouragé financièrement l'adoption spontanée par les compagnies de ces techniques depuis 1990, avec l'aide et la supervision de la* Royal-Aeronautical Society. *La plupart des compagnies se sont mises en conformité avant 2000 sur un modèle minimaliste mais relativement homogène.*

Ces deux exemples, que l'on pourrait aisément compléter par d'autres exemples pris dans les transports terrestres et aériens (temps de travail des opérateurs par exemple), la réglementation routière, l'environnement (chimie, rejets sols), la construction et la certification des aéronefs, soulignent quelques traits culturels stables différenciant les façons de réglementer la sécurité dans différentes régions européennes.
La France, et plus globalement les pays de l'Europe du Sud (Italie, Grèce, Espagne, Portugal) se caractérisent par les points suivants :
- la réglementation sur des sujets de sécurité tend à être considérée comme un incitateur pour la mise en conformité de l'industrie ou des services publics visés. Les règles sont promulguées dans un contexte où l'on sait que l'industrie – ou le service public – ne sera pas encore capable de respecter le règlement ;
- cette stratégie conduit à une abondance de réglementation très prescriptive, émanant souvent du plus haut niveau de l'État. Inversement, les simples recommandations sont peu nombreuses et peu écoutées par l'industrie, et le support associatif de soutien à l'application réduit et peu aidé par l'État ;
- la mise en conformité est logiquement lente, et les dérogations multiples ; ces dérogations deviennent souvent un mode de régulation pérenne du système ;
- les observatoires et les outils de la mise en conformité sont construits pour remonter avant tout de l'information aux donneurs d'ordre étatiques. Ils distribuent en revanche peu d'information en retour aux unités de production de bas niveaux ;
- le caractère centralisé des décisions et des outils de surveillance gomme les effets de responsabilités individuelles au profit d'une responsabilité centrale. Ce sont le plus souvent l'État et les grands organismes qui prennent en charge la réparation en cas de faute.

Le bloc anglo-saxon, typiquement États-Unis et Royaume-Uni, privilégie une approche opposée :
- pas de règle tant qu'une majorité de l'industrie n'est pas capable de la suivre ;
- en revanche, recommandations précoces, nombreuses, très accompagnées par l'État et le tissu associatif, avec une écoute réelle de l'industrie (une recommandation

promulguée par la FAA sous forme d'AC [*Advisory Circular*] vaut pratiquement une règle française dans ses effets comparés sur l'industrie) ;
– l'observatoire est très démultiplié et les sanctions individuelles sont plus fortes ; la logique des assurances est différente ;
– les Allemands et les pays nordiques sont dans une position intermédiaire, avec un régionalisme plus fort dans ses particularités de réglementation, un système plutôt moins exigeant que le système français, mais où la tolérance à l'écart est très faible.

Quelles leçons retenir ?

Dans tous les cas, et contrairement aux principes de bon sens vus dans l'introduction, la sécurisation entraîne toujours un effet paradoxal : elle est une préoccupation des systèmes et des sociétés déjà devenus sûrs ; elle est en quelque sorte une préoccupation de riche, quand le reste des besoins essentiels est déjà satisfait.
Pire, le niveau de sécurité possède l'étonnante propriété de ne jamais être suffisant, et d'engendrer une exigence sociétale qui augmente en parallèle des progrès réalisés. C'est une variable sans maximum, et toute amélioration rend le jugement d'autrui encore plus sévère sur les quelques cas d'insécurité persistants. Plus la sécurité s'impose, plus elle devient un objet difficile à manier qui va se mettre à sérieusement freiner la productivité du système.
C'est cette « impossible sécurité » doublée d'un « frein de productivité » quand on sécurise plus qui vont créer les conditions de l'émergence d'une rupture permettant de repartir dans un nouveau cycle de vie basé sur une autre innovation/organisation industrielle.
Pour durer, pour survivre dans un paradigme industriel exposé à sa fin de cycle, il va falloir suivre trois types d'actions peu avouables au grand public :
– ne pas dépasser la demande sociétale ni aller trop vite vers l'ultrasécurité (en quelque sorte garder des marges de progression) ;
– adapter les compromis entre sécurité et performance et les nécessaires investissements en fonction du cycle de vie du système. Les outils et les solutions adaptés de sécurité changent dans le décours du cycle de vie ; c'est d'ailleurs un des points les plus difficiles pour l'industrie, car les solutions adaptées et performantes pour un passé récent peuvent s'avérer dangereuses et inadaptées au même système placé à une autre phase de vie de cycle industriel. Dit autrement, on ne soigne pas une grippe chez une personne âgée porteuse de polypathologies comme on soigne une grippe chez un jeune de 20 ans. Le compromis dans la force du traitement doit forcément être infiniment plus sophistiqué chez la personne âgée, faute de tuer la personne en la guérissant de la grippe. L'idée même de traitement de compromis est encore plus importante pour la sécurité, si l'on admet que la préoccupation sécuritaire est une propriété du vieillissement des cycles technologiques ;
– anticiper la crise de fin de cycle et investir à temps sur le cycle suivant pour ne pas mourir soi-même de la fin du cycle. Encore une fois, le besoin ne s'efface pas et les

cycles se succèdent, mais les bénéficiaires industriels peuvent changer (et changent le plus souvent). L'exemple de l'écroulement en quelques mois de la photographie argentique dans les années 2000 est à cet égard une illustration caricaturale de ces fins de cycles redistribuant brutalement les cartes industrielles.

Les chapitres suivants abordent la construction des nécessaires compromis de sécurité chez les opérateurs, les équipes (chapitre 2), et les organisations et les grands systèmes (chapitre 3).

2

L'erreur humaine au centre des débats sur la sécurité

Ce chapitre est centré sur la découverte du modèle de sécurité utilisée par les individus pour réaliser leur travail sans incident ou accident. Il donne une perspective micro sur la sécurité. Son contenu reprend une synthèse du livre sur la conduite des systèmes à risques publié en 1996, augmentée des travaux plus récents sur les biais communs de l'analyse des erreurs, et l'importance des concepts de suffisance, de compromis, d'arbitrages, et du rôle central des routines.

Les erreurs humaines, grandes étapes de la construction des savoirs

Les humains ne cherchent pas à travailler sans erreurs ; ils cherchent à obtenir un résultat satisfaisant en minimisant les coûts négatifs (temps perdus, incidents). L'objectif central de l'humain est de progresser vers son résultat en restant en contrôle cognitif de la situation. Cette supervision est à deux volets : d'une part la progression vers le but en contrôlant le résultat externe des actions, et d'autre part le maintien d'un coût raisonnable de l'exécution cognitive du travail (fatigue, investissement, sacrifice d'autres activités qui pourraient être menées en parallèle). Dans ce contexte, le flux d'erreur est important (particulièrement pour les erreurs de routine) mais (i) ce flux ne prédit pas le risque d'accident, et (ii) ce flux doit être relié à un autre flux : celui de la détection et de la récupération des erreurs dont la dégradation est plus prédictive pour le risque d'accident.

Qui n'a pas entendu que 70 % des accidents ont une cause humaine liée aux erreurs des opérateurs ? Et qui n'a pas entendu que si l'on ajoute la part des concepteurs et des managers dans l'occurrence de ce que l'on appelle les erreurs techniques (pannes) ou les erreurs d'organisation (options de gouvernance, climat social), ce sont en fait 100 % des accidents qui ont une cause directe ou indirecte liée aux facteurs humains.

De tels chiffres donnent une priorité naturelle à comprendre les erreurs humaines pour les réduire, le bon sens fait penser que leur réduction s'accompagnera forcément d'une réduction des accidents.

La réalité est loin d'être aussi simple. Ce chapitre dresse quatre constats : (i) les erreurs sont encore plus fréquentes qu'on ne l'imagine, plusieurs par heure, (ii) mais largement autodétectées et récupérées, de sorte que les conséquences observées sont bien inférieures à ce que prédit la fréquence d'erreur, (iii) elles sont inhérentes au fonctionnement cognitif, notamment routinier, et ne peuvent donc pas être supprimées, sauf à supprimer l'homme, (iv) la simplification excessive – et erronée – du lien entre erreur et sécurité n'a pas vraiment résolu les questions de sécurité.

Les systèmes conçus sur des contresens et des mauvais arguments scientifiques ne permettent pas à l'opérateur de se coupler efficacement. Ils provoquent un cercle vicieux en ne faisant que déplacer les erreurs et rendre plus difficile leur contrôle et leur gestion. La poursuite du raisonnement conduit naturellement à automatiser encore plus pour obtenir (enfin) une vraie fiabilité. Ce faisant, on troque la fiabilité humaine contre la fiabilité technique, mais on échoue totalement dans la synergie et la sommation des deux. Le résultat est forcément moins bon que ce qu'on espérait.

Le chemin vertueux consisterait plutôt à déconstruire ce lien entre erreur et accident, traverser le miroir, se mettre dans la tête de l'opérateur, et comprendre que la gestion des risques individuels se base sur des savoirs extrêmement sophistiqués de compromis et de contrôle global de la situation. L'erreur en elle-même ne porte jamais seule le risque d'accident, mais la perte de son contrôle, de la conscience des compromis de risques acceptables, et des capacités de gestion de la situation, peut très vite conduire à l'accident.

C'est pourquoi ce chapitre sur l'erreur et la gestion des risques individuels comporte une ossature théorique relativement importante. Il nécessite plus que les chapitres suivants de corriger les fausses bonnes idées.

Ce n'est que récemment, dans les années 1970, que l'étude de l'erreur humaine est devenue un objet scientifique à part entière de la psychologie. Auparavant, à l'exception des Gestaltistes dans la première moitié du XX^{e} siècle, les erreurs n'étaient considérées que comme un score de performance parmi d'autres dans l'approche expérimentale des phénomènes physiques ou psychiques.

L'apport initial de la Gestalt : l'échec permet d'accéder à la compréhension

Les premiers travaux significatifs sur l'erreur (en fait plutôt sur l'échec) remontent à l'avant-guerre (années 1910 à 1940) et sont à mettre au compte de la *Gestalt theory*, la

théorie de la forme. Cette théorie est considérée comme le fondement de la psychologie cognitive moderne.
Les Gestaltistes (Koffka, Köhler, Wertheimer) s'étaient d'abord intéressés aux organisations de l'environnement visuel imposant à nos cerveaux des interprétations perceptives souvent erronées de scènes complexes (figures ambiguës).
Chacun a déjà croisé ces figures complexes qui provoquent des illusions d'interprétation.

Un exemple d'illusion d'interprétation décrite par les Gestaltistes. Cette variante de l'Illusion de Müeller-Lyer utilise deux flèches. Quand on demande de comparer la taille des lignes (hors pointes) qui sont égales, l'observateur désigne la flèche avec les pointes vers l'intérieur comme la plus grande.

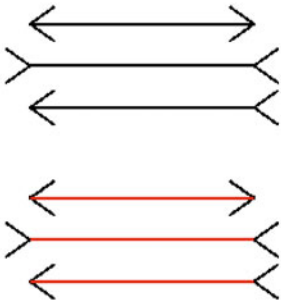


Fig. 2

Très vite, cette approche de la perception va conduire à admettre que voir n'est pas un simple processus objectif (tout le monde ne voit pas la même chose dans une même situation). Il s'agit plutôt d'une construction active de notre cognition (dirigée par nos connaissances et nos attentes) filtrant et corrigeant les propriétés de l'environnement pour y lire ce qu'on recherche. Cette construction active issue des travaux sur la perception s'est rapidement étendue aux théories du champ social dans les années 1930 (Lewin[1]), puis à la compréhension des situations complexes et de la décision dans les années 1940 (Duncker[2]).
C'est la réorganisation des prémisses (les conditions initiales du raisonnement et de la perception initiale de la situation) en étant capable de modifier son champ cognitif (penser à une autre solution possible) qui conduit à reconsidérer les faits observables (voir de nouvelles choses qu'on n'avait pas vues jusque-là) et qui fait finalement jaillir la solution (l'insight).
Quand le sujet prend sa décision en restant sur son impression de départ, il reproduit en général une solution connue. Duncker montre qu'il existe souvent des solutions plus rapides, plus élégantes, qui ne sont même pas imaginées par le sujet tant que sa solution

1. Lewin Kurt (1935) A dynamic theory of personality. Mc Graw-Hill.
2. Duncker K (1945) On Problem Solving. Psychological Monographs 58: 270.

routinière fonctionne. Ce n'est que devant l'échec que l'opérateur réenvisage ses hypothèses, reconsidère les faits disponibles dans la situation et *produit* (et pas simplement *reproduit*) une solution.

> L'échec et le blocage sont pour les Gestaltistes une condition importante voire indispensable au déclenchement de la compréhension et de la production d'idée nouvelle. Cette vision positive de l'échec va irriguer une grande partie de la littérature moderne sur l'erreur.

Les premiers travaux sur les erreurs : le rôle essentiel du contrôle de l'activité cognitive

Le deuxième départ des études sur l'erreur est plus récent, et d'une tout autre origine, puisqu'il s'inscrit dans la prolongation du débat sur les théories de l'attention et les routines.

Les premiers modèles sur l'attention avaient mis l'accent uniquement sur les limitations. Le modèle de canal limité de Broadbent (1958)[3] interprétait l'attention comme un filtre triant l'information disponible dans le monde extérieur, et la faisant pénétrer dans la cognition en pipeline dans un « canal unique », avec un ordre de priorité.

Miller (1956)[4] confirmait la contrainte en montrant que la mémoire à court terme était limitée en durée et en capacité (7 éléments ± 1).

Ces approches furent rapidement critiquées pour leur caractère peu réaliste, les données s'accumulant pour montrer que les limites prédites étaient faciles à dépasser par tout opérateur. Shiffrin et Schneider (1977)[5] proposèrent alors un modèle devenu célèbre, distinguant deux niveaux tournant en parallèle avec des boucles d'interaction :

- un niveau conscient et contrôlé, nécessitant un contrôle attentionnel. Ce niveau est contraint en volume et en durée (si on doit faire attention en voiture à son chemin de sortie d'un carrefour complexe, on arrêtera quelques instants la conversation en cours, on perdra ce qui s'est dit à la radio, car on ne dispose pas assez de ressources pour faire deux choses à la fois) ;
- un niveau automatique, routinier, sans contrôle attentionnel, et quasiment sans limites de parallélisme (bien que l'on ait arrêté la conversation à l'entrée du carrefour, on continuera à pouvoir piloter la voiture avec des routines de changement de vitesse et de freinage qui ne sont pas vraiment conscientes, et on pourra gérer encore plein d'autres activités de bas niveaux en parallèle comme manipuler le son, manipuler le clignotant…).

3. Broadbent D (1958) Perception and Communication. London: Pergamon Press.

4. Miller GA (1956) The magical number seven, plus or minus two: some limits on our capacity for processing information. Psychological Review 63: 81-97.

5. Shiffrin R, Schneider W (1977) Controlled and automatic human information processing: perceptual learning, automatic attending and a general theory. Psychological Review 84: 127-90.

Ces idées vont être opérationnalisées en termes de charge de travail par la métaphore d'une cognition disposant d'un réservoir de ressources[6]. Les processus attentionnels consomment les ressources alors que les processus routiniers n'entament pas le réservoir. Les experts savent mieux que les débutants utiliser leurs routines et gérer ce réservoir, et sont donc plus aptes à gérer des situations de forte charge de travail.

Dans la foulée de ces travaux, Donald Norman est le premier auteur à avoir utilisé ces idées, pour en déduire une théorie sur les erreurs des routines en pointant le paradoxe qu'elle concerne en premier les experts.

Le premier modèle qu'il propose[7] comporte deux dimensions :

- une dimension horizontale, qui contient une série de fils à fonctionnement autonome ; chaque fil fonctionne avec des procédures bien connues et routinières (en psychologie cognitive, ces procédures sont appelées schémas ou scripts) ;
- une dimension verticale, interagissant avec la structure horizontale pour la guider et la réguler.

Le niveau horizontal permet de réaliser les activités routinières sans contrôle, dans la mesure où l'action progresse normalement vers le but. L'attention et la motivation interviennent comme variables verticales en modulant l'activation des fils (schémas) chaque fois que des obstacles, des saturations ou des choix sont à opérer parmi les buts et les routines en opération.

Norman déduit alors[8] plusieurs modes de défaillance dans la gestion de ces schémas routiniers. Ces erreurs sont appelées « ratés » (***slips*** en anglais). Il distingue :

- les ratés résultant d'une mauvaise activation des schémas : il peut s'agir d'une activation involontaire (« passez trop près d'une habitude bien établie et elle capturera votre comportement ». Par exemple vous devez faire un détour pour raccompagner exceptionnellement quelqu'un, mais à la première bifurcation que vous empruntez tous les jours, vous oubliez le rendez-vous et vous vous retrouvez devant votre domicile [capture de routine]). Le schéma peut aussi perdre de sa pertinence : il continue à se dérouler alors que l'on a oublié pourquoi on avait lancé l'activité ;
- les ratés résultant d'un mauvais déclenchement des schémas. Le schéma est correctement choisi et activé, mais au mauvais moment, ou il est mélangé à un autre schéma et le résultat est incorrect : une secrétaire tape une lettre en pensant au rendez-vous qu'elle a à 12 h 30 et inscrit sur la lettre « la réunion aura lieu à 12 h 30, au lieu d'écrire le bon texte : « la réunion aura lieu à 14 h 00 ». Il peut s'agir aussi d'un changement de l'ordre d'exécution d'une macroroutine qui finit par faire sauter ou oublier une partie du travail à faire : on arrose des plantes dans le salon tous les matins en se levant, mais ce jour-là des amis couchent dans le salon et on ne peut y accéder. On remet à plus tard le travail d'arrosage, et on finit par l'oublier.

6. Wickens C (1984) Varieties of attention. New York: Academic Press.

7. Norman D A, Shallice T (1986) Attention to action: willed and automatic control of behavior. Consciousness and self-regulation. Davidson GS, Shapiro D. New York, Plenum Press 4: 1-18.

8. Norman D (1981) Categorization of action slips. Psychological review 88: 1-15.

L'apport de Rasmussen : le modèle SRK

En 1983[9, 10], Jens Rasmussen introduit le célèbre modèle SRK qui distingue trois modes de fonctionnement cognitif et autant de types d'erreurs. Il distingue :

- le niveau basé sur les connaissances (***knowledge-based behaviour***) : on mobilise tout ce que l'on sait pour comprendre et agir sur la situation, dans une démarche rationnelle, typique des démarches apprises à l'école ;
- le niveau basé sur les règles (***rules-based behaviour***) : on mobilise des règles professionnelles (si, alors) qui permettent de gagner du pragmatisme et de l'efficacité dans l'action par rapport au mode précédent. Par exemple, considérez une règle banale de cuisine qui dit « si l'eau bout, alors seulement mettre les pâtes à cuire » ; inutile de se remémorer avant de mettre les pâtes pourquoi on doit attendre pour la cuisson, pourquoi l'eau bout, pourquoi l'eau s'évapore dans ces conditions d'ébullition, et pourquoi sa température d'ébullition change avec l'altitude… La connaissance de la règle permet une action efficace sans se poser de question de son « pourquoi » ;
- le niveau basé sur les routines (***skill-based behaviour***). L'action devient complètement automatique en réponse au stimulus : je vois ma maison, et je commence à sortir mes clés sans même en avoir pris conscience.

Dès le départ, cette distinction s'inscrit dans le contexte de la fiabilité humaine.

> Tout apprentissage part d'un fonctionnement basé sur les connaissances pour finir par un fonctionnement basé sur les habitudes et les routines. L'expert se caractérise par la plus grande disponibilité de ces routines qui lui permet de travailler plus vite, et de résister à une plus grande charge de travail.

Les routines sont donc d'abord un marquage de l'expertise et elles représentent la base habituelle du travail d'un professionnel. Ce n'est que lors des échecs des routines que seront exigées des réversions de plus en plus coûteuses et aléatoires pour la cognition. Si la routine ne marche plus, et que la progression vers le but se trouve bloquée, l'opérateur passera sur un mode basé sur les règles, et s'il ne trouve pas de règle qui le sauve, il basculera dans un mode basé sur toutes ses connaissances.

Par exemple, vous partez pour un rendez-vous et vous pensez connaître la route. Vous roulez en routine, écoutez la radio et pensez à votre rendez-vous. Mais vous tournez trop tôt à droite… Vous devrez quitter votre mode de conduite en routine (arrêter d'écouter la radio, et vous concentrer sur la navigation), vous chercherez très probablement à mobiliser dans votre mémoire une règle qui pourrait vous aider ; par exemple : « si j'ai tourné trop tôt, alors il faut que je fasse demi-tour, sauf si tout est bouché en sens inverse » ou « si j'ai tourné trop tôt, alors je suis forcément parallèle et si je

9. Jens Rasmussen est un ingénieur visionnaire, autodidacte des facteurs humains, capable de lire et faire des ponts entre courants théoriques qui s'ignorent entre eux. Il va réorienter sa carrière vers la fiabilité technique et humaine à la suite de l'accident nucléaire de Three-Miles Island aux États-Unis en mars 1979. Il va devenir un des pionniers des approches modernes sur la sécurité des systèmes complexes. Il influencera profondément toute une génération de chercheurs qui ont été ses élèves directs, notamment James Reason, Erik Hollnagel, Dave Woods, et… l'auteur de ce livre.

10. Rasmussen J. (1983) Skills, rules, knowledge: signals, signs, and symbols, and other distinctions in human performance models. IEEE Transactions on Systems, Man and Cybernetics 13: 257-66.

continue, je n'aurai qu'à faire une baïonnette plus loin dans la bonne rue ». Vous essayez une de ces règles. Si la situation ne s'améliore pas, vous vous déclarerez « perdu » et vous basculerez sans doute dans un fonctionnement beaucoup plus analytique, basé sur toute votre connaissance générale : sortir la carte, chercher un plan, demander de l'aide.
Chacune de ces étapes crée des opportunités d'erreurs différentes (erreur de routine, de règles ou de connaissance).
Pour résumer, la variabilité des performances inter- et intraopérateurs (lors de répétitions) tient pour une large part à des variations dans le niveau de contrôle de l'activité cognitive. En temps normal, les opérateurs qualifiés utilisent au maximum le niveau basé sur les habitudes (des routines), une attitude qu'ils paient par un grand nombre d'erreurs de routines. Quand la situation devient moins familière, les sujets basculent dans un contrôle plus attentif en suivant plus formellement les règles, ou dans les situations les plus dégradées, en créant ex-nihilo de nouvelles procédures ; les erreurs seront alors plus souvent des erreurs de règles et de connaissance.

La synthèse de James Reason

Reason[11, 12], s'inspirant du modèle SRK de Rasmussen, va reprendre cette classification des erreurs en trois catégories, qui reste LA référence :

- les erreurs de routine correspondent au fonctionnement basé sur les routines de Rasmussen (*skill-based behaviour*). Il s'agit de défaillances de la surveillance de l'exécution. L'action se déroule sans contrôle conscient, dans le cadre de projets familiers. Le sujet n'a pas pris conscience qu'il avait un problème. Ces erreurs caractérisent le travail des experts très entraînés. Elles sont nombreuses (80 % du total des erreurs commises), mais très largement récupérées (90 %), et, contrairement à ce qui a l'habitude de se dire, ne sont que rarement responsables d'accidents graves (mais elles sont souvent responsables d'incidents et d'oublis) ;
- les erreurs d'activation de règles. Le sujet est face à une difficulté qu'il ne peut pas résoudre en routine (il a conscience d'avoir un problème). L'erreur va résulter de la sélection d'une mauvaise solution par activation d'une mauvaise règle. Cette erreur n'est pas contradictoire avec l'idée que le sujet possède par ailleurs la connaissance de la bonne solution ; mais il n'a pas su l'activer, la recouvrir en mémoire, ou pas pu (faute de temps) s'en servir dans son contexte. Une autre solution, moins valide mais immédiatement disponible, s'est imposée à sa logique d'action. Ces erreurs sont moins fréquentes (15 % des erreurs totales) mais plus redoutées que les erreurs de routine pour leurs conséquences sur la sécurité. On les appelle souvent « erreur de représentation » parce que l'opérateur « applique bien sa procédure, mais dans un

11. James Reason a été longtemps professeur à l'université de Manchester, aujourd'hui retraité ; il est sûrement l'auteur le plus connu en matière de théorie sur l'erreur humaine. Il a publié de nombreux ouvrages, dont un fait référence sur le sujet ; il a été fortement influencé par Jens Rasmussen, avec qui il a travaillé étroitement au milieu des années 1980.

12. Reason J. Human error, Cambride University Press, 1990, traduit en Français PUF, Paris, 1993 ; traduit en espagnol, Modus Laborandi, 2009.

mauvais contexte où cette procédure n'est pas pertinente ». Le thème des « erreurs de fixation » (ne pas changer de représentation, s'enfermer dans une vision erronée) est un cas particulier de ce type d'erreur, très commenté dans la littérature car difficile à résoudre. La solution de sécurité apparaît davantage relever d'un bon travail de groupe et de la capacité d'apporter en temps réel des visions différentes du problème[13, 14] ;

– les erreurs par manque de connaissance[15]. Le sujet est ignorant de la solution du problème qu'il a à régler. Il mobilise toute sa cognition, lentement, pas à pas, pour produire une nouvelle solution. L'erreur peut alors revêtir différentes formes : bonne solution hors délais, mauvaise solution… Ce type d'erreur est (heureusement) rare chez le professionnel (moins de 5 % du total des erreurs), mais évidemment toujours plus sévère dans ses conséquences sur la sécurité.

Différents types d'erreurs et leurs caractéristiques (inspiré de Reason, 1990).

Dimension	Erreurs basées sur les automatismes de comportements	Erreurs basées sur les règles	Erreurs basées sur les connaissances
Type d'activité	Actions routinières	Activités de résolution de problème	
Concentration de l'attention	Sur autre chose que la tâche en cours	Sur des considérations liées au problème	
Mode de contrôle	Schémas	Règles stockées	Processus conscients limités
Caractère prédictible de l'erreur	Largement prédictible	Variable	
Fréquence	Élevée dans l'absolu, mais paradoxalement faible en proportion du grand nombre de routines…	Faible dans l'absolu, mais élevée en proportion du très faible nombre de ces situations d'ignorance quasi totale	
Capacité de détection	Élevée	Très faible sans intervention extérieure	
Risques pour la sécurité	Modérés	Importants à très importants	

13. Fioratou E, Flin R, Glavin R (2012) No simple fix for fixation errors : cognitive processes and their clinical implications. Anesthesia 65: 61-9.

14. Besnard D, Greathead D, Baxter G (2004) When mental models go wrong : co-occurrences in dynamic, critical systems. Int J Human-Computer Studies 60: 117-28.

15. Attention à la traduction et aux faux amis : en anglais, ces erreurs sont appelées FAULT, mais leur traduction en français ne doit pas être FAUTE (trop connoté) mais ERREUR DE CONNAISSANCE.

Les travaux sur la détection et la récupération

Parler de mécanisme de production d'erreur ne résume pas l'analyse de l'erreur, loin s'en faut. L'erreur ne devient un problème que par ses conséquences. La détection et la récupération précoces des erreurs avant qu'elles n'aient de conséquences sont au cœur de la gestion des risques.

Or cette détection et cette récupération des erreurs sont particulièrement efficaces chez les humains.

Hayes et Flower[16] ont été les premiers à s'intéresser à la capacité de détection des fautes d'orthographe et de syntaxe par les rédacteurs. Ils ont distingué deux mécanismes : (i) une détection intentionnelle à la relecture (*editing*), et (ii) une détection itérative durant l'écriture (*reviewing*), de loin la plus efficace.

Allwood et Montgomery[17] ont augmenté et théorisé ces premiers travaux en travaillant sur les erreurs commises par des élèves dans des exercices de physique et de mathématique. Ils individualisaient trois phases dans le processus de correction : la détection, le diagnostic du problème, et la récupération. La détection correspondait simplement à la perception d'un problème dans le décours de l'action (sans identification). Le diagnostic correspondait à l'identification de l'erreur. La récupération correspondait à l'annulation des conséquences de l'erreur ou de ses conséquences.

Ces premières études ont conclu à l'existence de quatre familles de stratégies de détection des erreurs :

- stratégie 1 : les évaluations en fonction de connaissances sur le résultat (*affirmative évaluation*). Le sujet contrôle son résultat en fonction de fourchettes réalistes qu'il connaît sur la valeur du résultat attendu ;
- stratégie 2 : les contrôles de routine (*standard check*). Le sujet fait un contrôle indépendamment de toute suspicion précise et découvre son erreur ;
- stratégie 3 : le contrôle orienté (*direct-error-hypothesis formation*). Le sujet réagit à un résultat bizarre et forme tout de suite une hypothèse sur le type d'erreur qu'il a pu commettre ;
- stratégie 4 : la simple suspicion (*error-suspicion*). Une partie des résultats est jugée bizarre mais sans pouvoir formuler d'hypothèse explicative.

La stratégie qui détecte en volume le plus d'erreurs est « le contrôle orienté », puis dans l'ordre d'efficacité « la simple suspicion », les « évaluations en fonction des connaissances sur le résultat », et loin derrière « les contrôles de routine » qui correspondent aux contrôles appris à l'école.

Au total, ces stratégies sont redoutablement efficaces.

16. Hayes J, Flower L (1980) Identifying the organization of writing processes. Cognitive processes in rriting. L. Gregg, Steinberg, E. Hillsdale, Lawrence Erlbaum Associates.

17. Allwood C, Montgomery H (1982) Detection errors in statistical problem solving. Scandinavian Journal of Psychology 23: 131-13.

70 à 80 % des erreurs commises sont détectées par celui qui les a commises, dans un temps très court, dont 90 % des erreurs de routine, et, sans surprise, à peine 20 % des erreurs de connaissance[18, 19, 20].

Ces travaux nous apprennent aussi que les meilleurs sujets pratiquent plus de contrôles de routine, alors qu'on vient de voir que cette stratégie est apparemment peu rentable pour détecter des erreurs. Sans doute les erreurs qu'elle détecte ne sont pas récupérables par les autres stratégies, et de ce fait font la différence entre les sujets qui négligent ces contrôles systématiques et les experts.
Plus important encore, Allwood (op cité) montre :
- que l'efficacité dans la résolution de problème est significativement corrélée au taux des erreurs détectées pendant la résolution ;
- qu'il n'existe aucune corrélation entre le nombre d'erreurs commises et l'efficacité finale du sujet.

Lutter contre les fausses bonnes idées : le volume d'erreurs ne prédit pas la performance, c'est la récupération des erreurs qui prédit le mieux la performance du sujet.
Les erreurs commises semblent servir au sujet à prendre conscience de son activité et à régler son compromis cognitif pour converger vers la solution.
Le sujet se sert des erreurs qu'il commet pour autoévaluer en continu son fonctionnement cognitif et régler ses prises de risques. Les activités réflexives (se regarder travailler) sont évidemment au centre de ce réglage.

Ces résultats ont été validés dans les situations industrielles

Une des premières applications industrielles[21] a concerné une situation d'imprimerie avec une gestion de bases de données caractérisée par un grand nombre de tâches à gérer en parallèle et une complexité des tâches variable selon les ateliers. L'étude a montré que **les ratés augmentent avec la complexité de la tâche, mais leur détection augmente aussi avec l'expérience des sujets**. L'étude confirme que ce sont les vérifications de routine qui contribuent à cette amélioration significative de la performance chez les sujets experts.
La même étude montre que les erreurs de règles ne sont pas plus fréquentes quand la tâche se complexifie et ne sont pas significativement mieux détectées avec l'expérience. Les rares erreurs de connaissances sont en revanche beaucoup mieux détectées par les sujets experts. Ces travaux confirment de manière spectaculaire la complexité de la gestion du compromis cognitif.

18. Allwood CM (1984) Error detection processes in statistical problem solving. Cognitive science 8: 413-37.

19. Wioland L, Amalberti R (1996, November 12-15). When errors serve safety: towards a model of ecological safety. In: First Asian conference on Cognitive Systems Engineering in Process Control (CSEP 96), sous la dir. de E. Hollnagel. Kyoto, Japan: 184-91.

20. Doireau P, Wioland L, Amalberti R (1997) La détection des erreurs par des opérateurs extérieurs à l'action : le cas du pilotage d'avion. Le Travail Humain 60: 131-53.

21. Rizzo A, Bagnara S, Visciola M (1987) Human error detection process. International Journal Man-Machine Studies 27: 555-70.

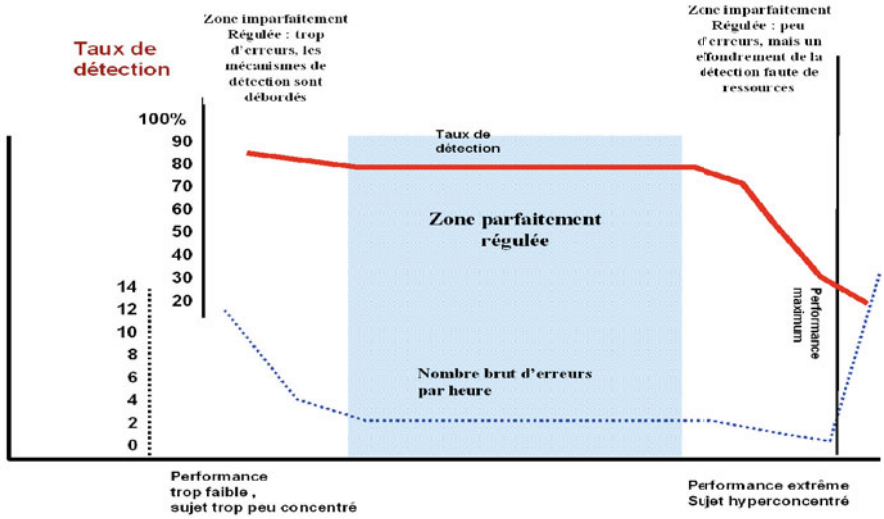
Lutter contre les fausses bonnes idées : les routines augmentent quand la tâche se complexifie.
Quand la tâche devient plus complexe, les domaines d'incompréhension se multiplient. Le sujet redoute de commettre des erreurs de compréhension et investit prioritairement ses ressources dans ces activités de compréhension, au détriment des activités qu'il croit mieux maîtriser et qu'il traite par routine et sans contrôle. Le paradoxe est évidemment qu'il commet de plus en plus d'erreurs de routine.

L'expert redoute ces erreurs de routine et s'en protège par des contrôles en série. Mais finalement, ce sont bien ces erreurs de routine qu'il commet le plus, simplement parce que la limitation en ressources le pousse à utiliser le plus possible des comportements automatisés. On voit nettement apparaître ici les défenses en profondeur du système cognitif, qui n'a pas d'autre choix au départ que de consentir des risques (en automatisant ses comportements) pour faire face au goulet des ressources disponibles, mais qui se protège par la suite pour les risques acceptés par une série de contrôles.

Lutter contre les fausses bonnes idées : le taux spontané d'erreurs est considérable chez les humains mais ne prédit pas l'accident.
Ce taux peut atteindre 10 erreurs à l'heure en conditions inattentives et relaxées.
En conditions plus attentives, le taux moyen d'erreurs est plutôt de deux erreurs à l'heure (taux relevé en aéronautique civile sur des séries de plus de 3 000 vols, résultats obtenus grâce aux techniques de l'audit en ligne à grande échelle type LOSA, Line Oriented Safety Audit[22, 23]).
Ce flux d'erreurs prédit peu les accidents, car la très grande majorité, sinon la totalité des erreurs sont détectées et récupérées par l'opérateur lui-même.
Quand la situation demande une grande attention avec de forts enjeux de performance, l'opérateur peut encore réduire son taux d'erreurs vers 0,5 par heure. Mais paradoxalement, l'opérateur dans ces cas extrêmes ne perd pas le contrôle parce qu'il fait plus d'erreurs (il en commet moins), mais parce qu'il déséquilibre son système de régulation, et n'a plus les ressources suffisantes pour récupérer les quelques erreurs restantes.

L'accumulation de résultats sur la production et la détection d'erreurs[24] conduit à considérer les deux phénomènes comme liés dans une même logique cognitive. La fiabilité humaine relève d'un système en équilibre dynamique qui couple un taux de production d'erreurs et un taux de détection et de récupération.
Le système s'effondre aux deux extrêmes de la performance, soit parce que le sujet est *trop peu concentré* et le taux d'erreurs finit par déborder le taux de détection, soit parce que le sujet est *trop concentré*, commet peu d'erreurs, mais consomme pour ce faire toutes les ressources qui alimentent les boucles automatiques de détection de la cogni-

22. Amalberti R, Wioland L (1997) Human error in Aviation. Key note address at the International Aviation Safety Conference 1997 (IASC-97), Rotterdam Airport. In: H. Shoekkha ed, Aviation Safety, VSP BV: The Netherlands, p. 91-108.
23. Helmreich R (2000) On error management: lessons from aviation. Br Med J 320: 781-5.
24. Amalberti R (2001) La conduite des systèmes à risques. Paris: PUF.



tion. Dans ce dernier cas, la perte de contrôle survient paradoxalement quand le sujet ne commet quasiment plus d'erreurs (de Keyser[25] ; Wioland, Amalberti, opus cité).
Dans la réalité, il faut encore noter qu'une fraction importante des erreurs détectées ne nécessite pas de récupération par retour à l'erreur et correction immédiate (UNDO), simplement parce que beaucoup de ces erreurs (i) sont sans conséquences immédiates (on a laissé la lumière allumée au bureau), ou (ii) ouvrent de nouvelles options tout aussi acceptables que celles imaginées avant l'erreur (on voulait passer par telle rue, mais finalement on s'est trompé, on réorganise son plan, on ne revient pas sur l'erreur initiale, et on utilise un nouvel itinéraire compatible avec le but visé).
L'ensemble des mécanismes de production, détection et récupération est regroupé sous le terme de ***gestion de l'erreur***.

En médecine aussi… Les hôpitaux les plus sûrs ne sont pas ceux qui ont le plus d'erreurs mais ceux qui détectent et récupèrent le mieux les erreurs qu'ils ont commises[26].
Les auteurs étudient la mortalité ajustée à l'hôpital pour une cohorte de 84 730 patients ayant subi une chirurgie vasculaire dans tous les États-Unis. Les taux de mortalité varient beaucoup d'un centre à un autre (3,9 à 6,9 %), et la variable la plus explicative du taux de décès n'est pas le taux de complications bénignes ou graves survenues dans ces hôpitaux (quasi constant pour tous les établissements), mais la gestion défaillante de ces complications. Les patients des hôpitaux à forte mortalité ont deux fois plus de chances de mourir de leur complication majeure

25. De Keyser V (1996) Les erreurs temporelles et les aides techniques. In: La gestion du temps dans les environnements dynamiques, sous la dir. de Cellier JM, De Keyser V, Valot C. Paris: PUF, p. 287-310.
26. Ghaferi A, Birkmeyer J, Dimick J (2009) Variation in hospital mortality associated with inpatient surgery. N Engl J Med 361: 1368-75.

que dans les hôpitaux les plus sûrs. Ce résultat important conforte l'idée de plus en plus répandue que l'approche traditionnelle de la sécurité du patient passe à côté de plusieurs points essentiels du contrôle du risque, en étant trop centrée sur la prévention et l'évitement des problèmes et pas assez sur la récupération des problèmes déjà existants. C'est une véritable relecture et un repositionnement de l'approche de sécurité qu'il faut accepter de réaliser.

Trois biais récurrents sur l'erreur humaine

L'étude des erreurs humaines est parsemée de biais. Trois sont particulièrement importants : la reconstruction après coup, l'attribution excessive de la causalité de l'erreur à l'opérateur de front de ligne, et le lien inexact entre erreur et accident.

Les catastrophes industrielles ont largement participé à l'engouement général pour l'étude des défaillances humaines et des erreurs humaines. Sans le nucléaire et ses catastrophes de Three-Miles Island et Tchernobyl, et plus récemment de Fukushima, sans l'aviation et l'accident de Ténériffe, et sans la catastrophe de Bopal pour la chimie, les théories sur l'erreur, la sécurité, et la fiabilité humaine auraient très peu progressé.
En retour, l'utilisation des connaissances sur l'erreur a été particulièrement intensive dans la sécurité des systèmes complexes, mais pas toujours très heureuse par le fait de multiples contresens, ou de transferts trop partiels de la théorie à la pratique.
Malgré, ou à cause, de cette profusion de littérature à la mode et inégale où tout peut se lire et son contraire, on a vu s'installer trois biais récurrents dans l'utilisation industrielle de l'analyse des accidents.

Reconstruire après coup

Le premier biais est celui d'*hindsight* ou de « **reconstruction après coup** » de l'histoire de l'accident. On est tenté de prêter à l'opérateur un comportement rationnel attentif à tout, et de le juger sur la base de ce que l'on a découvert dans l'enquête, notamment d'un passé d'incidents annonciateurs qui aurait dû l'alerter. Mais dans la plupart des cas, l'opérateur travaillait en routine, n'était pas au courant du passé des incidents annonciateurs, et n'imaginait pas se mettre dans des conditions dramatiques par ses décisions. Tout écart à un suivi idéal de la procédure est vu *a posteriori* comme une erreur ou une violation, alors que ces écarts se justifient dans la réalité du contexte de l'instant (gestion de la charge de travail de l'instant, anticipation, perturbation externe…[27]).

27. Lire le très bon commentaire écrit par Dave Woods sur le biais d'hindsight dans l'enquête sur l'accident de la navette Columbia http://researchnews.osu.edu/archive/hindbias.htm.

Attribuer tous les torts au dernier qui a fait l'action causant le sinistre

Le second biais est **l'attribution excessive de la cause des accidents aux opérateurs de première ligne** (les personnes qui sont dans l'action). Les facteurs liés à la complexité globale des systèmes disparaissent dans la plupart de nos analyses rationnelles qui veulent décomposer le travail en sous-parties distinctes[28]. Mais attention ! Il ne s'agit pas de basculer simplement l'analyse en considérant que les causes trop centrées sur l'opérateur doivent maintenant être analysées sous leur forme « profonde » en accusant les erreurs latentes de la conception et de l'organisation. Le modèle de Fromage Suisse de Reason a malheureusement induit ce biais dans l'industrie aussi grave que les précédents… car il ne fait que faire passer le « token » des causes à l'une ou à l'autre de ces parties, ce qui revient toujours *in fine* à commettre les mêmes fautes d'attribution et à ne pas traiter « le tout » (lire à ce sujet Dekker[opus cité], ou Johnson et Holloway[29]). L'enjeu est au contraire de considérer le modèle de couplage dynamique de toutes les parties du système.

Un troisième biais va dans le même sens : l'analyse se limite le plus souvent à ne considérer qu'un univers habituel de causes déjà connues et répertoriées (opérateurs, organisation, management, conception). Chris Johnson parle de « manque d'imagination »[30] des analystes « incapables de voir le non-standard » dès qu'une cause habituelle est attrapable. Le résultat est dramatique à la fois pour la compréhension des accidents, et pour les actions promulguées à la suite des accidents : les actions décidées pour chaque sous-secteur jugé défaillant entraînent une complexité croissante des protections locales, souvent contradictoires entre elles par le fait d'une conception en silo séparé, et dont le résultat est au mieux inefficace et au pire plus dangereux pour la situation globale.

Heureusement, ou malheureusement, ce handicap de sécurité lié à l'absence de vision globale ne caractérise que les systèmes industriels les plus sûrs ; les systèmes plus simples profitent longtemps d'actions locales. Un modèle de sécurité traité par parties et trop localement ne devient vraiment un inconvénient qu'au fur et à mesure que l'on sécurise ce système, mais il est alors aussi plus difficile à abandonner, car il est adossé à la mémoire de tous les succès passés de la progression du système.

Confondre erreur et accident

À force de se centrer sur les défaillances, des ambiguïtés durables se sont installées sur le lien erreur-accident. On confond souvent les deux termes, et on diabolise toute défaillance dans une quête d'optimalité d'un système cognitif assimilé au fonctionnement d'une machine.

---

28. Dekker S (2006) Ten questions about human errors. Avebury-Ashgate Publisher.

29. Johnson C, Holloway C (2004) Systemic failures and human error in Canadian aviation reports between 1996 and 2002. In: HCI in Aerospace 2004, sous la dir. de Pritchett A et Jackson A, Eurisco, Toulouse, p. 25-32.

30. Johnson C (2004) Human Error and the Failure of Imagination, In: Human Error, Safety and Systems Development, sous la dir. de CW Johnson, P. Palanque, Préface. Kluwer Academic Press.

On a minimisé pendant vingt ans le rôle structurant de l'erreur dans la résolution de problème. On a aussi négligé l'accumulation de résultats démontrant que l'opérateur commet beaucoup d'erreurs, mais en récupère la plupart.

On oublie aussi trop facilement que faire des erreurs (de routine notamment) est un prix à payer pour travailler vite, et donc pour une certaine efficacité sociale et économique. Vouloir tout contrôler et tout éviter en matière d'erreur se solde généralement par une lenteur telle dans l'exécution que le risque le plus redouté se transfère sur « ne pas faire le travail lui-même ».

Ainsi, une infirmière pourrait probablement réduire son nombre d'erreurs de routine en se concentrant sur chacun de ses gestes, tout comme un ouvrier sur son métier, mais dans ce cas, elle traiterait probablement cinq fois moins de patients dans la matinée (c'est le cas d'une infirmière novice). Si on adopte un critère d'analyse systémique, on conçoit qu'on pourrait prendre plus de risques pour les patients à ne *faire strictement aucune erreur de routine dans la prise en charge d'un patient donné* du service (erreurs de routine qui sont, comme on l'a vu précédemment, récupérées à 90 % sans avoir de réelles conséquences sur le patient), tout en acceptant le risque secondaire *de ne pas traiter des patients laissés pour compte dans le même service faute de temps disponible.*

Il a fallu attendre des circonstances plus favorables pour commencer à changer le mode de pensée dominante sur l'erreur, au moins dans les sphères de la recherche. L'industrie s'est aperçue de deux problèmes récurrents avec les approches classiques de sécurité : (a) son taux d'accident arrivait en plateau malgré l'optimisation des solutions de blocage des erreurs (Amalberti, 1996, op cité), et (b) la course à toujours plus de procédures pour obtenir toujours moins d'incidents et d'accidents sécrétait les germes d'une moins grande adaptabilité des opérateurs, faisant perdre une partie de leur utilité pour la gestion des risques.

Toutes les conditions étaient réunies pour une bascule théorique et pratique des idées sur la fiabilité humaine. En quelques années, le paysage de la recherche a changé, avec une révision profonde de ce que l'on entend par « bon » fonctionnement cognitif.

Le « bon » fonctionnement cognitif des opérateurs, celui qui serait recherché par l'entreprise comme étant le plus « sûr », ne doit plus se décliner en termes de recherche de fonctionnement absolument sans erreur, et particulièrement de moindre déchet instantané (évitement de toute erreur et défaillance ou récupération absolument immédiate, temps de réponse minimal, compréhension maximale).

Il se décline plutôt en termes de ***compromis*** permettant une atteinte *dynamique* de l'objectif (mais on devrait dire « des » objectifs) avec une ***performance suffisante.***

Trois idées sont centrales dans cette révision théorique :

– celle de suffisance de la performance, souvent comprise à tort comme le reflet d'une certaine paresse ou d'un certain laxisme. Elle doit plutôt être comprise comme une réponse adaptée à l'environnement apportant une satisfaction sociale à celui qui fait le travail, compte tenu de ses buts, du contexte, du regard des autres, des attentes sociales, et de ce qu'il sait faire. La notion de « suffisance » est reconsidérée à chaque exécution, et n'est pas contradictoire avec une performance très élevée et un coût cognitif élevé (par exemple un jour d'examen) ;

– celle d'adaptation dynamique, avec des fluctuations importantes de performance dans le temps, mais finalement une réponse globale acceptable à l'échéance visée. Le temps disponible et les échéances visées sont les unités sur lesquelles il faut juger la performance cognitive, et non le résultat à chaque instant de ce temps disponible avant que les échéances ne soient atteintes. Les erreurs s'avèrent n'être finalement que le prix à payer à un compromis bien contrôlé, et ne sont souvent que des variables secondaires dans la maîtrise de la situation ;
– enfin celle de métacognition ou de réflexivité (le regard sur soi), qui permet de régler la gestion des risques acceptables et acceptés, et notamment du contrat de performance de départ.

Le concept de « suffisance » comme outil cognitif de gestion de risques contradictoires

> On ne demande presque jamais une performance maximale aux opérateurs (performance qui serait d'ailleurs très différente d'un opérateur à l'autre), mais on demande plutôt une « performance suffisante » pour l'objectif social du système de production (une performance telle que tous les opérateurs puissent l'atteindre, et qui soit donc ainsi plus prédictible).
> Cette « suffisance » (ce qu'il suffit de faire) s'inscrit comme un reflet pratique de l'ambition du moment où on réalise un travail, et de notre compréhension des attentes sociales en général.
> Elle touche la sécurité comme les autres domaines. Chaque opérateur intègre et ajuste en permanence sa représentation de ce qui « suffit » pour le contexte dans lequel il est.

L'estimation de « suffisance » renvoie à des mécanismes très variés et très sophistiqués dans la cognition, pour une partie automatisés dans la gestion de l'expertise, qui peuvent aussi expliquer des débordements dans la prise de risque si l'on n'a pas pris certaines précautions dans la façon dont on organise le poste de travail.

Suffisance dans la représentation mentale et la planification

Il est parfaitement inutile pour un humain voulant décider de l'action à mener de rechercher un isomorphisme parfait entre le monde réel et la représentation qu'il s'en fait, c'est même un handicap.
Des écoles éloignées géographiquement (Norman aux États-Unis, 1983[31] ; Ochanine en Russie, 1981[32] ; Piaget en France, 1974[33]) avaient toutes très tôt, avec des mots différents, souligné la déformation des modèles mentaux par rapport au monde réel, leur laco-

31. Norman D (1983) Some observations on mental models. In: Mental models, sous la dir. de G. Stevens et S. Gentner. Hillsdale, NJ : LEA.
32. Ochanine D (1981) L'image opérative, actes d'un séminaire et recueil d'articles. Université Paris V.
33. Piaget J (1974) La prise de conscience. Paris: PUF.

nisme et leur finalisme, et *in fine*, avaient souligné l'utilité de ces déformations en termes de réussite dans l'action (et la communication).

Ces simplifications et déformations du réel sont des réponses à l'impossibilité psychologique, intensive et qualitative, de tout percevoir, tout savoir, tout comprendre, et tout faire (une idée aussi au centre des travaux d'Herbert Simon, prix Nobel en 1978 pour ses travaux sur la rationalité limitée[34]).

D'ailleurs, le modèle mental[35] ne sert pas en premier à refléter un réel, il sert à prédire ce que l'on va faire, ce qui peut arriver, et cette fonction est essentielle.

La représentation du monde permet à l'opérateur de transformer mentalement le monde, de redouter des événements et d'anticiper des corrections (notion de fonction de précorrection de Piaget, op cité). À preuve, les standardistes expertes, les médecins, comme les pilotes experts, passent plus de temps à éviter par avance les problèmes, qu'à gérer des problèmes réels[36]. Les travaux sur la planification et la résolution de problème ont régulièrement retrouvé ces propriétés de l'adaptation et de la correction par anticipation[37].

Inversement, l'intérêt de tout planifier et tout anticiper a ses limites dans la conduite pratique du travail par l'opérateur. Il planifiera activement des alternatives tant que persistent des doutes sur la crédibilité de sa solution retenue, ou qu'il estime que le coût de sa mise en jeu est trop important, et notamment pas assez facile pour lui. Mais la planification s'arrêtera bien souvent avant d'atteindre la capacité maximale de raffinement dont il serait capable. On parle[38,39] de « coût cognitif utile » : quel intérêt aurait l'opérateur à sophistiquer son plan, si c'est pour ajouter des éléments qui vont se périmer (l'action n'est pas exécutée immédiatement et le contexte va changer), ou si ce qui est déjà acquis est suffisamment robuste compte tenu des savoirs possédés et des enjeux. En fait le plan le plus important avant l'action doit surtout fixer l'ambition de résultat (le contrat de performance), cerner les points durs probables de l'exécution, se protéger ou les éviter par une réflexion préalable ; le reste de l'exécution s'accommode sans problème d'une adaptation en ligne, comme le montre l'ensemble des études sur le pilotage de combat et la préparation des situations à risques (Amalberti[40,41]).

---

34. Simon H (1982) Models of bounded rationality, vol. 1. MIT Press.

35. Les termes « modèle mental » et « représentation mentale » sont synonymes en français et peuvent être interchangés.

36. Falzon P, Amalberti R, Carbonell N (1986) Dialogue control strategies in oral communication. In: The future of command languages: foundations for Human Computer communication, sous la dir. de D. Hopper et IA Newman. North Holland: Elsevier Science Publisher, p. 73-98.

37. Hoc J M (1988) Cognitive psychology of planning. London: Academic Press.

38. O'Hara K, Payne S (1998) The effects of operator implementation cost on planfulness of problem solving and learning, Cognitive Psychology 35: 34-70.

39. O'Hara K, Payne S (1999) Planning and the user interface : the effect of lockout time and error recovery cost. International Journal Human Computer Studies 50: 41-59.

40. Amalberti R (2001) La maîtrise des situations dynamiques. Psychologie Française 46-2 : 105-17

41. Amalberti R (2002) Use and misuse of safety models in design. Lecture Notes in Computer Science 2485: 1-21.

Suffisance dans le domaine de la décision

Le renouveau des théories sur la décision naturelle[42,43] a amené plusieurs arguments à l'idée de suffisance. Ce courant de travaux a accumulé des observations dans presque toutes les industries à risques (aviation civile, transports publics, nucléaire, chimie, pompiers, activités militaires, urgences médicales…).
Il met en évidence que les biais dénoncés dans les théories classiques de la décision humaine[44] sont en fait sans réelle importance ni pertinence en situation naturelle complexe et dynamique.
Les observations sur le terrain montrent en effet que la décision est un processus continu, couplé à l'environnement. Ce processus passe par des décisions partielles, plus ou moins pertinentes, mais qui dans le flot, finissent en général par conduire à des résultats acceptables compte tenu des marges des situations réelles. Dans bien des cas, la décision en contexte est relativement guidée par les traits de la situation (l'affordance[45]). Enfin, les opérateurs ont souvent une bonne connaissance des « mondes » auxquels s'appliquent ces décisions, si bien que des décisions en théorie peu valides sont finalement peu dangereuses, notamment grâce aux réactions adaptées des autres agents cognitifs du monde environnant ; pire ou mieux, les opérateurs ont une forte expertise sur ce qu'ils peuvent contrôler en termes d'écart, et tolèrent de ce fait une faible validité de leur décision tant qu'ils considèrent qu'elle ne les conduit pas dans une situation en impasse par rapport à leur expertise.

Suffisance dans le domaine du contrôle et de l'exécution

Compte tenu des caractéristiques de « suffisance » de la représentation, le modèle mental est loin de spécifier toute la procédure à mettre en jeu pour l'exécution ; il contient seulement les éléments guidants essentiels et s'appuie presque uniquement sur l'interaction routinière avec les marqueurs lus dans l'environnement pour progresser vers son but.
Gibson et Crooks[46] dans un article historique (1938) sur la conduite automobile parlaient d'attirance spontanée (d'espace d'affordance). Des régions désirables, attirantes pour l'action (*safe field of travel* : régions sans obstacles, éclairées, dont on perçoit les possibilités d'interaction) émergent de l'environnement et s'imposent à un

42. Klein G, Zsambok CE (1997). Naturalistic Decision Making. Mahwah, NJ: LEA.

43. Gibson J (1979) The ecological approach to visual perception. Boston: Houghton-Mifflin.

44. Kahneman D, Slovic P, Tversky A (1982) Judgement under uncertainty: heuristics and biases, Cambridge, Ma: Cambridge University Press.

45. Le terme affordance est un néologisme provenant de l'anglais, signifiant l'idée d'inciter, d'inviter. Il se rapporte à une structure physique de l'environnement qui favorise spontanément une action particulière sur cette structure physique (par exemple pousser ou tirer une porte en fonction de la forme de la poignée) (voir Norman D (1988) The design of everyday things. New York : Double Day Curency, pour un développement du concept inspiré de Gibson).

46. Gibson J, Crooks L (1938) A theoretical field analysis of automobile-driving. American Journal of Psychology 51: 453-71.

guidage perceptif automatisé, alors que des régions dangereuses sont naturellement évitées (région dans l'ombre, sols mal visibles). Cet espace désirable intègre le résultat de toutes les contraintes perçues ou imaginées, y compris sur ses propres compétences à agir (on retrouve bien sûr ici un précurseur de la notion d'espace problème de Newell et Simon[47], à ceci près, que l'espace est ici largement guidé par l'environnement et ses représentations externes, physiques).
Le modèle fait le pari que l'opérateur va chercher dans sa lecture de l'environnement le chemin le plus attirant, faisant le plus sens pour progresser en routine vers le but.
Maturana et Varela[48] vont encore plus loin en considérant que la « réalité perçue » n'est une construction consensuelle, qui naît dans ce couplage dynamique avec l'action pour guider l'action dont on est capable. Ces auteurs parlent d'autopoëise et d'énaction pour dire que la « réalité perçue » émerge littéralement par le contact entre les motivations et les circonstances locales, et qu'elle évolue sans arrêt au gré de ce couplage dynamique.

Deux niveaux de supervision

Tous ces travaux sur la suffisance convergent vers un modèle cognitif de l'individu qui gérerait en parallèle deux supervisions pour assurer la maîtrise de la situation : celle du processus physique et de la situation (on parle de contrôle ou de supervision externe), et celle de soi-même, acteur cognitif du processus (on parle de contrôle ou de supervision interne). Ces deux supervisions souvent en conflit d'intérêt expliquent la nécessité fondamentale de mécanismes de compromis et de suffisance.
La supervision du processus externe[49] permet un usage intensif des routines en s'appuyant sur la planification et sur le guidage procuré par les attirances de l'environnement. Ce n'est qu'en cas de problèmes et de blocage des processus routiniers que la sollicitation cognitive augmenterait ; il faudrait alors à la fois procéder à un usage plus intensif de la cognition, mais aussi réguler cette intensité pour qu'elle rende des résultats utiles aux dates butées du processus qui continue à évoluer. [50]

Orientation des rondiers dans les couloirs des centrales nucléaires.
En utilisant une simulation réaliste[50], une étude montre que les rondiers de centrale nucléaire contrôlent leur activité de déplacement uniquement à de rares points clés et sans véritable prise de conscience de ce contrôle. Soixante pour cent de ces points clés correspondent à des endroits où la confusion entre couloirs est maximale (mêmes couleurs, ressemblances diverses) et source évidente d'erreurs. Ces contrôles sont relativement communs à tous les rondiers, comme s'ils étaient déclenchés par simple

47. Newell A, Simon H (1972) Human problem solving. Englewoods Cliffs, NY, Prentice HAll.
48. Maturana H, Varela F (1992) The tree of knowledge, the biological roots of natural understanding. Shambala publications.
49. Zangh J, Norman DA (1994) Representation in distributed cognitive tasks. Cognitive Science 18: 87-122.
50. Noizet A, Amalberti R (2000) Le contrôle cognitif des activités routinières des agents de terrain en centrale nucléaire : un double système de contrôle. Revue d'Intelligence Artificielle 14(1-2): 73-92.

contact avec des traits particuliers de l'environnement. En revanche, les 40 % des contrôles restants sont sans lien à l'environnement, et surtout variables en fonction de la pression de travail pour chaque rondier. Tout laisse à penser que ces contrôles sont surtout dirigés vers la supervision de leur propre comportement (je me suis laissé distraire, ou je pense trop à ça et pas assez à mon travail immédiat).
Quand on soumet ces rondiers à une variation de pression temporelle (faire plus vite le travail), les contrôles externes restent stables, mais les contrôles personnels s'organisent différemment, sont plus rapprochés dans le temps, probablement pour mieux surveiller le risque mécaniquement croissant d'erreurs et de débordement.

La supervision interne ou cognitive (du processus mental) répond à des objectifs complémentaires de la supervision externe du processus physique[51] :

- d'une part, il s'agit de décider du lancement au bon moment d'opérations cognitives exigeant de l'attention (et donc contraintes en volume), centrées sur la (re)planification, la compréhension et la construction de nouvelles solutions, quand les routines sont bloquées ou les autoévaluations de performance négatives ;
- d'autre part, comme les processus attentionnels sont des processus lents et séquentiels, il s'agit de décider en continu des priorités, et *souvent de décider quels* arrêts (de réflexions en cours) sont à faire pour libérer des ressources (réduire la charge mentale) et pouvoir réfléchir à des objets prioritaires. La métacognition (le regard sur soi) est fortement sollicitée dans tous ces arbitrages. On commence à comprendre la nature de ces arbitrages. Certaines solutions sont locales : la priorité est en général donnée par l'opérateur à la fermeture des tâches en cours avant d'ouvrir d'autres pôles d'investissement. L'opérateur sait aussi réaliser des contrôles très sophistiqués pour gérer le partage de tâches en temps réel, comme le démontrent des résultats sur les pilotes d'avions[52]. Les pilotes disposent de savoir-faire pour passer d'une tâche à l'autre en minimisant les risques : estimation de butée temporelle, de temps restant avant achèvement de la tâche précédente, estimation de stabilité et prédiction des tâches dans le futur immédiat, utilisation des réseaux de redondances informelles et repérage symbolique d'alertes pour revenir sur une tâche laissée pour compte. D'autres solutions s'appuient sur l'ouverture de boucles cognitives parallèles qui vont travailler sur le processus à différents niveaux de profondeurs temporelles. Ce parallélisme, qui se couple nécessairement à un rendement sub-optimal pour chaque activité (puisqu'il faut se partager), n'est qu'exceptionnellement fatal parce que les situations réelles sont bien plus tolérantes que les situations de laboratoire. La faible exigence du monde extérieur génère des marges pour l'efficacité de l'action, et mécaniquement réduit les effets des erreurs. Cette faible exigence n'est évidemment pas fortuite : elle résulte pour une grande part de l'organisation

51. Hoc JM, Amalberti R (2007) Cognitive control dynamics for reaching a satisficing performance in complex dynamic situations. Journal of cognitive engineering and decision making 1: 22-55.

52. Valot C, Amalberti R (1992) Metaknowledge for time and reliability. Reliability Engineering and Systems Safety 36: 199-206.

du monde et des métiers, pour lesquels l'homme, en façonnant l'environnement, devient son propre générateur de marge et son propre « affordeur ».

On vient de le voir, la suffisance dans l'action passe par l'utilisation du temps et des niveaux de compréhension.

Le réglage de la suffisance par le temps

Le temps disponible est sûrement, après la suffisance, la deuxième grande valeur mal comprise de la cognition dans la littérature sur la fiabilité. La logique expérimentale n'a souvent vu dans le temps qu'un instrument de mesure (le temps de réaction ou de réponse). Plus le temps de réponse à un stimulus est long, plus il est apparu naturel de considérer que la situation était complexe à résoudre, ou que le processus intellectuel étudié était déficient (il pouvait s'agir de perception, de raisonnement ou de toute autre activité).

Récemment, le temps est redevenu un objet d'étude propre, et pas seulement un instrument de mesure. Les travaux sur les environnements dynamiques ont servi de catalyseur à cette révision[53].

Le temps est un outil de gestion de la sécurité sous deux angles :

- d'une part, il est encodé dans la représentation même de l'activité et sert d'indicateur temporel pour l'organisation du travail. De Keyser (1996) introduit la notion de systèmes de références temporelles pour montrer l'existence d'échelles totalement différentes de temps qui évoluent en parallèle dans les tâches professionnelles : certaines sont à l'échelle de la seconde, d'autres à l'échelle du mois. L'opérateur joue souvent sur les butées maximales comme des valeurs de repères sur lesquelles il peut organiser son activité en temps partagé. Ces butées multiples peuvent parfois le tromper, mais dans la grande majorité des cas, l'opérateur gère très bien ces systèmes de temps parallèles, et s'en sert comme marqueurs naturels de la répartition de ses activités au cours de la journée ;
- d'autre part, le temps est un moteur de la transformation du monde, et possède un potentiel de résolution propre des problèmes et des erreurs. Parce que les situations sont dynamiques, le problème d'un moment n'est en général pas le problème du temps suivant ; ne rien faire peut ainsi résoudre beaucoup de difficultés. De même, le temps, en changeant la situation et en accumulant mécaniquement les informations, transforme dans beaucoup de cas un problème complexe en un problème simple, particulièrement dans les systèmes très instrumentalisés ; les humains le savent et se servent constamment de cette propriété. Il est plus facile de gérer des situations prototypiques, pour lesquelles des réflexes de réponses sont connus et efficaces, que de gérer des situations floues pour lesquelles il faut d'abord investir en compréhension et où le risque d'erreur d'action est plus élevé.

53. Cellier JM, de Keyser V, Valot C (1996) La gestion du temps dans les environnements dynamiques. PUF: Paris.

Les contrôleurs de l'air laissent « le temps au temps » pour se simplifier le travail. Morineau[54] montre par exemple, en étudiant les situations de contrôle aérien, que les contrôleurs ne déclenchent le traitement des conflits que quand tous les éléments du conflit sont présents sur l'écran, et que tous les moyens d'actions sont disponibles. Le conflit est souvent vu depuis longtemps, mais difficile à caractériser dans des conditions partielles, et souvent impossible à corriger par les méthodes les plus faciles si le contrôleur se précipite dès qu'il le voit ; attendre devient un avantage évident, y compris en termes de gestion de la charge de travail. Enfin, la construction de l'artefact (les écrans de contrôle)[55] est pensée pour fournir les moyens à l'opérateur de disposer de marges confortables pour gérer les conflits.

Il en va exactement de même avec le contrôle des erreurs ; le temps est souvent un outil précieux pour repérer ses erreurs, voire pour en réduire les conséquences. Cette propriété du temps est développée à travers quelques exemples dans le paragraphe suivant, car elle est à la base de la régulation écologique des risques.

Le réglage dans le temps de la compréhension

Les opérateurs, s'ils ont le choix, préfèrent agir à comprendre, car l'action aide la compréhension. Ces façons de faire simples et spontanées contrarient souvent les services de sécurité des industries, et sont chroniquement combattues. C'est le cas dans le développement récent de la notion de conscience de la situation, qui, mal comprise et mal reprise par les personnes en charge des procédures de sécurité, laisserait supposer que la situation doit être totalement comprise à chaque instant avant d'agir[56]. C'est simplement impossible pour l'opérateur, et même dangereux pour la conduite du processus, car la vitesse de construction d'une représentation exhaustive du monde est beaucoup plus lente que la vitesse de changement de la situation, et il en résulterait souvent une lenteur d'exécution produisant une solution idéale mais hors des délais possibles d'intervention. Seuls des processus très lents comme le nucléaire peuvent s'accommoder (et encore dans certains cas seulement) d'une consigne de « non-action » pendant un temps fixé à l'avance et réservé à la réflexion après la survenue immédiate d'un incident. Plusieurs expérimentations dans des processus plus rapides, comme en aéronautique[57], montrent que les pilotes exposés à des pannes ne cherchent pas à

54. Morineau T, Hoc JM, Denecker P (2003) Cognitive control levels in air traffic radar controller activity. Int Journal of Aviation Psychology 13 : 107-30.

55. Dans l'exemple du contrôle aérien, l'écran radar fournit un zoom sur la situation qui laisse plusieurs minutes aux avions pour traverser l'écran de part en part ; l'écran dispose aussi de repères de distances sur des cercles concentriques, qui facilitent le positionnement relatif des avions les uns par rapport aux autres.

56. Endsley M (1995) Toward a theory of situation awareness in dynamic systems. Human Factors 37: 32-64.

57. Plat M, Amalberti R (2000) Experimental crew training to deal with automation surprises. In: *Cognitive Engineering in the Aviation Domain*, sous la dir. *de* NSR Amalberti, Hillsdale- New Jersey: Lawrence Erlbaum Associates, p. 287-308.

obtenir une compréhension totale avant d'agir ; ils limitent au contraire leur analyse et préfèrent agir vers l'objectif pour rester compatibles avec la dynamique de la situation.

Le réglage dans le temps de la gestion des erreurs

La confiance[58] dans la capacité à maîtriser les risques est au centre du contrôle cognitif du risque.

Dans un travail de thèse effectué sur la régulation des appels d'urgences au Samu 75, Marc[59] étudie la contribution de chaque membre de l'équipe à la sécurité du groupe. On regarde particulièrement le temps écoulé et les critères d'intervention des individus (signalisation aux autres, récupération sur décision personnelle) pour récupérer un risque détecté dans la situation collective. Les résultats montrent que les opérateurs téléphoniques attendent souvent plusieurs minutes entre le moment où ils perçoivent l'accumulation de ratés dans le traitement des appels et leur intervention pour corriger ces ratés ; ils interviennent plutôt par « touches » successives, augmentant le niveau d'alerte du groupe, avant de véritablement provoquer une alerte forte ou tenter une récupération. Tout se passe comme si les opérateurs acceptaient que le groupe dérive en permanence vers un niveau de risque significatif, tout en intervenant en butée sur ce niveau de risque pour le garder à une échelle gérable et réversible. On peut trouver plusieurs rationalités à ces comportements : gestion croisée de leur propre charge de travail avec l'activité au profit du groupe, contrôle des interruptions sur les autres pour limiter d'autres risques, ou confiance dans le temps et les autres acteurs pour corriger les problèmes. [60, 61]

L'utilisation du temps en médecine générale pour se faciliter le travail[60, 61].

Une étude récente a porté sur près de 1 000 dossiers de plaintes de médecine générale sous l'angle de la maîtrise du temps et du risque d'erreur associés.

L'activité médicale gère une immense variété de cas et de situations, qui sollicite plusieurs types d'anticipations pour garder le contrôle du patient et du cabinet. L'analyse propose 4 différentes sources de temps, ou tempos, qu'il faut contrôler chacun pour ce qu'il représente de risques propres, et au niveau du tout (de la synchronie de ces 4 tempos) pour garder le contrôle global de la situation.

L'art du médecin consiste à jouer des temps plus qu'à être pris par le temps. Le temps est un révélateur de l'évidence. Plus on attend, plus les phénomènes qui ont une évolution propre se révèlent. Jouer avec le temps est donc fondamental, particulièrement en ville puisque les patients ont des pathologies plus volontiers débutantes.

58. Valot C, Amalberti R (1992) Metaknowledge for time and reliability. Reliability Engineering and Systems Safety 36 : 199-206.

59. Marc J, Amalberti R (2002) Contribution de l'individu au fonctionnement sûr du collectif : l'exemple de la régulation du SAMU. Le Travail Humain 64: 201-20.

60. Amalberti R, Brami J (2011) Tempos management in primary care: a key factor for classifying adverse events, and improving quality and safety, BMJ Quality & Safety Online First, published on 2 September 2011 as 10.1136/bmjqs.2010.048710.

61. Brami J, Amalberti R (2009) Les risques en médecine générale. Springer Verlag France: Paris.

En même temps, le temps gagné sur l'une des dimensions citées précédemment est toujours réutilisé pour un bénéfice, pour une autre dimension (on peut parler de crédits de temps). La personne âgée qui vient pour un renouvellement d'ordonnance ne sera pas déshabillée, et ce temps gagné profitera peut-être à la demi-heure d'explication qu'il faut consacrer à une annonce difficile à la jeune patiente d'après, ou à un temps social gagné à la maison par un retour plus tôt que d'habitude. Tous les temps et tous les tempos s'échangent dynamiquement ; ce que l'on donne à l'un est enlevé aux autres, mécaniquement, puisque l'écoulement total du temps est lui guidé par des lois physiques externes. Cette gestion peut être aidée, elle est tout sauf intuitive, et son dérapage chronique peut conduire à une explosion des erreurs médicales.
Les 4 tempos identifiés sont :
– **le tempo de la maladie et du traitement**. Il classe le patient dans une boîte de temps disponible pour guider l'action que l'on a avec lui, le revoir, le transférer, le gérer avec des boucles externes importantes. Le docteur sait par exemple que la plupart des cancers ont une évolution assez lente pour autoriser une exploration sans hospitalisation, sans prendre de risques inconséquents d'aggravation sur une période de 1 à 3 mois (le temps de récupérer tout le bilan) ;
– **le tempo du patient**. Le patient contrôle une partie de l'agenda de sa maladie ; il décide d'exprimer ses symptômes selon des modalités fortement pondérées par sa personnalité et ses propres angoisses. Il se plaint souvent de retard de diagnostic mais les études montrent qu'il est lui-même très souvent participatif à ces retards, tardif dans sa demande, négligent dans l'exécution des examens prescrits, noyant la demande dans un concert d'autres demandes jugées plus prioritaires, ou simplement participant par son ton et ses attitudes à réduire l'échange avec le médecin[62, 63] ;
– **le tempo du cabinet** est le plus familier. Il conjugue (i) le temps de l'examen, (ii) les interruptions incessantes, qu'il s'agisse de téléphone, de malades surajoutés, de visites impromptues, (iii) tous les temps administratifs à glisser dans la journée, (iv) et les temps privés. La médecine n'est qu'un morceau de vie, et il faut souvent accorder des priorités ponctuelles à des temps de vie privée glissés dans l'agenda professionnel ;
– **le temps du système médical**. En ville les patients sont libres, toute prescription d'examen ou de consultation spécialisée est balistique. On ne sait jamais totalement quand le patient va revenir, va obtenir le rendez-vous, va obtenir le résultat…

62. Barber N (2002) Should we consider non-compliance a medical error? Qual Saf Health Care 11: 81-4.

63. Buetow S, Kiata L, Liew T, *et al.* (2009) Patient error : a preliminary taxonomy. Ann Fam Med 7: 223-31.

Synthèse : un modèle de sécurité individuelle basé sur la construction permanente de compromis

Les bases de ce qui pourrait être appelé une théorie de sécurité écologique[64] éclairent d'un jour complémentaire certains acquis de la littérature sur la maîtrise des situations dynamiques.

La clé d'une interprétation cohérente des résultats réside dans les points suivants :

- la maîtrise de la situation exige une double supervision : celle du processus externe et celle du processus mental ;
- la priorité des activités cognitives du champ conscient est d'assurer la supervision de la charge de travail et de la progression cohérente vers le but ; quand celle-ci est bien assurée, la supervision du processus physique peut être traitée à un niveau relativement routinier, en utilisant les savoir-faire fortement procéduralisés.

En bref, quand la maîtrise est assurée, la supervision du processus physique est largement automatisée, alors que la maîtrise de la situation (supervision interne) exige paradoxalement de mettre un frein constant sur soi pour ne pas être tenté d'entrer inutilement dans des optimums locaux (compréhension parfaite, action parfaite) décorrélés des demandes sociales et des butées de la situation.

La sécurité à l'intérieur de chaque supervision est assurée par des mécanismes cognitifs différents :

- pour la supervision externe (on surveille le résultat obtenu), les routines incorporent un premier niveau autonome de contrôle et d'ajustement. Ces contrôles ont un seuil de déclenchement relativement tardif, nécessitant une dérive significative des valeurs du processus physique pour activer (automatiquement souvent) l'exécution d'une routine de correction. Ainsi, plus la situation dérive de façon franche et rapide (mais en restant dans des limites habituelles et raisonnables), plus la correction sera facile à déclencher pour la routine (exemple du suivi de trajectoire latéral et horizontal en conduite automobile). Inversement, moins la dérive est franche et visible, plus le déclenchement de la correction demandera du temps, des ressources, et une sollicitation de la supervision interne avec une résolution de problème non routinière à la clé ;
- la supervision interne (on se regarde travailler) gère les activités attentionnelles nécessaires à la coordination du processus. Mais elle doit aussi s'économiser et utiliser un maximum d'arbitrage pour atteindre une « suffisance » compatible avec ses ressources. Tout point douteux ne peut pas être compris à fond, et le temps disponible (avant action nécessaire) laisse rarement la chance d'explorer toutes les solutions disponibles et connues. Flirter avec une expérience de risque qui demeure maîtrisable devient un outil de la gestion cognitive de tous les instants. Comme pour la supervision externe, mais ici avec un mécanisme différent, le contrôle tactique de la cognition s'appuie sur le temps restant avant les dates butées, et sur les *limites turbulentes* du système cognitif (NDA : la notion de *limites turbulentes* est reprise

64. Amalberti R (2001) La conduite des systèmes à risques. Paris: PUF.

du vocabulaire de Gibson), limites signalées par l'émergence d'alertes annonçant l'éminence de perte de contrôle. Ces alertes reflètent la prise de conscience de difficultés de supervision interne : trop d'erreurs, trop de temps à détecter les erreurs, trop d'autocensure à comprendre faute de temps et de ressources (alors que le sujet est certain qu'un peu de temps permettrait de comprendre), bref un sentiment de débordement quantitatif des actions à conduire. Par expérience et apprentissage, ces signaux sont tels qu'ils interviennent bien avant la perte réelle de maîtrise, dès les premières difficultés ressenties (notion de marges). Leur survenue s'accompagne d'un changement de stratégie et de mode de contrôle de l'opérateur, qui consiste le plus souvent à réviser son contrat d'objectif.

Le modèle de sécurité écologique : un investissement cognitif qui suffit aux objectifs poursuivis

La compréhension du cerveau humain révèle un fonctionnement extrêmement fiable et sophistiqué, tout à l'inverse d'un message d'insuffisance et de manque de fiabilité habituellement associé aux comportements humains, par méconnaissance, résultant d'études trop centrées sur les nombreuses erreurs (mal comprises) et les rares accidents (exagérément étudiés).

Rappelons ici que si près de 80 % des accidents graves dans les industries à risques ont une cause humaine, on observe aussi 99,9999 % des situations de travail sans accident grave[65], résultat largement obtenu grâce aux étonnantes capacités cognitives de l'opérateur.

Il est urgent d'en tirer les leçons pour les attentes que l'on a vis-à-vis de l'opérateur, et de revoir profondément les indicateurs et la façon dont on aborde le diagnostic de sécurité, notamment en réhabilitant les études de situations « normales » et en évitant le prisme réducteur des erreurs comme variable principale d'analyse.

Conséquence : suivre les procédures c'est pouvoir s'en écarter autour d'un point moyen…

Une vision naïve de la cognition « idéale » espèrerait de l'opérateur un gain de sécurité et une réduction des erreurs, si l'on arrivait à lui faire suivre idéalement à la lettre la procédure préconisée sans écart.

Cette attente est largement naïve et jamais atteinte pour au moins deux raisons :

– une raison sociologique, avec l'idée de la « fabrique de sécurité » proposée par Gilbert de Tersac dans son analyse de la catastrophe d'AZF[66] (dramatique explosion d'usine à Toulouse survenue le 21 septembre 2001, 10 jours après l'attentat des Twin Towers), « les règles de sécurité relèvent d'un travail d'organisation qui ne se réduit pas à l'énoncé de procédures à respecter, encore moins de constats d'écarts ou d'infractions, mais à l'invention de règles d'usages qui viennent compléter les règles formelles qui ne sont que des « règles papiers » tant que leurs destinataires ne les mobilisent pas » (page 10). Le passage de ces règles affichées, conçues par des

65. Dans la plupart des grandes industries à risques (nucléaire, transport…), le taux de catastrophe est de 1 pour 1 million (1×10^{-6}) d'unités de compte d'activité (par exemple mouvement aéroport, ou passager par kilomètre dans le rail).

66. De Tersac G, Mignard J (2011) Les paradoxes de la sécurité, le cas d'AZF. Paris: PUF.

happy fews de la direction et de la sécurité, aux règles appliquées par tous nécessite la construction de règles sociales de consensus sur l'appropriation et l'application non écrites, et une interprétation contextualisée de chaque acteur sur ce qui est acceptable ou non dans l'application de la règle et l'écart toléré. L'auteur appelle cette construction d'un joli terme : la fabrique de sécurité ;

– une raison cognitive, liée au modèle décrit dans les pages précédentes : même si la « fabrique de sécurité » arrivait à la conclusion que la règle formelle doit être suivie sans écart, cela serait tout simplement impossible pour l'opérateur, et même rapidement intolérable pour la direction. Le suivi sans écart de la règle entraînerait mécaniquement une baisse de la performance par l'exigence de contrôle renforcé qu'elle imposerait sur le contrôle cognitif (désengagement des routines, retour à un mode plus contrôlé et plus lent dans l'exécution). Ce ralentissement de la production serait tout à fait considérable, proche d'une performance de débutant, et sans doute d'un facteur d'ordre 2 à 3 fois inférieur au rendement « normal et espéré » de l'ouvrier/opérateur expert ! Par ailleurs, cette approche sans écarts correspondrait à un manque de *feedback* de la situation pour l'opérateur (un découplage au réel, un gommage des sensations en fonctionnant trop loin des limites « turbulentes et parlantes » de l'environnement), et s'avérerait à l'usage particulièrement inconfortable, contribuant à faire baisser sa vigilance et ses mécanismes naturels de récupération, et l'exposant à des dérives lentes de paramètres vues trop tardivement[67, 68].

> La cognition ne sait vraiment bien gérer ses risques internes et externes qu'en les côtoyant ; vouloir interdire à l'opérateur l'expérience de ces risques et lui imposer une marche sans écart est un non-sens psychologique et ergonomique.
> Bien sûr, le bénéfice de cette recherche constante d'exposition aux microvariations de l'environnement pour mieux les contrôler n'est efficace qu'à l'intérieur d'une enveloppe de niveaux de risques (et d'erreurs) convenue et habituelle (on pourrait dire quotidienne), pour laquelle l'opérateur possède des savoir-faire de récupération en routine. On ne parle pas ici d'exposition à des niveaux de risques dépassant les compétences de l'opérateur ou le surprenant totalement.

Les liens complexes entre sécurité et compétences : une courbe en U renversé

La représentation de ses compétences (la métacognition) est une autre variable déterminante d'une maîtrise réussie de la situation. Les critères que le sujet s'impose sur l'objectif (le contrat initial passé avec lui- même et l'entreprise) influencent toutes les stratégies et tactiques de supervision et sont la première source de réglage du niveau de risque qui va être accepté pendant l'exécution.
Ce modèle de réglage de la prise de risque ajusté en permanence sur le reflet de sa compétence et de sa confiance en lui n'a pas que des avantages pour la sécurité.

67. Rasmussen J (1997) Risk management in a dynamic society. Safety Science 27: 183-214.
68. Polet P, Vanderhaegen F, Amalberti R (2003) Modelling the border-line tolerated conditions of use. Safety Science 41: 111-36.

En effet, avec un tel système, plus on donne des compétences techniques à l'opérateur, plus il accumule les succès qui valident la maîtrise de sa situation, plus ses routines intègrent la capacité de récupération et s'ajustent (c'est un processus automatique, irrépressible, et sans prise de conscience du sujet) en allant chercher des limites turbulentes dans l'environnement plus loin (des signaux écarts) pour s'autocontrôler. L'opérateur expert conduit donc son processus en routine, sans même en être conscient, avec plus d'écarts à la règle que l'opérateur moins expert.

Mais ce n'est pas le pire pour la sécurité en matière de gestion des compétences. Sur le plan des processus conscients (le point précédent ne concernait que le réglage des processus routiniers), l'opérateur expert et surentraîné ajuste progressivement son contrat de performance en fonction de ses réussites et de ses échecs. Plus il accumule de réussites, plus sa cognition intègre qu'il peut élever son contrat de performance si la situation le nécessite. Ce mécanisme de *feedback* cognitif est automatique et largement irrépressible. En quelque sorte, le succès nourrit en retour la représentation des connaissances de l'expert, favorise la montée de sa confiance, et l'encourage mécaniquement à prendre plus de risques, et à toujours chercher à valider son savoir « un pont plus loin ». En retour, la reconnaissance de l'entreprise ou de la société pour la réussite (le statut de héros, ou à tout le moins le statut d'expert) renforce progressivement un certain niveau d'exigence vis-à-vis de soi-même dans les exécutions du travail à venir (montrer que l'on a bien ce rang d'expert).

Ce mécanisme d'autorenforcement de la confiance est à la base de l'apprentissage, et contribue longtemps à la sécurité pendant la courbe d'apprentissage (réduction progressive des erreurs, prise de confiance) ; mais il n'a pas de fin (l'expertise est infinie), et surtout, n'a que peu à voir avec la contrainte réglementaire externe.

En quelque sorte, peu importe ce que dit la règle imposée, plus on donnera de compétence technique à un opérateur sur son métier, plus sa cognition intégrera qu'il peut affronter des risques plus élevés pour le bénéfice d'une performance plus grande dans son travail ; il le fera d'abord dans des circonstances attendues (atteindre le niveau professionnel), puis dans des circonstances de sollicitations exceptionnelles où son expertise sera valorisée, puis de plus en plus en routine dans des circonstances qui ne l'exigent pas, bien au-delà de ce qu'attend une posture de sécurité raisonnable. Et plus la société, l'entreprise, ou la tutelle, le « conforteront et le fêteront » en retour pour ce niveau de performance, plus l'opérateur expert ira s'exposer un pont plus loin quand l'occasion le permettra.

La relation entre sécurité et compétences est donc une courbe en U renversé.

Dans ces conditions, on conçoit que l'entraînement à devenir un expert capable d'agir dans des circonstances rares et techniquement difficiles n'est plus automatiquement associé avec un gain de sécurité ; c'est même l'inverse. L'expert ainsi entraîné aura certes une performance meilleure, mais avec une accoutumance au risque que sa cognition va sublimer, et qu'il va utiliser au quotidien même quand ce n'est pas souhaité par l'entreprise.

Les systèmes ultrasûrs l'ont bien compris, faisant volontairement le deuil d'entraînements des opérateurs à des performances exceptionnelles pour ne pas s'exposer à une surconfiance et à des écarts et des prises de risques trop grands dans des situations

habituelles. L'aéronautique a fait par exemple le choix de renoncer à entraîner ses pilotes à des manœuvres inhabituelles, notamment rattraper un avion de ligne avec une inclinaison latérale supérieure à 45°, ou un avion moderne en situation de décrochage, en considérant que l'entraînement à ces manœuvres ne seraient utiles qu'exceptionnellement (moins d'une fois par 10 millions d'heures de vols… Un pilote fait 300 à 500 heures par an) mais auraient pour effet de conforter excessivement les pilotes dans leur confiance à tous les vols, et de voir ces manœuvres difficiles exécutées même quand elles ne sont nécessaires.

En quelque sorte, compte tenu de la compréhension des caractéristiques de la cognition humaine pour gérer les risques, qui s'autoajustent sans limite haute à ce qui est perçu comme maîtrisé, il faut être très clair sur les objectifs et les types d'entraînements proposés aux opérateurs.

- Si l'on veut former des experts capables de performances exceptionnelles (forces spéciales d'intervention, pilotes de chasse, chirurgiens et médecins qui travailleraient dans des services réputés pour leurs innovations majeures), l'entraînement et l'exposition à des situations de plus en plus difficiles sont un bon choix, mais on sacrifiera dans ce cas en partie la dimension sécurité (le compte des évènements indésirables sera plus élevé que pour des opérateurs standard).
- Si l'on veut former des opérateurs spontanément respectueux d'un contrat de performance fixé par l'entreprise, il vaut mieux s'éviter de former les opérateurs à devenir des « sur experts » et savoir gérer des niveaux de risques exceptionnels. Cette logique s'applique à la plupart des environnements professionnels.

La compétence exceptionnelle est associée à une prise de risque augmentée. Une très intéressante étude a été publiée en 2004 sur les profils des victimes d'avalanches survenues de 1972 à 2002 aux États-Unis[69]. Plus de 75 % des avalanches mortelles sont survenues dans des lieux et conditions à très hauts risques, largement prévisibles, connues et annoncées par tous les médias locaux des stations concernées. Près de 70 % des groupes décédés comprenaient un ou plusieurs experts parmi eux : habitués aux conditions hivernales difficiles (24 %), amateurs experts formés à la survie en avalanche (28 %) ou même guides de haute montagne enseignant la survie dans les avalanches (15 %). Cette proportion de (très) grandes compétences dans les groupes de victimes est très supérieure aux standards des groupes qui pratiquaient régulièrement des activités de hors-piste et de haute montagne à la même époque (1972-2002). Les groupes accidentés étaient composés en moyenne de plus de membres (8 à 10) que les groupes exposés qui n'ont pas eu de victimes (2 à 4) ; ils étaient plus souvent dotés d'un leader charismatique reconnu, étaient connus pour avoir plus souvent déjà réussi à traverser ces mêmes difficultés ou des difficultés équivalentes dans le passé, et ils s'étaient retrouvés plus souvent le jour de l'avalanche mortelle

69. McCammmon I (2004) Heuristics traps in recreational avalanche accidents: evidence and implications. Avalanche News: 68.

dans des conditions difficiles de décision réclamant une grande expertise (nuit qui tombe, conditions météorologiques changeantes, fatigue ou épuisement de certains membres questionnant un itinéraire sûr mais beaucoup plus long…). En bref, voici une étude qui démontre parfaitement le mécanisme décrit dans ce paragraphe : les grands experts augmentent leur prise de risque, longtemps valorisée pour la performance exceptionnelle qui en résulte, avant d'être sanctionnée par des accidents dramatiques. En matière d'alpinisme, l'histoire est banale. « Il faut par exemple mettre des chiffres pour donner la mesure de la folie qu'engendre le K2 : entre le 24 juin et le 4 août 1986, 27 alpinistes, tous experts exceptionnels de leur art et pour beaucoup connus mondialement, ont atteint le sommet du K2. 13 personnes sont mortes, dont 10 après avoir réussi le sommet ou s'en être approchées de très près. Dans les cinq années suivantes, cinq autres « summiters » sont morts en montagne. Wanda Rutkiewitz a réussi la première ascension féminine. Elle est morte en 1992 au Katchenjunga. Cinq femmes ont gravi le K2, toutes sont mortes en montagne. Répétition encore. En 1995, six alpinistes dont la Britannique Allison Hargreaves qui venait de réussir la première féminine de l'Everest sans oxygène, ont été cueillis par une violente tempête au-dessus du goulot de la bouteille, descendant du sommet du K2. Tous sont morts. » Charlie Buffet. *Le Monde,* 30 août 2001

Au bilan, la mise en jeu de la compétence individuelle dans la maîtrise du risque s'exprime par quelques paradoxes pratiques, exprimés depuis longtemps par Dietrich Dörner[70].

- Le sentiment de bonne maîtrise de la supervision s'exprime par une performance instantanée souvent imparfaite, mais avec la conscience pour l'opérateur qu'il peut atteindre un objectif ambitieux avec ses savoir-faire personnels ou ceux collectifs sur lesquels il peut compter. L'anticipation « regarde loin », le flux d'erreur est assez important (erreurs de routines surtout), la compréhension de la situation est limitée au strict nécessaire, libérant des ressources pour d'autres tâches et notamment le guidage stratégique vers le but ; le guidage tactique immédiat est confié aux routines couplées à leur environnement. Ainsi la « copie[71] » cognitive (le résultat obtenu à chaque instant dans le travail) est à lire comme un devoir inachevé quand le sujet maîtrise complètement sa situation. Le sujet est conscient qu'il n'a pas (encore) tout fait ce qu'il aurait fallu faire, et qu'il a commis des erreurs çà et là qu'il n'a pas encore récupérées. Cette sphère de conscience de « l'inachevé » ordonne ses priorités cognitives, et explique souvent des déviances de l'instant, qui n'ont pour seuls buts que se donner plus de temps pour récupérer des retards. Cette notion de brouillon inachevé est indispensable à la gestion dynamique de la cognition, et s'avère performante sur le but (malgré toute cette imperfection de chaque instant, le résultat final est le plus souvent correct) ; mais elle crée aussi beaucoup de difficultés dans

70. Dorner D (1997) The logic of failure: recognizing and avoiding error in complex situations. Perseus Books.

71. Le terme « copie » est utilisé ici métaphoriquement pour reprendre l'idée d'une copie d'élève rendue à son maître.

la conception et le couplage aux aides, car ces dernières sont souvent très directives dans la correction immédiate des défauts et perturbent gravement – en voulant bien faire – le réglage de cette gestion dynamique des risques.

- Paradoxalement, quand le doute s'installe chez cet opérateur sur son sentiment de maîtrise (ce qui ne veut pas dire que cet opérateur a déjà perdu le contrôle), il entre dans un sentiment de débordement cognitif qui se traduit par une réduction de ses « déchets de comportement » : il fait « plus attention », commet moins d'erreurs, rejoint le trait nominal de la solution qu'il pensait efficace, anticipe « moins loin », ralentit son activité, réduit son ambition, réduit le parallélisme d'activités (notamment les pensées de la sphère personnelle) et lance une activité intense de recherche de solutions alternatives (en privilégiant des inférences linéaires qui sont souvent inefficaces). À noter, et ce n'est pas le moindre des paradoxes : ce comportement est souvent jugé plus rassurant et plus sûr par des audits externes que le comportement de maîtrise décrit précédemment, dans la mesure où l'opérateur suit mieux les procédures, et colle plus aux consignes. L'opérateur connaît d'ailleurs souvent cette attente, et adopte ce comportement quand il se sait observé ou évalué.
- Quand il a totalement perdu la maîtrise, l'opérateur se replie vers un sous-espace du problème qu'il maîtrise bien et pour lequel il ne fait aucune erreur (recherche de réassurance), mais le reste de la situation et le sort final du problème est abandonné (éventuellement confié par défaut au collectif ou à un automate).

Quelles leçons retenir ?

Le modèle de sécurité écologique, individuel, spontané de gestion des risques qui émerge de ces travaux ne garantit pas une sécurité totale. Il porte en lui les germes de défaillances potentielles très sévères. Mais il permet de comprendre différemment ces défaillances par rapport aux modèles classiques d'erreurs.

L'hypothèse de base repose sur une cognition qui « veut survivre » et qui se donne les moyens de sa sécurité. Mais elle se doit aussi d'être efficace ; une position maximaliste en contrôle complet et permanent de la performance réduirait considérablement le potentiel de performance. Le système cognitif s'est configuré dynamiquement pour répondre à ces deux objectifs contradictoires. Cette configuration repose sur deux piliers : (i) s'adosser aux routines et à leur couplage automatique à l'environnement pour procéder aux corrections tactiques quand la cognition atteint les premières limites de contrôlabilité (encore aisément récupérables, donc avec des marges) ; (ii) s'appuyer sur la métacognition (la vision de ses propres compétences) pour gérer le caractère stratégique et garder le contrat d'objectif dans une zone réalisable (par expérience).

Les défaillances graves peuvent survenir quand ces piliers cognitifs sont parasités, soit que les signaux de l'environnement sont masqués soit que la métacognition indique des capacités erronées de gestion, trop ambitieuses. Ces deux conditions ont été souvent remplies au début de l'automatisation des systèmes : les automatismes masquaient la perte de contrôle cognitive en garantissant une performance maximale même sans

intervention ni compréhension de l'opérateur ; et les connaissances de l'opérateur sur le système devenaient plus hétérogènes du fait de l'accroissement de la complexité globale. Les mécanismes de mémoire et de métaconnaissance finissaient par gommer une partie de cette hétérogénéité et faisaient croire à l'opérateur qu'il en savait plus que la réalité de sa cognition[72].

Eric Hollnagel a repris ces mêmes idées dans son modèle ETTO (*efficiency thoroughness trade-off*)[73] en insistant sur le bénéfice, y compris pour la sécurité, à parier sur le fonctionnement spontané de l'opérateur, efficace, très anticipatif, mais largement basé sur des routines et exposé à des erreurs (récupérées pour la majeure partie), plutôt que de lui demander de travailler constamment à contresens de ses disponibilités naturelles, avec un excès de méticulosité, de procédures, et d'attention portée à très court terme, qui le ralentissent et finalement lui font commettre des erreurs plus graves par négligence du moyen et long terme. Pour Hollnagel, les progrès de la sécurité passent plus par l'étude et l'optimisation de ces capacités naturelles humaines bien montrées dans les situations normales qui permettent d'atteindre un niveau de sécurité remarquable exprimé par un taux très important d'évitements et de récupérations de situations incidentelles (le positif… qu'on ne voit pas…) plutôt que par l'étude des erreurs et des défaillances (le négatif… finalement très petit en volume, et destiné inéluctablement avec les progrès à être de plus en plus marginal, difficile à étudier et sujet à des biais d'analyse).

Quelles conséquences pour une amélioration de la sécurité à cet échelon individuel

- Il faut arrêter les abus de langage sur les définitions de l'erreur ; on mesure (et voit) seulement les incidents et des écarts jugés coupables, et on commet l'abus d'assimiler cette fréquence d'incidents à la fréquence des erreurs. C'est faux. Il y a 100 à 1 000 fois plus d'erreurs que le taux d'incidents vus et recensés dans une usine ou un hôpital… mais la très grande majorité ont été récupérées avant d'induire un incident repérable. Cet abus de langage finit par avoir un contre-effet sur la sécurité : pas réaliste, inaudible pour l'opérateur, et injuste puisqu'il minimise la récupération des (presque) incidents.
- La sécurité ne consiste pas à supprimer les erreurs (un objectif utopiste), mais à réduire le nombre d'incidents et d'accidents ayant un impact sur le processus.
- La sécurité ne consiste pas à escompter une marche idéale imposée sans aucune flexibilité laissée à l'opérateur de part et d'autre du trait recommandé. Créer une situation de travail sûre (i) c'est d'abord concevoir une situation de travail qui maximise la « valeur » cognitive, épargne cognitivement l'opérateur, lui permet de travailler au maximum en utilisant ses qualités naturelles de contrôle du risque,

72. Amalberti R (1998) Automation in Aviation: a human factors perspective. In: Aviation human factors, sous la dir. de JWDH D. Garland. Hillsdale-New Jersey: Lawrence Erlbaum Associates, p. 173-92.

73. Hollnagel E (2009) The ETTO principle. Efficiency-Thoroughness Trade-Off, Ashgate Publishing.

d'anticiper, et lui permet ainsi d'exprimer ses qualités de récupération et d'intelligence dans la durée, entre le début et la fin de sa prise de poste, et (ii) c'est aussi concevoir une situation qui permet une production suffisante et compatible avec les impératifs économiques et sociaux (quel intérêt et même quel gain de risque aurait-on de concevoir une conduite automobile absolument sûre mais qui ne dépasserait jamais les 50 km/h !! ; la perte macroéconomique en productivité serait bien plus grande que le bénéfice local). On doit donc savoir admettre un taux d'erreurs liées à ces échanges de risques en se concentrant dans la démarche de sécurité sur leur récupération.

- La compétence sert la sécurité jusqu'à un certain point (courbe en U renversé). La poursuite de l'entraînement à des niveaux de risques croissants au-delà des risques rencontrés dans les conditions usuelles du travail (qui incluent le répertoire de situations dégradées habituelles) permet de former des « sur-experts », mais expose en retour à une dégradation de la sécurité par prise de risque excessive.
- Dans ce jeu de compromis nécessaires, attention aux éléments qui pourraient déstabiliser gravement le réglage et l'usage des routines des professionnels. Attention particulièrement aux situations d'intérims, d'expositions des opérateurs à des situations inhabituelles pour eux. Ces situations demandent une vigilance particulière dans la conception des postes de travail. On va en reparler dans une vision plus intégrée de l'approche du poste de travail dans le chapitre suivant.

3

Les clés d'une approche systémique réussie de la gestion des risques

Il est admis par tous qu'une approche de sécurité appliquée à nos univers complexes industriels (nucléaire, chimie, construction, métiers plus artisanaux) ou de services (médecine, banque et finance, transports publics et privés), ne doit plus se limiter à des solutions techniques locales ; elle doit être impérativement systémique, globale.

Mais que mettre derrière ces mots ?

Ce chapitre tente de répondre à la question, en faisant varier les angles de vue, en prenant des exemples dans plusieurs domaines d'applications contrastés, en cassant les biais et les préjugés, et en donnant des clés pratiques.

À propos de la sécurité, de la systémique, de sa complexité… et du plan du chapitre

La gestion des risques dans l'entreprise ne concerne pas que l'évitement ou la réduction des accidents (du système ou du travail). Elle concerne tout ce qui peut compromettre sa survie, que la menace soit économique, politique, sociale, ou de perte d'image notamment après les accidents.

Pour comprendre une approche systémique, il faut accepter que la gestion des risques couvre tous les risques qui peuvent « tuer » l'entreprise, qu'ils soient sociaux, techniques, ou financiers.

La réduction des risques d'un système socioprofessionnel est de ce fait un concept complexe, qui accepte beaucoup de définitions suivant le point de vue où on se place : moins d'accidents du travail, moins d'accidents de l'installation, moins de risques sur les conditions sociales et d'exploitation (pas de licenciement, protection des carrières),

moins de risques sur le *business model* (endettements, bénéfices, vulnérabilités économiques).

> La gestion des risques couvre tous les risques qui peuvent « tuer » l'entreprise. La sécurité par l'évitement des accidents n'est qu'un de ces risques ; d'autres risques (économiques, stratégiques) peuvent parfois tuer l'entreprise plus vite, et donc être plus prioritaires en investissement à court terme que l'investissement sur la sécurité.
>
> Dans ce cas, l'art de la gestion des risques consiste à donner les priorités, faire les arbitrages, conduire l'urgence (bien faire ce que l'on a décidé de faire), mais se rappeler aussi que certains domaines sont alors négligés et les traiter d'une façon particulière dans les directions concernées (bien savoir ce que l'on a négligé en développant une conscience chez le management et les opérateurs de ces vulnérabilités temporaires, par exemple en renforçant la détection et la récupération faute de pouvoir investir plus sur la prévention).

Toutes ces dimensions sont légitimes bien qu'elles soient le plus souvent antagonistes les unes des autres : la survie économique du *business model* passe souvent par une exposition accrue au risque d'accident que l'on gère plus ou moins rationnellement et effectivement après coup (Fukushima en est un exemple caricatural).

Ce texte endosse la perspective de la sécurité industrielle et du service (réduction des accidents, sécurité du patient en médecine) en montrant comment la littérature et l'expérience de terrain permettent aujourd'hui de construire une approche systémique gagnante, cohérente, et en contrôle des compromis concédés aux autres dimensions du risque dans l'entreprise.

La clé du succès de l'approche systémique peut se résumer dans trois points clés complémentaires (i) maîtriser les quatre étapes d'arbitrages toujours présentes dans la construction de la sécurité d'un système complexe, (ii) bien faire ce que l'on a décidé de faire, et bien savoir et contrôler ce que l'on a décidé de ne pas faire, (iii) penser futur et non passé.

Ces trois points clés organisent le plan de ce texte.

Le modèle des plaques comme archétype des modèles systémiques… et ses limites actuelles

Quand on parle de modèle systémique de gestion des risques, tout le monde pense au modèle des plaques de James Reason élaboré dans les années 1980[1,2].

Ce modèle à trois temps est simple, il nous dit : (a) qu'on ne peut pas complètement supprimer les erreurs (patentes) des personnes en prise directe avec le travail, (b) qu'il faut des défenses en profondeur pour éviter la propagation de ces erreurs jusqu'à l'accident, et (c) qu'il faut se méfier des erreurs d'organisation et de management (erreurs latentes) qui, sans être la cause immédiate des accidents, fragilisent les personnes et

1. Reason J (1990) Human error. Cambridge University Press.
2. Reason J (1997) Managing the risks of organizational accidents. Aldershot, England: Ashgate.

les défenses en prise directe avec le travail en ne leur donnant pas complètement les moyens d'être efficaces.

Ce modèle est toujours heuristique, et son auteur, un de mes maîtres et amis, mérite vraiment sa notoriété et sa place mondiale au panthéon des contributeurs à la sécurité. Mais il faut aussi convenir que ce modèle est aujourd'hui insuffisant pour établir une approche systémique de sécurité efficace pour les activités professionnelles complexes. Il souffre de quatre défauts majeurs :

- il reflète un modèle d'accident linéaire basé sur la propagation de défaillances des structures et composantes du modèle ; en ce sens, il renvoie à des idées déjà très anciennes et s'inspire du modèle des dominos d'Heinrich (1931)[3] ou de la chaîne d'erreurs, même s'il est plus complexe en introduisant le rôle des organisations et de la conception[4] ;
- le modèle reste profondément cartésien en décomposant l'univers professionnel en parties (structures et composantes, plaques) puis en appelant à chercher les vulnérabilités de chacune des parties ; il explique l'accident par des vulnérabilités locales, et fait chercher « l'erreur ». Certes, le modèle propose une vision du tout en évoquant les interactions et décalages dans l'alignement des plaques et des vulnérabilités (il ne faut pas aligner les défaillances), mais il prend mal en compte les risques d'accidents sans erreurs des parties liés aux mauvais assemblages de parties non défaillantes et aux propriétés et risques émergents du « tout » (typiquement la vision globale du système)[5] ;
- le modèle suggère que l'identification et la suppression complète des causes latentes et de l'exposition au risque constituent la (seule) voie de progression en sécurité. Ce faisant, il nous oriente vers un modèle d'évitement ou de réduction d'exposition au risque pour accroître sa sécurité, de suppression de toutes les vulnérabilités, alors que vivre avec l'exposition volontaire au risque est un élément réaliste (créer volontairement des trous dans les plaques) de la survie de beaucoup d'entreprises. La sécurité doit aujourd'hui accepter cette exposition et non la refuser, car les systèmes sociotechniques meurent souvent d'abord de leurs mauvais choix économiques, organisationnels et politiques. Le modèle de Reason fournit donc des clés d'action précieuses centrées sur un choix simple de sécurité, mais insuffisant dans le vrai monde industriel ;
- enfin, pour reprendre les points précédents, il reste dans la ligne des idées classiques et soutient implicitement l'idée que le mieux (pour l'entreprise) serait d'obtenir toujours plus de sécurité jusqu'à une suppression totale ou quasi totale des accidents et incidents. Cette vision, acceptable et de bon sens pour les systèmes peu sûrs, trouve une limite paradoxale pour les systèmes devenus très sûrs. Plus un système se sécurise, plus il lui sera difficile de survivre à ses derniers accidents, et plus ces derniers accidents seront des accidents de l'exceptionnel largement provoqués par le

3. Heinrich HW (1931) Industrial accident prevention. New York: McGraw-Hill.

4. Cette critique est particulièrement bien débattue dans Hollnagel E, Woods D, Levison N (2006) Resilience engineering: concepts and precepts. Aldershot, England: Ashgate.

5. Cette critique est particulièrement bien débattue dans Dekker S (2004) Ten questions about human error. A New View of Human Factors and System Safety. Aldershot, England: Ashgate.

système lui-même devenu trop sûr, trop rigide, trop procéduralisé, bref ayant perdu sa résilience native. On le voit chaque jour : les industries ultrasûres ont bien plus de difficultés à justifier leur politique sécurité (que chacun reconnaîtra efficace malgré quelques accidents résiduels très rares), que la pêche ou le trafic routier ont de difficultés à gérer la sécurité liée à leur cortège d'accidents quotidiens[6]. Pire, la quête du toujours moins (d'accidents, d'incidents, d'erreurs) inspirée par le nucléaire, l'aviation, et d'une façon générale par les (quelques) industries ultrasûres, finit par faire oublier qu'il existe d'autres authentiques modèles de sécurité (par exemple modèle HR0 ou modèle de résilience) avec leurs propres règles et leurs propres univers de progrès qui sont très bien adaptés aux milliers d'activités professionnelles n'ayant pas les critères d'exigences dictés par nos systèmes ultrasûrs.

Sur ce dernier point, il est important aussi de comprendre nos biais de construction de notre connaissance en matière de sécurité, liés au recrutement des applications professionnelles étudiées pour la construction de ces modèles de sécurité. En 20 ans (1990-2010), j'ai recensé plus de 2 072 articles conceptuels parlant de modèles de sécurité et de leurs caractéristiques, publiés dans huit journaux internationaux spécialisés dans les domaines de la sécurité industrielle, la sécurité du travail et la sécurité des services (notamment sécurité médicale, banque et route)[7]. Plus de deux tiers de ces articles (1 547) portent répétitivement sur la sécurité (du travail ou du processus) dans cinq grands domaines de la grande industrie (nucléaire, aviation, chimie, offshore, construction) ; près d'un quart (483), mais souvent juste pour répéter et valider les modèles de la grande industrie, concernent la médecine, la banque et la sécurité routière (*nda* : les travaux dans ce dernier domaine sont un peu plus originaux). Très peu (42) portent sur des monographies originales de sécurité appliquées à des activités artisanales à bas ou très bas niveaux de sécurité (mines, pêche professionnelle, artisanats divers). En quelque sorte, notre compréhension du risque et nos modèles de sécurité nous sont largement induits par le modèle de la grande industrie, certes responsable des catastrophes médiatiques, mais pas du plus grand nombre de morts, et finalement très homogène dans ses contraintes et préoccupations (niveau de sécurité compris en 10^{-5} et 10^{-7}, exigences réglementaires évoluées, priorité aux facteurs humains et organisationnels…) ; ce modèle de la grande industrie ne représente au final qu'une très faible fraction des activités professionnelles humaines sur la planète. Ce biais de recrutement explique beaucoup de nos erreurs en matière de généralisation des idées sur la sécurité des systèmes complexes, en limitant notre vision à un domaine étroit, presque un cas particulier.

6. Morel G. Amalberti R. Chauvin C (2008) Articulating the differences between safety and resilience: the decision-making of professional sea fishing skippers. Human factors 1: 1-16.

7. Interrogation Google et archives (sommaires de revue) en décembre 2011 circonscrites à huit journaux : Human factors, Safety Science, Ergonomics, Accident analysis and Prevention, Journal of Safety resarch, Journal of Risk research International Journal Quality in Health Care, British Medical Journal Quality and Safety.

Maîtriser la sécurité systémique : quatre étapes clés pour construire la sécurité d'un système complexe

La sécurisation d'un système complexe par une approche systémique nécessite toujours de passer par les quatre mêmes étapes : (a) savoir où sont les risques, prioriser et construire un système ad hoc de défenses, (b) confronter et ajuster ce modèle papier au réel, et notamment aux migrations diverses de pratiques, (c) élever le regard d'analyse et considérer les contraintes macroéconomiques et politiques, (d) une fois toutes les étapes précédentes réalisées, que le système est nettement plus corseté et contraint, il reste à s'interroger sur sa résistance résiduelle aux circonstances exceptionnelles ; la question de la résilience devient alors centrale.

La sécurité finale observée à un temps t_0 dans un système sociotechnique est toujours le résultat d'une construction en quatre étapes. Ces quatre étapes sont successives mais avec des boucles de rétroaction.

- La première étape est toujours l'identification des risques et l'établissement d'un modèle idéal de défense. C'est le domaine classique de la cartographie des risques, des matrices de décision, et plus globalement de la fiabilité des systèmes étendue à la fiabilité humaine. Une fois le risque identifié et priorisé, cette étape conduit à définir des lignes de défenses (barrières) pour réduire l'occurrence des accidents redoutés.
- La seconde étape est la confrontation de ce modèle idéal au réel. Dans de multiples circonstances, les opérateurs ne respectent pas ce modèle sans sanction particulière, en tout cas pendant une longue période ; les déviances sont nombreuses pour de multiples raisons qu'il convient de comprendre. Ces migrations de pratiques finissent tôt ou tard par se traduire par des incidents et des accidents. La sortie de cette phase est donc forcément en boucle sur l'ajustement du modèle idéal, mais la manière dont on interroge et corrige en boucle le modèle idéal est loin d'être univoque. Dans la plupart des cas, on commet l'erreur de considérer que le modèle idéal n'est pas à remettre en cause, et qu'il faut simplement renforcer ses défenses ou l'autorité sur l'opérateur pour qu'il suive les consignes et procédures. L'idée de renforcer « la culture de sécurité » de l'opérateur pour qu'il joue mieux la partition du modèle idéal auquel on croit est une piste souvent adoptée en parallèle d'un durcissement purement procédural et réglementaire du modèle idéal pour contraindre le suivi. Mais on devrait peut-être plus souvent questionner un certain nombre de fondamentaux de ce modèle idéal que penser à le faire coller au réel.
- La troisième étape est systémique. Personne n'imagine sécuriser totalement un système complexe en jouant uniquement sur la mise en place de procédures et de recommandations et en amenant les seuls opérateurs de première ligne à une

stricte obéissance de ces bonnes pratiques et recommandations. Un pas de plus est nécessaire pour consolider ce que l'on peut appeler le « système » et ce pas relève d'une stratégie de « gouvernance sûre » de ce système et d'action sur le middle et le top management : comment imaginer une structure sûre de ce système, les relations entre entités, professions, intérêts particuliers des uns et des autres, directions, divisions, filiales, et sous-traitants, quel niveau d'indépendance ou au contraire de dépendance donner à chaque acteur, quel risque assumer et comment, dans le réglage du compromis économie-profitabilité-sûreté-sécurité.

- La quatrième étape porte sur la résistance finale du modèle obtenu. La sécurité est souvent un problème encore moins maîtrisable quand toutes les étapes précédentes ont été franchies, que le système est devenu sûr ou ultrasûr, que les procédures, consignes de sécurité, et protections sont raisonnablement suivies et adoptées par les opérateurs de base, que la direction s'est impliquée personnellement dans les choix et arbitrages en faveur de la sécurité en acceptant parfois des sacrifices de profit, qu'une culture du signalement est acquise pour tout. En effet, aucun système sûr n'est à l'abri de catastrophes, certes plus rares, mais infiniment plus dommageables sur l'image d'une telle entreprise ou d'une activité devenue sûre, au point de provoquer plus facilement la crise, et dans certains cas la mort de cette entreprise. Le même accident survenu plus tôt dans l'histoire de la même entreprise à un moment où elle était moins sûre n'aurait sans doute pas provoqué les mêmes conséquences. Dans le fond, l'excellence du niveau de sécurité atteint devient le miroir du modèle prédit et recherché ; mais le système va mourir de ce qui n'est pas prédit. L'adaptation aux circonstances exceptionnelles n'est jamais inscrite dans les modèles strictement procéduraux. Le système n'est plus robuste aux aléas rares, il perd sa « résilience ». Cette section explique tout ce que cette dernière étape a de paradoxal. Plus on procéduralise, plus on gagne en conformité et sécurité par rapport à un modèle idéal, et plus malheureusement on « dé-entraîne » les professionnels et les managers. Leur exposition à des situations difficiles se raréfie ; ils perdent l'habitude de prendre des décisions de sacrifices entre dimensions contradictoires (qui caractérisent la survie à court terme dans ces conditions difficiles). En bref, la résilience est une propriété relativement native des systèmes peu sûrs où les opérateurs s'exposent à des situations très variées. Elle diminue quand on sécurise le système avec les trois étapes précédentes, et elle diminue tellement à la fin du processus, qu'il faut la renforcer par des mécanismes spécifiques dans les systèmes devenus ultrasûrs. Malheureusement, cette phase de réinjection de résilience est souvent délicate voire impossible, car elle contrarie les solutions qui ont servi à renforcer le modèle idéal et à obtenir le niveau de sécurité actuel.

Voyons plus en détail le contenu de chacune de ces étapes, ce que l'on peut retenir et leurs défis respectifs.

Étape 1 : évaluer le risque et construire un château de défenses

Il est impossible de se lancer dans une démarche de sécurité sans évaluer le risque et se protéger contre ce qui apparaît être une menace.
Les outils d'évaluation du risque *a priori* (sur la base d'une analyse systématique des vulnérabilités du système considéré) et *a posteriori* (sur la base de l'analyse des accidents et incidents réellement survenus) constituent l'outillage des fiabilistes ; ils sont bien connus et ne seront pas décrits dans cet ouvrage. Nous renvoyons le lecteur à la littérature pléthorique sur le sujet, et nous ne ferons que citer une petite sélection de références, sans doute incomplètes mais suffisantes pour avoir un rappel des principales méthodes[8].

Principales méthodes d'analyse des risques

Analyse *a priori*			
Analyse de processus	**Outil**	**Intérêt**	**Limites**
	Analyse fonctionnelle	Prérequis à d'autres démarches (AMDE/ AMDEC, APR, définition du besoin à satisfaire, analyse de la valeur) pour la mise en œuvre et la réalisation d'une activité nouvelle (prestation, produit) précisant dès la conception les fonctionnalités nécessaires à sa réalisation, les contraintes qui s'y appliquent et les critères de performance	Démarche complexe et consommatrice de temps adaptée à la conception d'une activité nouvelle Oubli d'une fonction

8. Les références sont très nombreuses sur ce thème et plutôt anciennes. On peut retrouver de multiples synthèses sur plusieurs sites notamment (mais sans exclusive)

http://pachome1.pacific.net.sg/~thk/risk.html consulté le 27 décembre 2011

http://www.statcart.com/ consulté le 27 décembre 2011

ou encore le remarquable travail de synthèse appliqué au domaine médical publié dans cinq articles en français par un groupe d'auteurs, notamment :

Roussel P, Moll MC, Guez P (2007) Étape 2 : Identifier les risques *a priori*. Risques & Qualité en milieu de soins IV 4: 239-47.

Roussel P, Moll MC, Guez P (2008) Étape 3: Identifier les risques *a posteriori*. Risques & Qualité en milieu de soins V-1: 46-58.

Analyse *a priori*			
Analyse de processus	**Outil**	**Intérêt**	**Limites**
	Analyse de processus	Prérequis à d'autres démarches (AMDE/ AMDEC, APR, HACCP) pour la description d'une activité qui intègre l'ensemble des contraintes de fonctionnement (flux, ressources…) pour identifier les points critiques et améliorer les étapes de son fonctionnement, en particulier quant aux interfaces entre services	Nécessite une connaissance du besoin à satisfaire au regard des moyens disponibles
Exemple d'utilisation de techniques de type WHAT if	**HAZOP** *Hazard and operability study*	Décomposition du système à construire en parties appelées « nœuds » puis, à l'aide d'un guide de mots clés, travail en brainstorming sur des possibles déviances, estimation des risques potentiels associés pour la sécurité des personnes, des biens et de l'environnement.	Démarche bien adaptée à l'anticipation de nouveaux dispositifs. Très utilisée dans la chimie. La qualité de la description est le reflet de la qualité des participants
Exemple d'utilisation de techniques de type WHAT if	**HACCP** *Hazard analysis control critical point*	Méthode interactive avec des experts, bien codifiée avec 7 étapes, applicable sur l'existant comme sur le prospectif	Fait autorité dans l'alimentaire
	APR *Preliminary-RiskAnalysis*	Identifie les scénarios d'accident en présence de danger, les évalue, les hiérarchise, et déduit la maîtrise des risques avec une relative exhaustivité	Démarche complexe et consommatrice de temps Applications dans des industries ultrasûres ou à très hauts risques (espace)

Analyse *a priori*			
Analyse de processus	**Outil**	**Intérêt**	**Limites**
	AMDEC Analyse des modes de défaillance et de leur criticité *failure mode effect and criticalityanalysis (FMECA)* **MADE** (*failure mode and effect analysis : FMEA)*	Méthode de sûreté de fonctionnement permettant l'analyse méthodique d'un processus critique allant de la description des étapes à risque jusqu'à la mesure de criticité des causes (produit de la fréquence par la gravité) AMDE : approche simplifiée de la méthode AMDEC utilisable en l'absence de données quantifiées	Sélection des processus critiques Démarche longue à aboutir, à réserver à des processus intrinsèquement très à risques
Suivi de Tableaux de bord	Indicateurs sentinelles Tableaux de bord	Mode de suivi possible d'une action de maîtrise des risques Permet donc la détectabilité du risque, l'anticipation et la prise de décision	Lourdeur éventuelle du recueil des données
États des lieux par comparaison à un référentiel	Audit	Vérifie la mise en œuvre et l'efficacité de mesures définies Simple à appréhender **Exemple particulier : le LOSA** *Line-Oriented Safety Audit : méthode recommandée par l'OACI reposant sur des auditeurs placés derrières les pilotes sur jump seat pour coder les erreurs des équipages* *Autres exemples : les audits facteurs humains et organisationnels*	Requiert une programmation et un travail préparatoire (formation auditeurs), et un référentiel professionnel validé Peu adapté à l'analyse organisationnelle La gestion méthodique des suites est essentielle pour tirer un bénéfice de l'observation des dysfonctionnements observés

Analyse *a priori*			
Analyse de processus	**Outil**	**Intérêt**	**Limites**
	Visites de risques, *Walk rounds* CHSCT/ Health And Working Conditions Monitoring Committee	Levier d'engagement possible d'une démarche institutionnelle (assurances par exemple) et de la direction Une version particulièrement connue de ces visites s'applique aux actions partenariales (syndicats – directions) pour améliorer la sécurité des conditions de travail	Requiert un suivi des observations et une organisation précise pour être utile
Techniques informatisées	Go method Markov modeling Dynamic Event logic Analytical methodogy	Toutes ces techniques utilisent la formalisation mathématique et informatique du procédé pour générer automatiquement des graphes de propagation du risque à partir d'un événement	Complexe et réservé à des applications très précises
Analyse *a posteriori*			
Analyse d'accidents (*accident analysis*) ou de presque accidents *(near misses)*	Analyse approfondie *(in-depth analysis)*	Recherche de causes d'accidents Un exemple particulièrement utilisé en médecine : la méthode ALARM (*Association of Litigation and Risk Management*) inspirée du modèle de Reason et orientée vers la recherche d'erreurs latentes	Simple mais laisse une place importante à l'interprétation des analystes
	Arbres des causes *(Tree based techniques : fault tree analysis, event tree analysis, MORT-Management Oversight Risk tree)*	Série de méthodes partant de l'événement et utilisant des liens logiques pour établir les causes ; l'analyse peut aussi partir d'un **événement sentinelle** pour apprécier ses conséquences potentielles	Assez exigeant en temps si l'analyse dépasse le caractère superficiel, nécessite un climat favorable et une autorité suffisante pour trancher dans les conclusions

On débattra uniquement dans cette phase 1 de quelques points porteurs de difficultés propres à cette phase initiale et stratégiques en matière de choix et d'arbitrage.

Quel espace de référence pour caractériser et mesurer du risque ?

L'analyse du risque, sa caractérisation et sa mesure, questionnent dès le départ notre compréhension du périmètre du domaine que l'on considère pertinent pour expliquer le risque. En quelque sorte, notre analyse scientifique du risque, censée nous donner la mesure du risque par des méthodes les plus formalisées possible, dépend dès le départ de valeurs subjectives.

Prenons un exemple simpl(iste) : une banque veut dresser la cartographie de ses risques financiers pour sa direction « produits financiers ». L'analyse classique va porter sur le périmètre des processus mis en jeu par les services de *trading* pour interagir sur les marchés : organisation du service, flux des ordres, règles d'engagement, pertinence des modèles mathématiques de risque utilisés, outils informatiques, délégation d'engagement, supervision et contrôle. Si on se limite à ce domaine, on reste dans une vision relativement étroite et technique typique d'un processus interne à la banque et propre au *trading*. Mais on peut facilement imaginer que le risque réel dépend plus d'équilibres politiques mondiaux que de techniques bancaires de *trading*. Élargir le périmètre de l'analyse du risque technique à l'analyse du risque politique à l'échelle nationale, voire à l'échelle de la planète, change le modèle de processus à considérer pour nourrir la cartographie, modifie les résultats des modèles HAZOP, AMDEC et APR qui caractérisent le risque, et *in fine* change une partie de la mesure considérée comme pertinente pour ce risque.

On comprend qu'un domaine trop étroit de l'analyse puisse résulter assez facilement dans une analyse de risque qui ne couvre qu'une fraction du risque réel, et parfois même une fraction assez marginale.

Un pas plus loin : échanger les analyses de risque

La médecine évalue en permanence les risques et l'efficacité de ses stratégies. Imaginons des stratégies de prise en charge de l'obésité chez les enfants. On analyse le risque et le bénéfice des médicaments donnés et des prises en charge pour cette pathologie. Mais on sait que les habitudes des milieux sociaux défavorisés et la pression industrielle des vendeurs de sodas et de sucreries (qui se cumulent pour favoriser une alimentation déséquilibrée dans les écoles et au domicile) représentent une source potentielle de risques beaucoup plus grands pour l'obésité que la mauvaise prise en charge médicale. Dans ce cas, le périmètre à considérer dans la prévention du risque obésité gagne à considérer un domaine élargi aux risques associés à l'action sociale plutôt qu'aux seuls risques associés au domaine restreint de l'action médicale.

Cet exemple simple rejoint un des cœurs de l'analyse coût-bénéfice et des analyses économiques en matière de sécurité : comment considérer la sécurité dans une logique de meilleure efficience, produire mieux et plus sûr, pour le même coût, voire si possible pour un coût inférieur.

Ce type d'analyse n'est pas nouveau, mais toujours aussi difficile à mettre en jeu car il force précisément à élargir le périmètre de l'analyse des risques bien au-delà du petit

milieu technique qui déclenche l'analyse du risque sur son processus pour évaluer son propre travail.
On entre typiquement dans l'approche systémique.
Par exemple, un article déjà ancien[9] propose un inventaire de 500 activités humaines à risque évaluées en QUALI (années de vies perdues en pratiquant l'activité ou en s'exposant passivement au risque – riverains d'installations industrielles ou autres). Sans vouloir discuter sur le fond la méthode utilisée pour la comparaison, cet article adresse une question fondamentale : chacun pratique son analyse de risque dans son petit domaine (de profit) et donne à suivre des solutions locales de réduction et de contingentement des risques parfois extrêmement complexes et coûteuses. Mais quand « on regarde le paysage vu du ciel » de ces centaines de silos défendus chacun pour leurs risques propres, on peut vraiment s'interroger sur la pertinence d'une approche de risques qui resterait intrasilo.
On devrait, dans l'analyse de risque, pouvoir honnêtement à un moment donné considérer les échanges de risques et le risque comparé avec d'autres silos couvrant le même domaine, avec d'autres solutions alternatives (le cas de l'obésité précédent… ou cas plus difficile et plus tabou encore, celui des risques associés à l'activité commerciale réalisée par télé-présence grâce à des environnements virtuels *versus* le risque consenti à la sécurité du transport aérien pour répondre au même problème avec déplacement physique des opérateurs). On comprend la réticence à ne pas s'engager dans ces logiques, puisque chaque modèle de risques intra-silo correspond à un *business model* peu intéressé à une vision plus globale qui pourrait mettre à mal son activité. L'exemple du risque nucléaire ou de l'exploitation difficile du pétrole en eaux très profondes vis-à-vis des technologies alternatives d'énergie montre combien il faut aller jusqu'à des catastrophes, et encore, pour accepter réellement ce regard global en toute transparence.
Il en va de même en considérant l'horizon temporel et la capacité de récupération et d'atténuation. Les analyses de risque tiennent peu compte des échanges souvent positifs à prendre des risques sur le court terme pour mieux préserver le long terme.
Imaginons une matrice de risque qui considère une intervention dans une usine dans un contexte difficile, avec fuite d'une vanne sous pression. Le risque consenti immédiatement jouera sur le risque à long terme. Et même si l'intervention se solde par un accident du travail sur le court terme, elle peut au total être d'un coût-bénéfice considérable sur le long terme, en évitant une détérioration plus grande de l'installation et sans doute des conséquences plus graves. Faut-il s'interdire de prendre le risque immédiat pour bénéficier de cette sécurité à long terme. Et où est l'horizon temporel critique ?

Dans le fond, on voit clairement que gérer les risques, ce n'est pas toujours les réduire, mais c'est souvent les échanger entre eux et dans le temps.

9. Tengs T, Adams M, Pliskin J, *et al.* (1995) Five-hundred life-saving Interventions and their cost-effectiveness. Risk analysis 15, 3: 369-90

Ces échanges sont à la fois gagnants et perdants selon le périmètre et l'horizon temporel regardé.

Pour la direction sécurité de l'usine, l'accident du travail lors d'une intervention difficile ne respectant pas les codes de sécurité sera presque toujours considéré à charge d'une gestion des risques mal maîtrisée, même s'il préserve le long terme. La seule dérogation relève de l'interprétation émotionnelle, s'il est clairement établi qu'il s'agit d'une action héroïque (en d'autres termes, que le bénéfice est clairement et immédiatement identifiable sur le très court terme, par exemple sauver un employé blessé dans un environnement toxique sans protection et sans respect de consignes de la part du sauveteur).

C'est exactement la même logique qui s'applique à une lymphangite du bras causée par une perfusion de produits traitant le cancer et « passant » ce jour-là à côté de la veine. L'effet immédiat est catastrophique pour le patient, extrême douleur, gros bras, handicap, des semaines entières pour récupérer, mais l'effet à long terme sera absolument mineur. Le bénéfice global de traiter le cancer apparaîtra d'une ampleur très supérieure à cet incident de parcours sans conséquences à distance.

Toute la difficulté est finalement d'avoir un système acceptant la dynamique et l'intelligence de ces échanges. En général, cet élargissement du périmètre est rendu impossible parce que le système est d'abord incarné par des Hommes, des carrières, des postures individuelles à justifier, des jeux d'intérêts financiers et de pouvoirs, et il faut bien reconnaître que le bénéficiaire final de l'échange à long terme des risques est rarement celui qui doit assumer le choix des risques sur le court terme.

La question de choix du périmètre peut être posée sous d'autres formes, en passant par la question du jugement social qui va changer l'analyse de la matrice d'acceptation du risque.

Imaginons un alpiniste amateur effectuant des courses en montagne avec des ascensions risquées et techniquement pointues. Il s'expose à un risque qu'il sait très élevé parce que son analyse coût-bénéfice (plaisir) est positive. Si on élargit cette analyse à son cercle familial, l'évaluation coût-bénéfice par son épouse va forcément être différente, pondérant beaucoup plus le plaisir et majorant beaucoup plus les effets de l'absence et du risque d'accident. Mais si on l'élargit à la société, l'analyse coût-bénéfice donnera une très faible valeur positive (incidence économique positive dans les stations de haute montagne) pour une très forte valeur négative : coût des secours, coût du handicap. Selon le périmètre considéré, l'analyse va donc déboucher sur des résultats différents d'acceptation de la matrice du risque.

Quelle place au signalement volontaire (ou obligatoire) des incidents dans cette première phase ?

Une vaste littérature couvre les difficultés du signalement dans toutes les industries et les services[10,11] ; les constats sont souvent les mêmes : une sous-déclaration massive à la fois (a) par la peur des conséquences (légales mais surtout internes dans l'entreprise, image personnelle et sanctions), (b) par une mauvaise compréhension chronique de ce qui est à déclarer (une représentation de ce qu'attend l'administration ou l'entreprise… et qui filtre nombre de problèmes jugés non pertinents pour ces cibles, hors sujets, pas assez graves, récupérés, trop habituels…) et (c) par l'exploitation inefficace du résultat obtenu.

Des solutions ont été trouvées au problème de la protection des déclarants. Plusieurs cadres législatifs (*no blame, no shame*) protègent les déclarants dans certains pays (États-Unis et Danemark notamment[12,13]) dans plusieurs domaines industriels et de services. Par exemple, le système national de signalement des incidents aériens aux États-Unis (ASRS – *Aviation Safety Reporting system*) protège depuis plus de 25 ans les professionnels de l'aéronautique signalant leurs erreurs, en leur garantissant l'anonymat et l'impossibilité de poursuite juridique[14]. Des systèmes similaires existent maintenant dans le domaine médical.

Mais la plupart des difficultés de prise en compte du signalement volontaire dans une approche de sécurité sont d'une autre nature et restent d'actualité.

Le signalement du risque reste très lié à la notion de culture de sécurité, moins à la notion d'amélioration des résultats en matière de sécurité

Un système doit accepter sa transparence sur l'erreur comme un prérequis à devenir sûr. Reason[15] cite quatre traits essentiels à la construction d'une culture de sécurité efficace, tous plus ou moins liés au signalement des erreurs : la capacité à ne pas punir ceux qui signalent sauf violations volontaires avec graves conséquences (*just culture*), la capacité à partager ces événements rapportés (*informed culture*), la capacité à tirer des leçons de ces signalements (*learning culture*) et la capacité à changer de modèle d'organisation chaque fois que le signalement montre l'inefficacité du modèle actuel

10. Obstacles to participation: the top 9 reasons why workers don't report near misses, 2011 , http://ehstoday.com/safety/news/9-reasons-near-miss-reporting/.
11. Johnson C (2003) Failure in safety-critical systems: a handbook of accident and incident reporting. University of Glasgow Press, Glasgow, Scotland.
12. Danish act on patient safety, http://www.patientsikkerhed.dk/admin/media/pdf/133907d0940e4d5f751852ec8f6b1795.pdf.
13. US patient safety and quality improvement act, 2005, http://www.ahrq.gov/qual/psoact.htm.
14. http://asrs.arc.nasa.gov/overview/immunity.html#, consulté le 26 décembre 2011.
15. Reason J (1997) Managing the risks of organizational accidents. Aldershot, England: Ashgate.

(*flexible culture*). Ces idées sont maintenant bien établies et sont largement reprises par d'autres auteurs[16, 17].

Ceci dit, le signalement et la mesure de la culture de sécurité (souvent largement centrée sur cet aspect signalement) posent un problème de fond sur le lien réel entre ampleur du signalement et bénéfice pour le niveau de sécurité.

Ce lien est évident en aéronautique et dans le nucléaire, mais plus discutable dans les autres industries.

On a en effet un biais de cas particulier induit par le modèle de l'aviation civile et du nucléaire, marqué par la puissance de ses autorités de tutelles mondiales, régionales et nationales (OACI, EASA, National Aviation Authorities, Nuclear Energy Agency, NISA, IAEA…), la réalité d'une surveillance externe totale et permanente (contrôle aérien et boîtes noires). Bref, il s'agit de systèmes relativement singuliers où signaler les incidents ne laisse pas beaucoup de marges aux professionnels puisque de toute façon ils seront vus et lus par les superviseurs si la moindre conséquence s'est produite. En ce sens, le modèle de l'aviation civile ou du nucléaire est effectivement un modèle exemplaire de signalement volontaire. Effectivement la densité de signalement est corrélée à la sécurité des compagnies en aviation civile, parce qu'elle traduit un fonctionnement absolument incontournable dans ce milieu.

Mais combien d'autres modèles industriels sont proches de ce modèle ? Presque aucun… La supervision est bien moindre, l'autonomie des acteurs bien plus grande ; il n'est pas étonnant que les études transversales sur les modèles de culture de sécurité dont les traits principaux nous viennent de l'aviation, du nucléaire et de la chimie, n'aient pas toujours de résultats aussi probants dans les autres industries, particulièrement la médecine.

Signalement et culture de sécurité : quel lien entre culture de signalement et performance de sécurité dans l'industrie ?[18, 19, 20]

On retrouve au niveau organisationnel neuf dimensions testées répétitivement dans les questionnaires de culture de sécurité : la politique de gestion des risques et du signalement des incidents vient en premier, suivie de la qualité de la plateforme technique, la qualité de la maintenance, les procédures, la qualité et la quantité de personnel et du planning, les compétences, l'engagement collectif, la communication et le suivi des changements. Les exploitations de questionnaires montrent une certaine agrégation et superposition de valeurs parmi ces neuf dimensions, avec le management largement prédictif de toutes les autres valeurs.

16. Marx D (2001) Patient Safety and the "Just Culture": a primer for health care executives. New York, NY: Columbia University.

17. Dekker S (2007) Just culture, balancing safety and accountability. Aldershot, UK: Ashgate.

18. Guldenmund F (2007) The use of questionnaires in safety culture research – an evaluation. Safety Science 45: 723-43.

19. Guldenmund F (2000) The nature of safety culture: a review of theory and research. Safety Science 34 (1-3): 215-57.

20. Flin R (2007) Measuring safety culture in healthcare: a case for accurate diagnosis. Safety Science 45: 653-67.

Au bilan, un certain nombre de questions restent en suspens, notamment le lien formel entre mesure d'un type d'organisation particulier et risque d'accident. On mesure des valeurs qui ont probablement du sens pour la sécurité, comme le signalement d'incident, largement relayées par l'organisation au plus haut niveau, et donc avec des dimensions finalement peu indépendantes entre niveaux macro, méso et micro. On peut se demander si, compte tenu des limites des questionnaires, des techniques d'audit ne seraient pas plus appropriées.

La volonté de lien signalement est encore plus aléatoire en médecine que pour le reste de l'industrie[21]

L'ensemble de la littérature indique que les systèmes utilisant les déclarations des professionnels de santé font l'objet d'une sous-déclaration massive. Le fait n'est pas nouveau. En 1995, une étude menée sur 6 mois dans un hôpital d'Harvard montrait que le taux de déclarations représentait à peine 6 % du taux réel des EIG (Événements Indésirables Graves) estimés par analyse rétrospective des dossiers (Cullen, 1995). En 1998, des résultats proches étaient retrouvés à l'hôpital Brigham & Women Hospital de Boston : un système de détection automatique d'EIG à partir des dossiers patients électroniques avait détecté 2 620 alertes (Jha, 1998) ; après vérification, 365 EIG ont été identifiés. Une analyse rétrospective des dossiers (réalisée indépendamment du processus précédent) a permis d'identifier 385 EIG alors que, pendant la même période, les professionnels de santé avaient déclaré 23 EIG. Sur les 617 EIG distincts détectés par au moins l'une des trois méthodes, 65 % étaient identifiés par l'analyse rétrospective, 45 % par le dossier électronique et seulement 4 % par les déclarations dans le système de signalement officiel. La littérature retrouve des chiffres constamment similaires (entre 3,5 et 10 %), ce qui atteste du très faible rendement de ces systèmes de signalement spontanés. Un autre résultat récurrent (Lawton, 2002 ; Ricci, 2004) est la sur-représentation massive des déclarations des infirmières (70 à 80 % des bases de données) par rapport à celles des médecins. Parmi ces derniers, les médecins seniors sont quasiment absents des bases de déclarants (Vincent, 1999). Les résultats plus récents (Evans, 2006) confirment ces difficultés.

21. Lawton R, Parker D (2002) Barriers to incident reporting in a healthcare system. Qual Saf Health Care 11: 15-8.

Cullen D, Bates D, Small S, *et al.* (1995) The incident reporting system does not detect adverse drug events: a problem for quality improvement. Jt Comm J Qual Improv 1: 541-8.

Jha A, Hupeerman G, Teich J, *et al.* (1998) Identifying adverse drug events. JAMIA 5: 305-14.

Goldman RM, de Leval AP, Cohen MR, *et al.* (2004) Pitfalls of adverse event reporting in paediatric cardiac intensive care. Archives of Disease in Childhood 89: 856-85.

Vincent C, Stanhope N, Crowley-Murphy M (1999) Reasons for not reporting adverse incidents: an empirical study. J Eval Clin Pract 5: 13.

Evans SM, Berry JG, Smith BJ, *et al.* (2006) Attitudes and barriers to incident reporting: a collaborative hospital study. 15: 39-43.

Paradoxalement, la condition « no blame no shame » et les questions sur le signalement volontaire pourraient devenir moins pertinentes à l'établissement d'une cartographie des risques dans le futur

Comme on vient de le voir, la question du manque de protection des déclarants vis-à-vis de la justice, de leur hiérarchie et de leurs tutelles a été un point qui a longtemps obsédé la littérature[22]. C'était à l'époque où la déclaration des acteurs représentait quasiment la seule source d'information.
Demain devrait être différent ; l'apport des signalements d'incidents par les acteurs de terrain va devenir marginal, en rapport des autres moyens de récupérer l'existence de déviations et d'incidents. L'informatique et la supervision constante des systèmes (boîtes noires) ont commencé à faire basculer le signalement vers des procédures automatisées. Dans ce cas, la difficulté de départ consiste à « extraire la défaillance automatiquement d'un flux de données ». Mais la vraie difficulté à l'arrivée sera de savoir quoi faire du nombre sans doute impressionnant de déviations relevées par le système traceur automatisé (sans aucune mesure avec le nombre déclaré aujourd'hui volontairement par les acteurs).

L'automatisation dans la détection des incidents. Une étude de 2010[23] compare les résultats obtenus par trois méthodes de recueil d'événements indésirables graves (EIG) utilisées en médecine aux États-Unis : (1) un système de signalement national volontaire des professionnels médicaux (système de l'AHRQ *Agency for Healthcare Research and Quality*) ; (2) un système reposant sur les déclarations obligatoires des professionnels de tous les incidents relatifs à une liste de 20 indicateurs nationaux de sécurité du patient (*Patient Safety indicators, PSI*) ; et (3) une méthode automatisée d'analyse du contenu de tous les dossiers médicaux électroniques des patients hospitalisés (méthode des *trigger tools*). Les trois méthodes ont été appliquées à la même cohorte de 795 patients provenant de trois hôpitaux généraux en 2004 ; la méthode automatisée de suivi des dossiers a révélé 10 fois plus d'EIG que les deux autres méthodes. 393 EIG ont été détectés au total, dont 355 uniquement par la méthode automatisée.

L'aéronautique a tracé le chemin par ses dispositions réglementaires d'analyse systématique des enregistreurs de bord (la cassette de chaque vol est lue et toute valeur aberrante au-delà d'une enveloppe de normalité est l'objet d'un complément d'analyse manuel[24]). C'est quasiment le même esprit qui a inspiré l'analyse des dossiers médicaux

22. Un bon résumé du débat dans Dekker S (2007) Just culture, balancing safety and accountability. Aldershot, UK: Ashgate.

23. Classen D, Resar R, Griffin F, *et al.* (2011) Global trigger tool shows that adverse events in hospitals may be in times greater than previously measured. Health affairs 30: 581-9.

24. http://www.iata.org/ps/intelligence_statistics/pages/fda.aspx.

par la méthode des *trigger tools*[25,26] : recherche automatisée de valeurs aberrantes qui donnent lieu à une analyse de compréhension manuelle dans un second temps.

La plus-value des méthodes lourdes de cartographie est évidente pour la grande industrie mais toute relative dans les industries innovantes

La plus-value des méthodes lourdes de cartographie des risques (par rapport à des méthodes simples du type réunions entre experts) est réelle, mais finalement assez fragile en regard du temps à consacrer à ces formalismes, particulièrement dans les systèmes industriels très innovants.

Pour ancrer les esprits, un simple partage d'expérience de quelques journées d'un panel de professionnels bien choisis, bien guidés, et réellement actifs d'un domaine (brainstorming guidé) ramène autour de 50 à 60 % du risque total d'un domaine ; une analyse de retour d'expérience (signalements d'incidents) non approfondie restant au niveau de la surface des anecdotes et des causes immédiates ne ramène quasiment rien de plus (les histoires déclarées sont souvent des tautologies, confirmant des risques déjà connus). En revanche, une analyse approfondie de ces mêmes incidents ramène 10 % de plus (soit 60 à 70 % du réel du risque quand elle s'ajoute au brainstorming de départ) en pointant les vulnérabilités systémiques (facteurs latents), mais il faut y consacrer quelques journées de plus et mobiliser à nouveau les experts. Enfin les méthodes formelles (analyse de processus, analyse fonctionnelle, AMDEC, APR…) ajoutent 15 à 25 % de connaissances nouvelles sur le risque, mais au prix d'un investissement lourd (plutôt chiffré en semaines et mois). Quand toutes ces étapes ont été conduites parfaitement, ce qui est rare et réservé à quelques industries ultrasûres compte tenu du temps et des ressources à allouer, la cartographie ainsi obtenue par la combinaison des méthodes peut couvrir jusqu'à 90 à 95 % du risque réel. Ce très beau résultat sur le papier est à pondérer par l'obsolescence naturelle du tableau ainsi dressé, qui perd entre 2 % (nucléaire) et 20 % (médecine ou industries des logiciels) de sa pertinence chaque année selon le rythme d'innovation et les restructurations du marché économique du système considéré ; compte tenu du coût de la cartographie formelle, il est bien rare qu'elle soit réactualisée au même rythme…

25. Resar R, Rozich J, Classen D (2003) Methodology and rationale for the measurement of harm with trigger tools. Qual Saf Health Care 12: 39-45.

26. Rozich JD, Haraden CR, Resar RK (2003) Adverse drug event trigger tool: a practical methodology for measuring medication related harm. Qual Saf Health Care 12: 194-200.

Maîtriser la sécurité dans un contexte de forte innovation : le cas de la médecine avec un *turnover* des connaissances de 5,5 ans.

Sjohania et ses collègues[27] ont analysé 100 revues de questions publiées entre 1995 à 2005 sur les stratégies thérapeutiques recommandées pour plusieurs domaines médicaux et se limitant aux meilleurs essais contrôlés, randomisés ou semi-randomisés. Ils ont utilisé deux critères de jugement : quantitatif avec la survenue ou non d'un changement sur le résultat clinique de plus de 50 % sur au moins un critère par rapport à la revue initiale, et qualitatif par une reconsidération de l'efficacité, de l'identification de nouvelles complications ou de nouveaux trous de connaissances inconnus dans la revue de départ. Ils retrouvent un des deux signaux dans 57 % des revues publiées. La durée moyenne de la demi-vie de connaissance avant apparition d'un signal d'obsolescence est de 5,5 ans. Dans 7 % des cas, la revue avait déjà un signal d'obsolescence au moment de sa publication, et 11 % des revues en avaient un en moins de 2 ans. La médecine est une des rares activités humaines professionnelles ayant un tel taux d'innovation (il n'y a guère que l'industrie des logiciels qui la dépasse). Ce rythme effréné d'innovation contraste avec le modèle de qualité que la médecine a choisi d'importer sur étagère des systèmes ultrasûrs (et en particulier de l'aviation), avec un temps de déploiement total de la méthode sur un objet innovant qui atteint 10 ans en moyenne : 2 ans pour voir le problème, 2 ans pour voir apparaître des solutions locales, 1 an pour s'en saisir en central au niveau de la tutelle, 2 ans pour sortir une solution consensuelle (une recommandation nationale) et 2 à 3 ans pour former tous les opérateurs de la nation à cette solution. Autant dire qu'en médecine, le cycle de qualité n'est jamais achevé, au profit de l'innovation. On conçoit qu'il faut faire quelque chose de particulier et ne pas utiliser les méthodes connues par l'industrie, car l'innovation est aussi, et même beaucoup plus que la qualité, un vecteur de progrès en sécurité que personne ne veut arrêter – par exemple la bascule en chirurgie ambulatoire (*day surgery*) en utilisant des techniques de chirurgie minimale par les voies naturelles effondre les taux d'infections nosocomiales (plus d'effraction de paroi, une promiscuité réduite au minimum) alors que la lutte proposée par les approches qualité a eu du mal à simplement maintenir ce taux (très haut) depuis des dizaines d'années. Autant dire qu'aucun professionnel de santé ne choisira de refuser cette innovation pour continuer à parier sur l'effet qualité, même si son introduction amène d'autres problèmes. Que vaudront les cartographies construites il y a 5 ans sur les risques comme celui de la chirurgie classique quand dans les 5 ans suivants, on sait que l'on va basculer massivement sur une autre chirurgie dans tous les pays occidentaux ?

27. Sjohania K, Sampson M, Ansari M, *et al.* (2007) How quickly do systematic reviews go out of date? A survival analysis. Ann Int Med 147: 224-33.

La construction des défenses après l'obtention des résultats de la cartographie reste un nœud stratégique pas facile à résoudre

Le dernier point (quelle stratégie de sécurité adopter en fonction de ce que l'on sait de la cartographie des risques) est évidemment encore plus stratégique puisqu'il touche au plan d'action. C'est le point final de cette phase initiale : on sélectionne les risques que l'on a décidé de protéger, puis on construit des barrières (des mécanismes de défenses) contre ces risques. Rappelons que les barrières disponibles sont de trois types complémentaires[28] (barrières de prévention, de récupération et d'atténuation), chacune de ces barrières faisant appel à une combinaison d'outils immatériels (formation, lois, recommandations) et d'outils matériels (détrompeurs, fermetures, accès impossible…). Arrêtons-nous quelques instants sur ces points.

Sélectionner les risques dont on se protégera : les matrices de décision en question

La cartographie fournit une liste de risques, mais pas de priorités d'attaque ; il faut donc une stratégie de décision qui accepte certains risques et se protège contre d'autres.

En matière de risques d'accidents, la solution est généralement apportée par l'utilisation d'une matrice de décision fréquence*conséquence[29]. On range les relevés de la cartographie dans des cases sur l'axe de fréquence (de très fréquent à exceptionnel) et sur l'axe des conséquences (de mineur à catastrophique). Le processus de décision consiste à accepter certains risques (très fréquents mais sans conséquences, ou tout à fait exceptionnels même si les conséquences sont catastrophiques), et à se protéger contre tous les autres risques. On peut se protéger soit en revoyant la conception ou les conditions d'emploi autorisées (prévention), soit en augmentant les capacités de récupération et d'atténuation (par la formation notamment).

Cette logique conduit à deux risques : effectivement bien se protéger contre les risques que l'on a identifiés comme prioritaires, et bien savoir ce sur quoi on a décidé de faire l'impasse. Ce dernier domaine est évidemment le plus difficile et renvoie au problème du traitement de la gestion des signaux faibles.

Les signaux faibles, un concept séduisant, et pourtant souvent illusoire dans sa gestion

La rationalité décrite précédemment conduit à se défendre contre toutes les parties de la matrice des risques jugées acceptables pour le système.

28. Hollnagel E (2004) Barriers and accident prevention. Aldershot, UK: Ashgate.

29. Dans le domaine de la qualité sur la ligne de la production, on utilise plutôt des méthodes de décision privilégiant uniquement la fréquence (la méthode de Pareto est la plus connue).

Le point faible de cette rationalité réside dans les risques exclus, particulièrement les signaux faibles dont la littérature et les congrès se font souvent l'écho en demandant une meilleure écoute et une meilleure prise en compte[30,31,32].

Or analyser les signaux faibles reviendrait précisément à analyser des parties de la matrice actuelle qu'on a décidé de ne pas analyser. Ce qui paraît simple dit ainsi est en fait très compliqué pour plusieurs raisons :

- la question du choix d'inclusion. Contrairement à la partie de la matrice que l'on traite et qui correspond à un nombre fini d'éléments, la partie non traitée, ou délaissée, est composée d'un nombre infini d'éléments (le complément de ce que l'on traite avec l'infinie diversité du monde). Il apparaît évident que toutes nos ressources ne suffiraient pas à traiter un ensemble infini de risques potentiels ; il faut donc faire des choix d'inclusions… mais comment ? Dans ce contexte, le problème du choix de ce que l'on inclut renvoie au modèle d'accident que l'on développe pour traiter ces événements. Ce choix se décline lui-même en deux autres questions ;
- la question du modèle d'accident choisi. On ne peut pas traiter les signaux faibles avec des modèles classiques d'accident, puisque ces signaux (faibles) sont justement écartés (avec rationalité) faute de gravité ou de fréquence suffisante. Il faudrait utiliser des modèles de percolation ou d'association de conjonctures où des signaux et événements mineurs se retrouvent associés dans un même contexte ; la réunion de ces signaux crée l'événement à risque. Inutile de dire que le maniement et la complexité de ces modèles de percolation n'ont rien à voir avec les modèles simples ; ils demandent du temps, des ressources (le traitement des signaux faibles aujourd'hui rejetés entraîne un surcroît considérable de travail), et surtout une grande compétence sur le fond (les personnes qualifiées sont plutôt des universitaires, exceptionnellement employés dans les entreprises) ;
- du coup le troisième facteur limitant est le coût macroéconomique d'une extension de la veille sur les signaux faibles. On peut à travers plusieurs essais çà et là estimer le surcoût à 5 à 10 fois le coût actuel de la sécurité[33]. Car le surcoût est double : il est bien sûr dans l'inclusion dans l'analyse de ces signaux, mais encore plus dans les coûts indirects induits par les stratégies de protection qui seraient développées contre ces risques faibles (qui gèleraient un certain nombre d'initiatives industrielles et de prises de risques innovantes)[34].

30. Gerstein M, Ellsberg M, Ellsberg D (2008) Flirting with disaster: why accidents are rarely accidental. Sterling Publishing.

31. Ostberg G (2009) Some intangibles in human handling of risks, Lund University, Sweden RISC-Research Paper No. 3, http://www.wisdom.at/Publikation/pdf/RiskBerichte/RRR_GOestberg_SomeIntangibles_09.pdf.

32. Chateauraynaud F, Torny D (1999) Les sombres précurseurs : une sociologie pragmatique de l'alerte et du risque. Paris, EHESS.

33. Amalberti R (2006) Optimum system safety and optimum system resilience: agonist or antagonists concepts? In: Resilience engineering: concepts and precepts, sous la dir. de E. Hollnagel, D. Woods, N. Levison. Aldershot, England: Ashgate, p. 238-56.

34. Woods DD (2005) Creating foresight: lessons for resilience from Columbia. In: Organization at the Limit: NASA and the Columbia Disaster, sous la dir. de W.H. Starbuck and M. Farjoun, Blackwell, p. 289-308.

Au total, si le concept de signaux faibles est particulièrement séduisant, on peut aisément en déduire qu'il est assez irréaliste en matière de gestion cartésienne des risques au quotidien.

Dans le fond, la meilleure utilité des signaux faibles est d'exister socialement à travers les *whistle blowers*. Cette existence d'un contre-pouvoir et d'un activisme interrogateur sur des risques refoulés ou négligés, même si l'analyse de fond cartésienne portée sur ces dires n'est pas conduite à fond, maintient au moins le sentiment dans la société et chez les managers du risque qu'on ne contrôle pas tout, loin de là, dans les modèles de risques et d'accidents déduits par la rationalité.

Étape 2 : comparer le modèle de papier à la réalité du terrain

Une fois le modèle de défense théorique construit à partir de la cartographie, il faut le faire vivre et durer dans le temps ; la réalité questionne la théorie et fait remonter des écarts qu'il faut comprendre, et en retour combattre (ou accepter en faisant évoluer le modèle) pour que le modèle garde sa pertinence.

Le problème le plus difficile à traiter est celui de la migration progressive du système et de l'augmentation mécanique des violations avec l'amélioration de la sécurité[35].

La migration des pratiques est la norme de tous les systèmes[36]. Les conditions techniques et économiques introduisent régulièrement des contraintes nouvelles au travail : il faut faire souvent plus (de performances) avec moins (de personnels, de matériels). Ces conditions dégradées, d'abord réservées à des cas ponctuels ou des périodes commerciales critiques, ne sont pas sanctionnées immédiatement de mauvais résultats ou d'incidents (en général, c'est même tout le contraire avec un bilan plutôt positif d'augmentation de la performance) ; les migrations deviennent de ce fait un standard accepté par tous. Ce standard « illégal-normal » s'accompagne d'un retour de bénéfices (pour les travailleurs) censé répondre et compenser l'effort consenti à produire : la hiérarchie leur accorde souvent plus d'autonomie (on conteste moins certaines initiatives, on laisse les plannings et les remplacements s'auto-organiser, bref on tolère plus, on donne des primes pour pénibilité aggravée, et on oublie progressivement ces écarts dans le retour d'expérience). On serait d'ailleurs bien en difficulté si l'on récupérait du signalement sur ces migrations puisqu'elles rendent service à l'entreprise (performance) et aux travailleurs (bénéfices secondaires). La part de l'entreprise fonctionnant dans un domaine « illégal-normal » peut facilement atteindre 40 à 50 % des procédures existantes dans les systèmes sous pression économique.

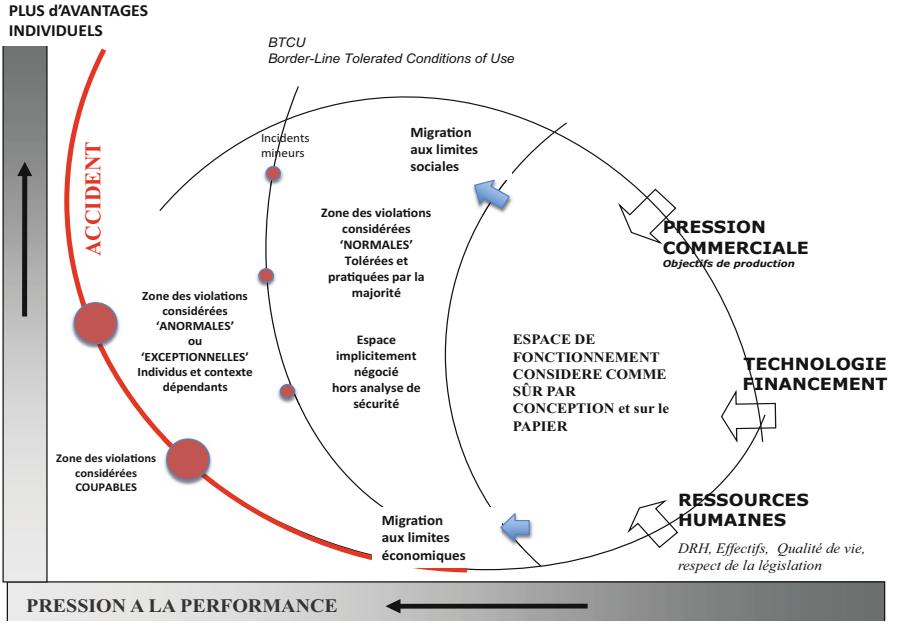
35. Aslanides M, Valot C., Nyssen AS, Amalberti R (2007) Evolution of error and violation description in french air force accident reports: impacts of human factors education. Human Factors and Aerospace safety 6: 51-70.

36. Amalberti R, Vincent C, Auroy Y, de Saint Maurice G (2006) Framework models of migrations and violations: a consumer guide. Quality and Safety in Healthcare 15 (suppl 1): i66-71.

Cette part cachée, non conforme au modèle prescrit, est d'autant plus grande que la marge calculée pour construire les barrières de sécurité a été importante sur le papier : la violation ou la déviance ne se définissent en effet que par rapport à une exigence réglementaire (qu'elle soit interne à l'entreprise ou externe). Si l'exigence réglementaire est contradictoire avec une demande en performance qui s'accroît, alors le nombre de violations augmente mécaniquement et le système se met en migration.

> Deux points paradoxaux à retenir sur les violations :
> (a) la violation est une caractéristique des systèmes sûrs (qui ont des procédures) ; elle n'existe pas dans les activités sans cadre législatif ni règles ;
> (b) la procédure mal conçue, trop exigeante, produit mécaniquement la violation.

Un modèle de migration typique des pratiques (Amalberti *et al.*, 2001, 2006, inspiré de Rasmussen, 1997) : les pratiques professionnelles sont réglées et limitées dès leur conception par une combinaison de règles et de barrières formelles et informelles pour éviter que la pression à la production n'entraîne une migration rapide vers une zone à risque. Mais cette pression à la production est si forte que le système va migrer, et ce d'autant plus que le système aura été enfermé dans un usage très (trop) prudent à sa conception. Les pratiques vont migrer à la fois vers plus de productivité et plus d'avantages pour les opérateurs. Ces violations « normales », tolérées par tous, peuvent concerner jusqu'à 50 % des procédures, et vont ponctuellement continuer à s'amplifier et à créer de vrais risques. C'est ce risque de migrations secondaires qui est la cible prioritaire de l'intervention de sécurité.



Comment contrôler les migrations ? Trois solutions s'offrent aux spécialistes :

- la première est une fausse bonne idée et porte sur la formation : elle consisterait à devancer la migration en augmentant sans limite les compétences des professionnels, de sorte qu'ils puissent maîtriser des pics de demande de production exceptionnelle mais qu'ils reviennent par contre au mode de conformité dès que ces pics sont passés. On l'a vu dans le chapitre précédent, cette solution est contrafactuelle : plus on forme techniquement les opérateurs à devenir encore plus experts, plus ils intègrent leurs succès passés, prennent confiance, et vont continuer à migrer « un pont plus loin » en conditions standard ;
- la seconde est typiquement systémique et porte sur la conception. On vient de voir qu'il existe d'autant plus de violations que le modèle de sécurité imaginé à la conception sur le papier est idéal, irréaliste, ne prenant pas en compte la contrainte économique de production. Retenons à ce stade qu'il vaut mieux un modèle de sécurité conçu comme moins ambitieux et compatible avec la performance demandée, que l'inverse. Retenons aussi deux autres points : aucun modèle de sécurité ne peut absorber dès sa conception toutes les transformations à venir des conjonctures économiques. Il est donc normal qu'un modèle de pratiques migre pour s'adapter à ces nouvelles conjonctures, et il est aussi normal en conséquence d'avoir à adapter régulièrement le modèle de sécurité, parfois en relâchant les contraintes et non pas nécessairement en les renforçant systématiquement. Pire, toute violation et toute migration étant d'abord le signe d'une dissociation entre les exigences du modèle de sécurité et le modèle de performance, on ne devrait jamais répondre à un début de migration par un renforcement de la procédure ou de la contrainte, puisqu'une telle réponse va augmenter le différentiel prescrit-réel et augmenter mécaniquement le nombre de violations ;
- la troisième est typiquement sociodynamique et porte sur la surveillance des individus particulièrement déviants : la migration des pratiques dans l'illégal-normal ouvre des brèches dans la tolérance sociale au non-respect de la procédure[37]. Si rien n'est fait, certains individus, plus prônes que d'autres à prendre leur autonomie, étendent rapidement ces autorisations locales à toutes leurs pratiques. On ne contrôle jamais ces individus par injonction de la hiérarchie, du moins tant qu'ils n'ont pas eu d'accidents ; pire, ce sont souvent des personnes brillantes, dont les succès accumulés et les performances réalisées sont souvent cités en exemple et confortent leur statut envié dans le groupe. Le seul moyen de contenir ces individus est de les remettre dans « l'autorité du groupe », une vieille solution historique inspirée de la protection fonctionnelle procurée par les groupes et les familles aux individus les plus fragiles, et qu'on retrouve souvent d'actualité dans l'ethno-psychiatrie moderne. L'installation d'une surveillance réciproque et consentie entre les membres du groupe, avec la complicité et la supervision des cadres de proximité, a largement démontré son efficacité pour réduire les déviances individuelles extrêmes (mais évidemment pas celles faisant consensus par tout le groupe). Ces techniques sont notamment à la base du succès des « vendeurs de conformité réglementaires

37. De Saint Maurice G, Auroy Y, Vincent C, Amalberti R (2010) The natural life span of a safety policy: violations and migration in anaesthesia, Qual Saf Health Care 19: 327-31.

pour la sécurité du travail » prônant les techniques de BBS (*Behavior-Based Safety*) par exemple la méthode de DuPont. Ces méthodes sont typiquement appliquées à la réduction des déviances dans le port des équipements de sécurité dans les industries[38]. Il reste que mettre en route ces techniques nécessite une formidable dynamique d'équipe (se signaler mutuellement toutes les déviances, avec une façon polie de le faire, du temps consacré à comprendre pourquoi…) ; autant dire plus de temps et plus d'implication personnelle, et un renoncement au culte du succès et du héros… Sans surprise, ces techniques sont rarement mises en place, hors le cas limité du port d'équipements de sécurité dans des usines, et quand elles le sont, elles apparaissent bien difficiles à maintenir dans la durée.

Étape 3 : agrandir l'angle d'approche, aborder la sécurité par les macro-organisations

Sécuriser l'environnement immédiat de l'opérateur ne saurait être suffisant pour sécuriser un système entier. Les deux premières étapes se sont presque exclusivement portées sur les niveaux micro (poste de travail et environnement de proximité) et méso (entreprise de proximité).
Un système est bien plus que cela.
Les conditions de l'économie générale des métiers, professions, et des régulateurs jouent un rôle majeur dans les possibilités de sécurisation du système[39].

Une différence de sécurité de facteur 100 à 1 000 entre les systèmes les plus sûrs et les moins sûrs

La différence des niveaux de sécurité dans l'industrie atteint un facteur 100 en sécurité du travail et un facteur 1 000 en sécurité du processus et des installations. Par exemple, en sécurité du travail, 1 pêcheur professionnel sur 1 000 meurt chaque année à son travail, comparé à des chiffres de 1,5 décès/an sur 10 000 pour les ouvriers du secteur de la construction, et de moins de 5 décès/an sur 100 000 dans tous les autres secteurs[40]. En sécurité des installations et du processus industriel les chiffres sont encore plus édifiants avec 1 patient sur 1 000 qui décède d'une surprise associée à un événement indésirable dans sa prise en charge à l'hôpital, comparé au risque d'1 décès prématuré (lié à l'exposition au risque) par million de résidents vivant 5 ans au voisinage immédiat

38. Cooper D (2009) Behavioral safety interventions. Professional Safety: 37.
http://www.behavioural-safety.com/articles/behavioral_safety_interventions_a_review_of_process_design_factors.pdf

39. Amalberti R, Auroy Y, Berwick D, Barach P (2005) Five system barriers to achieving ultrasafe health care. Ann Intern Med 142, 9: 756-64.

40. Morel G, Chauvin C (2007) A socio-technical approach of risk management applied to collisions involving fishing vessels. Safety science 44: 599-619.

d'une centrale nucléaire[41] ou de 1 décès prématuré par million de passagers prenant l'avion de ligne.

De telles différences conduisent à être modestes dans les capacités de changement relatif de position de niveau de sécurité de chaque grande catégorie d'activités humaines les unes par rapport aux autres. Pour qu'un changement soit visible sur une telle échelle, il faudrait par exemple que la médecine améliore sa sécurité au moins d'un facteur 10 (un vrai défi sachant qu'elle n'a pratiquement pas progressé en 10 ans), et même un tel changement serait encore négligeable pour se comparer à des systèmes comme l'aviation civile qui restent 1 000 fois plus sûrs.

Le rôle prépondérant des enjeux macro par rapport aux actions locales de sécurité

Les facteurs systémiques et la gouvernance centrale de l'entreprise imposent souvent une forte limitation aux initiatives de sécurité pouvant être conduites au niveau local[42].

Il peut s'agir *a minima* d'une volonté de coordonner toutes les politiques en central en freinant les initiatives locales isolées ; mais plus souvent encore, il s'agit pour la direction de préserver des enjeux contradictoires entre besoin de sécurité réel, maintien des autorisations par une réponse conforme aux attentes administratives des tutelles, tout en protégeant une volonté d'exposition à des prises de risques pour maximiser l'image, la production, le modèle économique ou la réussite personnelle des managers.

Les spécialistes de sécurité doivent apprendre à faire avec ce cadre paradoxal, et bien comprendre les mécanismes d'arbitrages utilisés par leur industrie.

Par exemple, le nucléaire a une tolérance sociale très faible à l'exposition volontaire au risque, tout comme l'aéronautique civile, et arbitre donc facilement en faveur d'initiatives de sécurité, tout en réclamant une complète cohérence centralisée (les actions locales isolées sont combattues). Mais ce n'est pas le cas (en tout cas jusqu'à un temps récent) pour la finance internationale, la médecine, la pêche ou la conduite automobile pour ne citer que ces quelques exemples ; dans ces derniers cas, la direction générale – ou l'institution au sens large – privilégie d'abord son exposition au risque, et les actions de sécurité sont plutôt à mener au niveau local en admettant leur valeur locale et limitée.

On comprend qu'un spécialiste de sécurité puisse aller d'un système à l'autre dans sa carrière, utiliser les mêmes outils, les mêmes connaissances, et pourtant obtenir des résultats extrêmement différents. Le cadre d'acceptation du risque joue comme une poutre sur le niveau de sécurité, alors que les actions locales ne sont que des pailles avec des effets de levier très limités dans le temps et dans l'espace, qui ont d'autant moins de chance d'être relayées par le management qu'elles seront perçues comme incompatibles ou gênantes pour l'économie globale du système.

41. Wilson R (1979) Analyzing the daily risks of life. Technology Review 81: 40-6, ou http://muller.lbl.gov/teaching/physics10/old%20physics%2010/physics%2010%20notes/Risk.html.

42. Rasmussen J (1997) Risk management in a dynamic society. Safety Science 27: 183-214.

On reverra ces points dans les paragraphes suivants en analysant les travaux sur les types de sécurité et les marges d'actions, puis ceux sur la façon de construire arbitrages et compromis.

Cinq barrières qui expliquent les différences entre les systèmes peu sûrs et les systèmes ultrasûrs[43]**.**

La première barrière est l'absence d'une limitation de performance imposée par la régulation autoritaire du système. Par exemple, le marin pêcheur peut rester en mer même par force 10, l'alpiniste professionnel peut décider de partir faire le sommet quelles que soient les conditions de risques, et le médecin de garde de l'équipe d'urgence doit voir toutes les personnes qui se présentent, sans espoir de relais même s'il est épuisé. En l'absence de régulation freinant l'exposition aux risques, ces métiers ne peuvent espérer avoir un niveau de sécurité supérieur à 10^{-3}. **La seconde barrière** porte sur l'autonomie des acteurs. Si seule la réalisation de votre but personnel compte pour vous, et que vous ne prenez pas en compte les conséquences pour les suivants de vos actes, vous n'avez aucune chance de dépasser un niveau de sécurité de 10^{-4} pour votre activité. Le chirurgien en retard de 4 heures sur son programme pourra réaliser son programme sans erreurs, mais le risque viendra de la remontée du patient opéré dans les étages à minuit ou 1 heure du matin dans des conditions où il y a moins de soignants et à un horaire vulnérable pour la surveillance postopératoire. Une attitude sûre consisterait à intégrer la contrainte de l'étage, et sans doute renoncer à son programme opératoire décalé. **La troisième barrière** « ou barrière de l'artisan » résume socialement les effets précédents. On ne se pose pas de question de qui est le pilote de ligne, ou qui est le biologiste, mais on choisit le bijoutier ou le chirurgien ; ce sont des artisans ; ils vendent leurs différences et leur savoir personnel. Or il n'existe pas de profession artisanale dans le monde qui bénéficie d'une sécurité supérieure à 10^{-4}. La raison est simple, la sécurité repose sur la réduction des différences et la stabilité du service 24 heures/24, alors que l'artisan se vend justement sur sa différence avec son voisin et concurrent : il crée donc par construction l'instabilité du système global. **La quatrième barrière,** dite « de surprotection » est déjà l'apanage de systèmes sûrs. Plus le système se sécurise, plus il s'expose paradoxalement à des enquêtes lors des accidents restants et des mises en cause de responsable ; la réponse est souvent de faire croître très rapidement les procédures parapluies censées protéger le management. Ces procédures parapluies corsètent inutilement le travail, alourdissent le travail et favorisent des déviances et des migrations de pratiques des opérateurs de proximité en augmentant paradoxalement le risque dont elles veulent se protéger. Enfin **la cinquième barrière** concerne la perte de la rationalité dans la communication de sécurité pour les systèmes devenus très sûrs. Les accidents sont moins nombreux, plus médiatiques. Une partie importante de la communication des dirigeants et des actions consiste alors à rassurer les médias. Les propos et

43. Amalberti R, Auroy Y, Berwick D, Barach P (2005) Five system barriers to achieving ultrasafe health care. Ann Intern Med 42: 756-764.

les affirmations sont souvent précipités (on lit les statistiques de surface et on se vante de progrès sans prendre le recul) dans le sens de ce qu'attend la presse (et pas nécessairement dans le sens du modèle de sécurité). Avec cette logique d'empilement de décisions non évaluées sur leurs résultats objectifs, le système de sécurité devient un gigantesque millefeuille de procédures et d'exigences, dont personne ne sait celles qui contribuent réellement à l'obtention du niveau de sécurité ; le système devient alors incapable de s'autonettoyer, se complexifie à outrance, et produit lui-même son asymptote de sécurité[44].

Étape 4 : une fois toutes les étapes franchies, est-on encore capable de résister à l'exceptionnel ?

Sécurité gérée et sécurité réglée

La sécurité des systèmes complexes est la somme de deux entités ; d'une part la sécurité procurée par toutes les interdictions, limitations, exigences légales (dite sécurité réglée) et d'autre part la sécurité portée par l'intelligence adaptative des opérateurs et professionnels du système (sécurité gérée). Ces deux concepts, maintenant largement repris dans la littérature, ont été introduits pour la première fois en 2008 dans l'article *princeps* publié dans *Human Factors* sur les travaux sur les pêcheurs professionnels dans la thèse de Gaël Morel[45].

Sécurité totale = sécurité réglée + sécurité gérée

Considérons les termes de cette équation pour l'appliquer à différents domaines professionnels.

Les systèmes artisanaux ont peu de règlements ; leur sécurité totale, assez modeste, repose largement sur les qualités et les compétences des opérateurs avec les fortes variations inhérentes aux qualités individuelles. En revanche, l'adaptation aux conditions exceptionnelles de ces experts est journalière et remarquable (tout du moins pour les meilleurs, ceux qui survivent économiquement et physiquement).

Sécurité totale (systèmes artisanaux) = sécurité réglée + sécurité gérée
(la taille des fonts exprime métaphoriquement la force de chaque terme de l'équation)

44. Perrow C (1984) Normal accidents: living with high-risk technologies. Basic Books: NY.

45. Morel G, Amalberti R, Chauvin C (2008) Articulating the differences between safety and resilience: the decision-making of professional sea fishing skippers. Human factors 1: 1-16.

Les systèmes très sûrs ont au contraire beaucoup de procédures et d'interdictions. Leur niveau de sécurité est élevé, mais l'expertise adaptative de leurs opérateurs est mécaniquement réduite, puisque ces derniers ne sont plus exposés à des situations exceptionnelles et ne s'entraînent plus à travailler hors cadre procédural.

Sécurité totale (systèmes ultrasûrs) = sécurité réglée+ sécurité gérée

Il n'y a pas à ce jour de solution connue préservant à la fois l'expertise des opérateurs aux situations exceptionnelles et le bénéfice d'une sécurisation maximale des systèmes par des voies procédurales.
On retient que la résilience ou art de s'adapter aux conditions exceptionnelles est une donnée native des systèmes humains confrontés à leur propre autonomie pour survivre ; elle disparaît mécaniquement avec les outils de sécurisation traditionnels utilisés dans l'industrie et les services. Souvent, on souhaiterait en avoir moins dans les systèmes peu sûrs (car elle s'assortit d'improvisations et de non-conformités en série) et on souhaiterait en avoir plus et la réintroduire dans les systèmes ultrasûrs (car elle permettrait une adaptation aux situations exceptionnelles qui est largement perdue à ce stade).

Le choix de sécurité de l'aéronautique : supprimer les héros et interdire l'entraînement aux situations trop exceptionnelles.
En 1995 surviennent deux accidents et incidents graves sur Airbus A310 qui laissent penser que les pilotes n'ont plus assez d'entraînement aux manœuvres difficiles. On a d'abord un accident au décollage de Bucarest avec un équipage distrait ou occupé, qui laisse partir l'avion en inclinaison latérale (*overbank*) et qui ne saura pas récupérer cette situation inusuelle ; quelques mois plus tard, en approche de Paris, un équipage d'un autre Airbus A310 est surpris par une attitude inattendue de la machine et récupère très difficilement et avec beaucoup de chances l'appareil sans dommage. Les deux commissions d'enquêtes insistent sur le manque d'entraînement de ces pilotes sur avions modernes clairement mieux formés à être gestionnaires d'ordinateurs et à utiliser le pilote automatique qu'à piloter eux-mêmes manuellement. La réponse des autorités de l'aviation civile est sans concession : hors de question de reprendre un entraînement au pilotage manuel, qui plus est dans des situations exceptionnelles. Ce serait rouvrir la porte aux « héros » qui sortaient trop souvent des procédures standard ; l'aéronautique a mis tant de temps à les éliminer. La solution préconisée sera de miser sur les alertes pour mieux signaler que l'avion sort de son domaine normal de vol, et de plus miser sur les automatismes et le *safety-net* pour récupérer ces situations inusuelles automatiquement. Cette posture s'est confirmée à chaque accident exceptionnel.
Il s'agit d'un exemple caricatural d'un système (l'aviation civile) qui a parié à fond dans la procédure et la supervision, et qui en bénéficie tous les jours en matière de résultat de sécurité (une des meilleures sécurités du monde) mais qui se trouve maintenant enfermé dans cette logique. Toute réintroduction d'improvisation dans des domaines hors procédures est d'abord vue comme une mise à risque du système et se trouve en conséquence bannie.

À noter aussi que le cas très connu de l'atterrissage réussi sur l'Hudson du vol US Airways en 2009 est simplement considéré comme un coup de chance dans le milieu de la régulation aéronautique, et ne remet pas en cause le modèle décrit précédemment (il n'y a d'ailleurs eu aucun apprentissage collectif et professionnel issu de cet accident dans le milieu aéronautique, même s'il a par ailleurs nourri nombre de cercles de chercheurs qui veulent le réutiliser pour leur propre cause).

La résilience institutionnelle : survivre à l'accident peut s'avérer aussi important qu'éviter l'accident

Les spécialistes de sécurité ont un modèle simple et unique en tête : réduire le nombre des accidents et des incidents. C'est oublier un pan entier de la sécurité typiquement systémique : savoir survivre aux accidents.

Cette approche peut paraître cynique, mais elle doit être intégrée comme une composante à part entière de l'approche moderne de sécurité d'une entreprise ou d'un système complexe.

Ce faisant, elle ajoute un volet critique aux deux thèmes bien connus de la gestion des crises (*savoir réagir à l'accident* et *savoir gérer la communication*) en insistant sur « *savoir préserver la production dans les suites de l'accident* ». À y regarder de près, ce troisième volet peut même être le plus important. Il encourage à prolonger la cellule de crise bien au-delà de l'accident, pour gérer les « préjudices d'image à distance ».

L'accident n'est qu'un événement isolé dans une vie d'un système. Il peut (c'est souvent le cas) se répéter à intervalle régulier. Chaque accident est comme une attaque cardiaque pour la vie humaine, ou une récidive de cancer. Il met en jeu le pronostic vital de tout le système.

Un modèle de résilience institutionnelle : l'exemple d'Air France.

La compagnie Air France a subi cinq accidents majeurs en 15 ans (747 à Papeete en 1993, 747 cargo à Madras en 1999, Concorde à Paris en 2000, A340 à Toronto en 2005, et A330 entre Rio et Paris en 2009) et une série d'incidents majeurs dans la même période. Cela fait d'Air France la plus risquée de toutes les compagnies majeures dans le monde. Pourtant, à la différence de ses concurrentes qui ont eu moins d'accidents (parfois un seul) et en sont (presque toutes) mortes économiquement (TWA, Swiss Air par exemple), Air France a su ne pas écorner son image après ses accidents, et parfois même gagner des parts de marché ! C'est un exemple de résilience d'entreprise. Un exemple : dans la nuit du crash de son A340 en 2005 à l'aéroport de Toronto causé par un mauvais jugement de son équipage, la direction d'Air France a réussi l'exploit d'induire une lecture positive de son image d'entreprise, immédiatement et à distance, grâce à un traitement « positif » de l'accident relayé par tous les relais de presse et les agences d'informations internationales, montrant sa capacité à évacuer un avion en difficulté. C'est cette image qui est restée dans le

grand public. Cette capacité ne doit rien au hasard. Elle se prépare à l'avance, se gère en direct, et s'inscrit dans un plan postaccident très anticipé. Cette capacité fait partie des savoir-faire de la compagnie.

Trois modèles de sécurité en équilibre, et non un seul

L'idée d'un modèle unique de sécurité qui s'appliquerait à tous, et consisterait à viser le zéro accident est naïve. La sécurité est une construction sociale, qui s'adapte à la demande. Ce paragraphe montre qu'il existe plusieurs réponses de sécurité, qualifiant plusieurs modèles authentiques de sécurité (résilient, HRO, ultrasûr), avec leur propre logique, leur propre avantage et leur propre limite. Ces modèles se distinguent entre eux en échangeant le bénéfice de leur adaptabilité avec le bénéfice de leur niveau de sécurité.

Trois stratégies bien différentes d'exposition au risque

Chacun conviendra qu'écrire un plan de sécurité n'est pas une garantie que ce plan soit mis en pratique.
Chacun conviendra aussi qu'il est rare dans un plan de sécurité de mentionner ce qui ne va pas être fait parce que des arbitrages en ont décidé ainsi.
Ces deux aspects (bien faire ce que l'on a décidé, et bien connaître ce que l'on a décidé de ne pas faire) sont stratégiques dans la gestion du risque sur le terrain.
Les exercices papiers et crayons obligés de cartographie et de protocoles de prévention des risques développés pour les tutelles sont sans doute indispensables, mais ne sont souvent que des efforts de l'instant (pour la démonstration) qu'il va falloir ancrer dans une réalité au quotidien, et sur une longue période… et c'est là un autre problème.
En l'absence d'une concertation et d'arbitrages réalisés au niveau supérieur, les cadres de proximité et les personnes au front du travail vont être le niveau d'intégration de toutes les contraintes (contradictoires) provenant des différentes directions : produire plus, dans des conditions d'adaptation assez forte à la situation, tout en appliquant les consignes et règles de sécurité. Tout est alors à craindre en matière d'interprétations locales erronées et de nouvelles vulnérabilités.

Trois familles de plans ou de solutions de sécurité s'offrent en permanence aux systèmes sociotechniques pour gérer les risques quotidiens.

• **PLAN A. La première famille de solutions de sécurité consiste à supprimer ou retarder l'exposition au risque, on l'appellera plan A :** l'aéronautique excelle dans cette stratégie. Grâce à sa couverture mondiale et à son autorité absolue, le contrôle aérien peut éviter l'exposition des avions aux conditions difficiles. C'est aussi le cas

du nucléaire, qui dispose de procédures d'incidents très robustes qui convergent vers la mise en sécurité immédiate de l'installation et l'arrêt temporaire. Cette supervision sert en retour une économie d'échelle dans la formation : inutile de former les pilotes à piloter dans des conditions d'ouragan si l'on sait pouvoir éviter tous les ouragans. Mais cette stratégie prudente exige aussi de grandes qualités de supervision systémique souvent hors de portée d'activités industrielles fragmentées, dérégulées et/ou très compétitives, en d'autres termes des systèmes artisanaux.

La capacité d'application du plan A dépend de l'organisation du système. Prenons l'exemple de comparaison entre deux systèmes de soins en France et au Royaume-Uni pour le cas d'une prothèse de hanche chez un sujet ayant des comorbidités (ayant d'autres maladies que son problème de hanche, comme le diabète ou l'hypertension). La prothèse dans ce cas n'a jamais un caractère d'urgence et il vaut mieux attendre des conditions de contrôle parfait des comorbidités avant l'intervention pour éviter les complications postopératoires. Cette stratégie d'attente de conditions favorables fonctionne assez bien au Royaume-Uni parce que le système d'accès aux soins est très régulé ; inversement, elle est assez inefficace en France car l'offre privée est trop grande et trop peu régulée ; les patients peuvent consulter autant de chirurgiens qu'ils le souhaitent, en étant remboursés, jusqu'à obtenir une date d'intervention très proche de leur convenance. Pas étonnant dans ce contexte que les chirurgiens français prennent plus de risques que leurs homologues anglais pour ne pas laisser partir le patient, et emploient moins le plan A.

• PLAN B. La seconde famille de solutions de sécurité consiste à accepter l'exposition au risque en respectant toutes les normes et procédures recommandées (on l'appellera plan B) mais en gardant une capacité de détection de variation dans le contexte, et d'adaptation locale et intelligente de ces procédures (la procédure au cœur du dispositif). L'application stricte et standardisée de toutes les recommandations professionnelles dans des conditions nominales de travail correspond au taux minimum d'accidents. Ces plans B nourrissent en général, avec les plans A, les réponses réglementaires aux tutelles.

Bien sûr aucun univers professionnel ne se déroule sans incidents, et notamment sans surprises. Il faut donc, pour tirer le maximum de bénéfice de cette approche, soit pouvoir revenir à un arrêt et une mise en sécurité rapide du système (*no go*), soit disposer de procédures non univoques pour traiter l'incident (procédures spécifiques pour traiter chaque cas répertorié d'événement anormal). Il faut dans ce cas que l'opérateur soit bien conscient de l'évolution de la situation, sache identifier les problèmes et appliquer ces procédures.

On notera que la mauvaise ergonomie des systèmes peut facilement compromettre cet objectif. Dave Woods, reprenant les travaux pionniers de Lisane Bainbridge[46], a par exemple largement pointé le risque de « surprises » dans les situations standardisées des univers ultrasûrs où les changements ne sont pas fréquents ; ces surprises sont surtout liées à une conception et une supervision ne maîtrisant pas les règles éthiques

46. Bainbridge L (1987) Ironies of automation. In: New technology and human errors, sous la dir.de Rasmussen, Duncan & Leplatedts. Wiley publ., p. 271-86.

de stabilité de l'outil de travail (voir exemple dans la suite du texte). Woods et Hollnagel[47]en avaient déduit quelques principes ergonomiques qui allaient marquer la conception des systèmes sûrs ; ils avaient notamment repris et popularisé sous le terme de *Joint Cognitive System* l'idée ancienne soutenue par l'ergonomie française depuis les années 1960[48] : « l'analyse ergonomique fait fausse route en décomposant de façon cartésienne le travail pour l'analyser partie à partie (l'analyse du travail) » ; l'engagement de l'opérateur fait corps avec le contexte technique et ne peut être étudié que comme un couplage dynamique. À noter aussi la contribution de Mica Endsley[49,50], qui a utilisé ce courant pour proposer de tester l'adaptation de la compréhension de l'univers dans lequel évolue l'opérateur par son concept de conscience de la situation (*Situation Awareness*).

Un exemple de surprise inacceptable liée à la conception[51]**.** À la fin des années 1980, les premiers Boeing 737 avaient une fonction ALT HOLD qui permettait de stabiliser l'altitude de l'avion sur un plan vertical (l'arrêter de monter ou de descendre) en appuyant simplement sur un bouton dédié ; or l'appui sur ce même bouton devenait inopérant dans la phase finale avant atterrissage, car le constructeur avait voulu se prémunir contre un actionnement involontaire de l'équipage du bouton ALT HOLD, qui aurait pu gravement perturber la procédure d'atterrissage automatique par conditions de visibilité dégradée (procédure CATégorie 3). À noter que cette protection avait été installée pour satisfaire aux exigences de sécurité imposées par les tutelles pour obtenir la qualification CAT 3. Le résultat a été éloquent : dans cette phase finale, pour obtenir le même résultat (stabiliser l'altitude), il fallait respecter une séquence d'action complexe : d'abord déconnecter le pilote automatique, puis déconnecter les deux directeurs de vols en place droite et en place gauche, puis reconnecter le pilote automatique, et enfin appuyer sur ALT HOLD. Plusieurs accidents et incidents graves ont été provoqués par cette ergonomie ingrate avant qu'elle soit corrigée : les pilotes, n'ayant pas réalisé qu'ils étaient dans ces conditions d'approche interdisant l'usage direct de ALT HOLD, appuyaient sur le bouton ALT HOLD et n'obtenaient rien, et il s'en suivait un moment de surprise et des actions inappropriées à la source des incidents/accidents.

• Plan C. La troisième famille de solutions de sécurité consiste à tolérer l'exposition dans des conditions hors normes en acceptant que les opérateurs improvisent ou sortent de la conduite procédurale. On l'appellera plan C. La vie dans beaucoup de

47. Woods DD, Hollnagel E (2006) Joint cognitive systems: patterns in cognitive systems engineering. BocaRaton, FL: 2006, Taylor & Francis.

48. deMontmollin M. L'ergonomie de la tâche, Peter Lang, Berne, 1986.

49. Endsley MR, Garland DJ (2000) Situation awareness analysis and measurement. Mahwah, NJ: Lawrence Erlbaum.

50. Endsley M (1995) Toward a theory of situation awareness in dynamic systems. Human Factors 37: 32-64.

51. Sarter N, Woods D (1992) Pilot interaction with cockpit automation: operational experiences with the flight management system. International Journal Aviation Psychology 2(4): 303-21.

métiers n'est pas faite que de répétitions procédurales, bien au contraire. Cette qualité de l'adaptation a beaucoup fait parler la petite communauté des sciences humaines autour de l'idée de résilience.

La métaphore de la falaise et du grimpeur. Considérez que les **dangers** sont des falaises. Ils sont inévitables et font partie de la nature. Dans l'industrie, ces falaises pourraient représenter des patients malades, des propriétés chimiques de composés, des radiations solaires… Les **risques** dépendent de la volonté et de la façon d'affronter ces falaises. On peut ne pas les monter (plan A), se limiter à monter les falaises connues avec toutes les procédures requises (plan B), ou affronter des falaises en situation non standard (sans matériel, sans entraînement, dans des conditions dégradées ou changeantes), ou pire monter des falaises inconnues (plan C). Plus un système est stable et supervisé, plus il pariera sur l'évitement, les plans A et B, et moins il est stable et plus il devra miser sur son adaptabilité aux conditions changeantes (plan C).
En bref, les solutions ne sont pas portables d'un univers à un autre ; elles renvoient à des objectifs différents, des modèles de sécurité distincts, des entraînements et des formations différents, et des logiques d'organisation différentes.

En dehors de quelques industries ultrasûres, la plupart des activités humaines professionnelles utilisent intensivement les plans C. Mais bizarrement, l'ensemble de la littérature sur la qualité et la sécurité des systèmes ne donne des prescriptions que pour les plans A et B.
Or ce n'est pas parce que les plans C ne suivent pas toutes les procédures et conduisent à improviser, qu'il n'existe pas de possibilité de sécuriser leurs pratiques. Mais le problème, c'est que les solutions sécurisant ces pratiques tout en acceptant leur réalité ne consistent pas à développer des procédures (sinon on se replace dans une logique de plan B, on répond ponctuellement, mais sans couvrir l'ensemble des cas d'une activité, qui par sa logique économique, est obligée à travailler très souvent en plan C). Les solutions de plan C relèvent plutôt des modèles résilients : être plus expert, savoir juger de la difficulté de la tâche en fonction de ses capacités, apprendre à apprendre, à tirer les leçons, à posséder des schémas de connaissances génériques sur l'adaptation aux circonstances limites.

Trois plans génériques pour gérer le risque :
– PLAN A : renoncer à faire, ou attendre des conditions idéales ;
– PLAN B : exécuter le travail en conditions idéales selon les procédures recommandées ;
– PLAN C : accepter d'intervenir sans avoir les conditions idéales, avec improvisation et travail hors procédures.

En aviation, le ratio est de 40 % de plans A, 55 % de plans B, et 2 à 5 % de plans C.
En médecine, le ratio est de 5 à 10 % de plans A, 40 % de plans B, 55 % de plans C.

Quel est votre ratio dans votre activité entre plan A, plan B et plan C ?
Si votre ratio de plan C dépasse 5 %, que valent vos procédures prévues pour le plan B dans ces cas où vous êtes en plan C ?

Deux univers professionnels et deux stratégies de sécurité diamétralement opposées = aider à survivre au risque *versus* protéger ses opérateurs de l'exposition au risque

Les systèmes qui ont un niveau de sécurité relativement modeste (inférieur à 10^{-4}) ont une exposition au risque considérable parce qu'ils vivent littéralement de cette exposition. C'est le cas des pilotes de chasse, des marins pêcheurs, des alpinistes professionnels. Pour ces professions, l'exposition et même la recherche du risque est l'essence du métier. Pour autant ces métiers veulent une meilleure sécurité. Une série de travaux chez les pilotes de combat[52] et les marins pêcheurs[53, 54] montrent un vrai besoin de sécurité. Par exemple, les pêcheurs souhaitent un système d'anticollision intelligent pour mieux les protéger par mer démontée sans visibilité et avec une mobilité imposée par le chalut (*Automatic Radar Plotting Aid*). Les pilotes de combat souhaitent un filet de sauvegarde électronique pour mieux les protéger quand ils font des manœuvres susceptibles de leur faire perdre conscience (*Electronic Safety Net*). Si l'on prend maintenant l'exemple de l'aéronautique civile, tout le monde veut aussi améliorer sa sécurité. Mais la solution est radicalement différente et consiste le plus souvent à ne plus exposer les équipages à des conditions de surprises ou de risques qu'on pense à l'origine d'accidents. Par exemple, l'épisode du volcan Eyjafjöll en Islande en 2010 a immédiatement conduit à clouer tous les avions au sol avec une logique simple : pas d'exposition donc pas de risque. Ces différents exemples mettent en valeur deux stratégies totalement opposées de traitement du risque : l'une, portée par les petits systèmes artisanaux ou hautement compétitifs, consiste à parier sur l'intelligence des opérateurs, et à les doter d'aides pour affronter le risque ; l'autre consiste à parier sur l'organisation et la supervision et à ne plus exposer les opérateurs aux risques. On peut aisément comprendre que les deux modèles ont leur logique propre, mais il faut alors accepter que les solutions pour la sécurité ne soient pas les mêmes dans les deux cas.

Trois authentiques modèles de sécurité et non un seul

Compte tenu des stratégies d'exposition au risque vues précédemment, il est logique de penser que chacune d'elles a donné lieu à une authentique organisation de la sécurité, originale, avec ses logiques et ses possibilités propres d'amélioration[55, 56].

52. Amalberti R, Deblon F (1992) Cognitive modelling of fighter aircraft's control process: a step towards intelligent onboard assistance system. International Journal of Man-Machine studies 36: 639-71.

53. Morel G, Amalberti R, Chauvin C (2008) Articulating the differences between safety and resilience: the decision-making of professional sea fishing skippers. Human factors 1: 1-16.

54. Morel G, Amalberti R, Chauvin C (2009) How good micro/macro ergonomics may improve resilience, but not necessarily safety. Safety Science 47: 285-94.

55. Amalberti R, Barach P. Improving healthcare: understanding the properties of three contrasting and concurrent safety models. Submitted.

56. Grote G (2012) Safety management in different high-risk domains – All the same? Safety Science, in press, 2012.

• **Le modèle résilient** concerne les métiers où la recherche de l'exposition au risque est l'essence même du modèle économique de la profession. Les professions artisanales notamment se vendent sur leur expertise à accepter d'affronter des nouveaux risques, voire à affronter l'inconnu, à innover, à maîtriser de nouveaux contextes, à résister, à gagner, et à faire du bénéfice là où les autres font naufrage ou ont peur d'aller. C'est la culture des champions, des winners… et des losers (les losers font partie du contexte, mais ils ne sont pas vécus comme les échecs du système mais plutôt comme le reflet de la qualité du savoir des champions). Les marins pêcheurs par exemple sont capables de rechercher les pires conditions de risques pour prioriser la capture du poisson le plus rentable, au meilleur moment (économique de vente) ; les experts en forages pétroliers doivent trouver le pétrole presque à tout prix une fois la procédure lancée ; seule la réussite a du sens. Les traders doivent maximiser leurs gains sans limites, les pilotes militaires d'avions de combat[57] ne peuvent que gagner… Tous ces métiers ont des statistiques objectives d'accidents plus ou moins calamiteuses. Pourtant, ils ne sont pas insensibles à leurs risques professionnels et les traitent avec une stratégie de sécurité et de formation tout à fait réfléchies, mais bien sûr dans une culture différente.
Dans ces métiers, l'autonomie et l'expertise des individus prennent le pas sur une organisation hiérarchique du groupe. Le groupe est d'ailleurs souvent très petit (deux à huit individus) et travaille dans un univers très compétitif. Le chef est reconnu pour ses qualités techniques, ses performances passées, son charisme, plus que par son statut officiel. Chaque opérateur est invité en permanence à utiliser une très grande marge d'initiative. La bonne estimation de ses compétences, le courage et l'expérience accumulée sont les clés pour être reconnu comme « un bon professionnel et un gagnant » ; la sécurité est d'ailleurs surtout associée à gagner, à survivre, et seuls les gagnants communiquent leur savoir-faire de sécurité à travers des récits de champions. Pour résumer, les procédures sont peu nombreuses, l'autonomie très grande, et le nombre d'accidents très élevé. Pour autant, on peut progresser en sécurité locale en se formant mieux au contact des meilleurs maîtres, en apprenant de leur expérience et en augmentant son catalogue mental de possibilités d'adaptation à des situations les plus dégradées. Les différences entre les opérateurs les moins sûrs et les opérateurs les plus sûrs dans un

57. Le cas des pilotes de combat est un cas particulier et intéressant de double contexte : en temps de paix, leur administration (l'Armée de l'air) déploie un modèle plutôt de type ultrasûr, mais dès que les avions partent au combat, le modèle d'exploitation change brutalement et retourne vers ses fondamentaux de résilience. Ces univers très opposés ne manquent pas de produire des surprises pour la sécurité dans les deux sens : persistances de comportements résilients et déviants (par rapport au modèle désiré en temps de paix) au retour des campagnes militaires, et pertes de chances importantes les premiers jours d'engagement par manque de pratique du modèle résilient, quand les pilotes sont projetés brutalement du temps de paix vers des théâtres opérationnels. Les capacités de l'aviation militaire peuvent d'ailleurs projeter un équipage d'avion de surveillance AWACS du temps de paix au temps de guerre sur l'espace d'une seule mission : départ d'une base française en France, après avoir accompagné les gamins à l'école le matin…, mission de 12 heures avec travail et survol d'un théâtre opérationnel à très haut risque d'engagement aérien où la résilience est particulièrement requise, et retour la nuit suivante en France sur leur base aérienne et à leur domicile totalement organisé autour des routines sociales et de problématiques du temps de paix.

même métier artisanal résilient sont de l'ordre de facteur 10[58], ce qui prouve bien que l'on peut progresser en intervention de sécurité même en restant dans la « microgaussienne » de distribution des professionnels pratiquant ces métiers périlleux.

• **Le modèle des HRO** (*High Reliability Organizations*) reprend la même idée de résilience parce qu'il prône aussi l'adaptation, mais c'est une adaptation plus locale, plus réglée, qui concerne des activités humaines nettement plus organisées, et moins en recherche de l'exploit (qui caractérise le modèle résilient pur). Le modèle HRO est même relativement aversif à l'exploit individuel sans contrôle du groupe.
Les HRO concernent typiquement les métiers où gérer le risque est quotidien, même si l'objectif reste de le contrôler et de ne pas s'exposer inutilement : lutte contre le feu, marines marchande et militaire, professionnels du bloc opératoire, forage pétrolier, exploitation d'usines chimiques.
Les HRO parient sur le leader et sur le groupe professionnel réunissant différents rôles et expertises pour assurer une vision permanente et globale de la progression vers le but (en s'évitant le risque de focalisation locale), avec une participation de tous les membres du groupe à détecter les anomalies de contexte (*sense making*), à les porter à la connaissance du groupe, à adapter la procédure à ces changements de contexte, y compris en s'écartant des procédures quand c'est nécessaire (mais faisant sens dans le groupe et communiquées à tous). Tous les membres du groupe sont solidaires de cet objectif de sécurité.
La lutte contre l'adversité fait partie intégrante de l'approche HRO, mais la forte régulation collective (pas nécessairement uniquement par le leader) limite considérablement les initiatives individuelles isolées et favorise des décisions collectives prudentes.
Le modèle HRO analyse ses échecs et cherche à comprendre leurs raisons. Mais les leçons tirées de ces analyses d'accident concernent d'abord la façon dont a été gérée la situation, et comment on pourrait mieux la gérer à l'avenir.
C'est donc un modèle qui parie d'abord sur l'amélioration des barrières de détection et de récupération, et secondairement sur les barrières de prévention (qui consiste à ne plus s'exposer à ces situations difficiles). L'entraînement collectif est la base de la formation. Là encore, les différences entre les meilleurs et les moins bons opérateurs d'un même métier sont de l'ordre de facteur 10[59].

• **Le modèle des systèmes ultrasûrs** ne parie plus en priorité sur l'expertise exceptionnelle de ces opérateurs de première ligne pour se sauver des situations difficiles ; il lui faut des opérateurs équivalents, interchangeables chacun dans leurs rôles respectifs, et forcément dans ce cas d'un niveau standard. Le modèle parie en revanche sur les

58. Le taux d'accidents mortels du travail en pêche professionnelle en haute mer varie en France de facteur 4 entre les armateurs, et de facteur 9 au niveau mondial, source Morel, Amalberti, Chauvin, 2009, opus cité.

59. Le taux d'accidents mortels du travail dans l'industrie de l'extraction du gaz et du pétrole varie de 130 décès pour 100 000 travailleurs dans certains pays africains, à 12 décès pour 100 000 travailleurs dans les meilleurs puits ; la moyenne mondiale est de 30,5 décès pour 100 000 travailleurs, source http://nextbigfuture.com/2011/03/oil-and-gas-extraction-accidents-and.html

qualités de supervision externe qui vont pouvoir éviter à ces opérateurs d'être exposés aux risques les plus exceptionnels ; en limitant l'exposition des opérateurs à une liste finie de pannes et de situations difficiles, le modèle peut devenir totalement procédural, à la fois en conduite normale et en conduite anormale. L'aviation de ligne, le nucléaire, la biologie médicale ou la radiothérapie sont d'excellents exemples de cette catégorie. Les accidents sont analysés pour en trouver les causes, et les éliminer de sorte que l'exposition à ces conditions de risques soit réduite ou supprimée à l'avenir. Le modèle parie d'abord sur la prévention. La formation des opérateurs de front de ligne est centrée autour du respect des rôles réciproques, de la coopération dans l'application des procédures et la réaction aux situations anormales pour enclencher les procédures *ad hoc*. Encore une fois, les différences entre les meilleurs et les moins bons opérateurs d'un même métier sont de l'ordre de facteur 10[60].

Quatre leçons sont à retenir :
– les trois modèles de sécurité sont radicalement différents. Ils répondent à des conditions économiques différentes, ils ont leur propre logique d'optimisation, leur propre logique de formation, leurs propres avantages et limites. Ils s'inscrivent sur une courbe qui échange la flexibilité et l'adaptabilité avec la sécurité. Mais tous les trois ont la même capacité de s'améliorer en interne en faisant progresser leur sécurité de facteur 10 (10 fois plus sûr) ;
– les trois modèles ne sont pas miscibles. Mélanger les traits de l'un avec ceux de l'autre conduit à l'échec en matière de progrès de sécurité, et peut même être contre-productif. Par exemple, il n'est pas certain que réintroduire de l'entraînement à dévier des procédures et à affronter des situations inconnues en aéronautique civile ne dégraderait pas la sécurité plutôt qu'elle ne l'améliorerait (c'est la raison pour laquelle les tutelles mondiales se gardent de prendre ce chemin). Inversement, introduire des procédures contraignantes en aviation de combat ou dans la pêche en haute mer revient peut-être à avoir moins de morts… mais à condamner la profession ;
– les interventions locales ne peuvent pas changer le modèle. Si l'on intervient localement pour améliorer la sécurité d'une entreprise ou d'une unité particulière de travail dont l'ensemble de la profession relève plutôt de tel ou tel modèle (résilient, HRO ou ultrasûr), on n'a aucune chance de faire adopter les traits d'un autre modèle de sécurité (par exemple si l'on intervient sur une pêcherie, il est illusoire de leur conseiller une stratégie de système ultrasûr). Il faudra plutôt parier sur la capacité à progresser à l'intérieur du modèle de cet univers professionnel (résilient pour la pêcherie) en utilisant les stratégies propres à ce domaine, dont on a vu qu'il a quand même des marges de sécurité importantes puisqu'il peut progresser de facteur 10 ;
– la bascule d'un modèle à un autre est possible, mais nécessite un événement de fracture qui adresse toute la profession et son économie. Par exemple la chimie industrielle, encore portée çà et là par des modèles résilients datés des années 1960 et 1970, a définitivement basculé sur un modèle HRO après les événements survenus à Seveso en Italie

60. Le taux d'accidents d'avion varie de 0,63 par million de départs dans les pays occidentaux à 7,41 par million de départs dans les pays africains. La différence est de facteur 12, source IATA statistics, 23 February 2011, http://www.iata.org/pressroom/pr/pages/2011-02-23-01.aspx

en 1976 et la directive européenne qui a suivi en 1982. Ce sont souvent les mécanismes de tutelle qui imposent la bascule vers un nouveau système. On notera que dans ce cas, le système migre progressivement, perd les avantages du modèle ancien (un plus grand niveau d'adaptation et d'inclusion des situations considérées traitables dans le métier), mais gagne les avantages du nouveau modèle (en sécurité notamment).

On peut lire l'intérêt de chacun de ces modèles avec différentes convictions, et différentes logiques.
On peut considérer que le modèle résilient des marins pêcheurs n'est pas un problème majeur puisque leurs accidents n'ont pas de grandes conséquences externes à leurs professions. Après tout, il s'agit là d'un choix qu'il faut respecter. Mais inversement, le modèle résilient en médecine pose des questions éthiques complexes entre deux logiques contradictoires : donner accès, espoir et soins à tous en toutes circonstances (ce que fait mieux le modèle résilient que le modèle ultrasûr) et en même temps ne rien faire qui puisse aggraver et blesser le patient (*first do not harm*) (ce que fait nettement mieux le modèle ultrasûr ou même le modèle HRO que le modèle résilient).
On peut aussi considérer que le modèle nucléaire n'est pas assez sûr et plaider pour encore plus de normes et de protocoles, s'appliquant à des situations recensées de plus en plus improbables. C'est par exemple le cas après Fukushima ; après avoir testé toutes les centrales du monde entier pour le risque d'écrasement volontaire d'un avion de ligne après l'acte de terrorisme sur les Twin Towers du 11 septembre 2001, on va tester maintenant les mêmes centrales pour leur risque sismique et leur risque d'inondation et prendre des mesures de renforcement dédiées. En quelque sorte, on va faire entrer dans le possible ce qui était alors jugé impossible, et appliquer à ce nouveau possible les recettes des systèmes ultrasûrs. Cette stratégie, typique des systèmes ultrasûrs, est tout le contraire d'une solution résiliente : on renforce l'idée que le système ne peut se défendre bien que contre des risques connus, mais ce faisant on refuse l'idée d'apprendre à improviser pour une nouvelle surprise exceptionnelle qui ne manquera pas un jour de survenir (demain ? dans 5 ans, 10 ans, 20 ans ?) dans une des quelques 500 centrales nucléaires en activité dans le monde.
Mais serait-il réaliste pour le nucléaire d'adopter une autre stratégie ? Une stratégie vraiment résiliente ? Imaginons qu'à la suite de Fukushima, le nucléaire mondial décide de former ses opérateurs à une résilience plus grande et recommande un entraînement à l'inattendu[61], aux conditions jamais vues jusque-là. Il faudrait sans doute alors entraîner des brigades d'opérateurs à l'improvisation et à la sortie des procédures. Mais il faudrait aussi être cohérent et accepter un système à deux vitesses, l'un ultraprocédural tel qu'il est aujourd'hui préservant l'exceptionnel niveau de sécurité actuel ($1*10^{-7}$) obtenu grâce à un strict suivi des procédures (un style de sécurité

61. L'inattendu dont on parle ici n'est pas la surprise de l'arrivée d'une panne répertoriée et pour laquelle existe une procédure. Évidemment les pannes et problèmes ne sont pas annoncés à l'avance, mais ils font partie intégrante du modèle ultrasûr, avec des opérateurs entraînés à réagir. On parle ici de conjonctures jamais rencontrées jusque-là et pour lesquelles n'existe aucune procédure écrite. Il faut alors improviser.

qui s'appliquerait à 10^7 journées de travail[62] soit pendant 27 ans), et l'autre reposant sur une formation de quelques opérateurs experts, présents dans chaque centrale en double des opérateurs normaux, capables d'improviser, dont on se servirait une fois toutes les deux générations, soit trois fois par siècle… et dont il faudrait en revanche interdire l'accès aux commandes pendant les 27 années sans surprise exceptionnelle pour s'éviter des improvisations dangereuses et inutiles. Poser les termes de l'équation revient déjà à donner la réponse : infaisable.

Autre exemple d'actualité : beaucoup considèrent que la crise financière des *subprimes* et celle de la dette européenne qui ont frappé le monde depuis 2009 ont les mêmes racines : celles d'un modèle trop résilient, porté par une minorité d'acteurs où le gain du bénéfice est maximalisé en prenant des risques insensés, en masquant et complexifiant volontairement les manœuvres et les produits financiers pour contourner tous les processus de supervision. Bref, beaucoup dans la rue imaginent aujourd'hui que ce système doit changer de logique et adopter des règles de sécurité plus encadrées, plus procédurales, qui selon les convictions politiques des uns ou des autres, le conduirait au moins à adopter des règles de système HRO, et pour certains à devenir un système totalement supervisé de type ultrasûr où toute autonomie de ses acteurs serait supprimée.

Mais les fondamentaux de ce système sont justement sa capacité à produire de l'argent sous un mode compétitif (libéral) pour refinancer le marché ; en bref, des conditions totalement contradictoires avec un système encadré.

Sans surprise, les propositions de moralisation de l'économie mondiale de marché et du rôle des banques, de leur réglementation et de leur encadrement sévère, voire de leur (re)nationalisation pour les plus ultras, bien que régulièrement au menu des sommets des G7 puis G10 n'aboutissent jamais, sinon sur des discours de bonnes intentions. La raison est simple : les modèles qu'il faudrait remettre en cause sont d'abord des modèles de société, avec des valeurs et des croyances construites sur les succès du passé que personne n'est réellement prêt à abandonner pour une hypothétique amélioration de la sécurité (dont on ne voit pas le résultat avant d'avoir fait tout le cycle de transformation et dont on voit tout de suite les inconvénients à assumer).

> On ne peut pas injecter un modèle de sécurité totalement nouveau contre la volonté des acteurs locaux et des valeurs considérées comme essentielles à ce système.
> Il faut d'abord faire bouger ces valeurs de fond pour prétendre après faire adopter un modèle de sécurité différent.

La leçon est simple, changer le modèle de sécurité demande à changer de système. Si les conditions ne sont pas réunies, et il faut parfois accepter ce fait, inutile de se battre contre les moulins ou d'inventer des solutions qui n'ont aucune chance de marcher.

62. Ce niveau de 10^7 de sécurité reprend le niveau garanti par les analyses de risques en conception pour l'aéronautique et le nucléaire.

Les propriétés de trois modèles de sécurité : le modèle de résilience, le modèle des HRO et le modèle des systèmes ultrasûrs.
Chaque modèle est une réponse à un type d'environnement, possède ses propres règles d'optimisation, et n'est que peu miscible avec un autre modèle. On note que chaque modèle peut progresser en sécurité d'un facteur 10 ; les chimères, mélangeant les éléments d'un système de sécurité avec un autre ne donnent en général aucun résultat de progression de sécurité (inadaptées, voire contra-productives).

	Modèle de la résilience	**Modèle des HRO *High Reliability Systems***	**Modèle de l'ultrasécurité**
Exemples	Alpinisme himalayen Pêche professionnelle Aviation de combat Finance internationale Urgences hospitalières	Marine marchande, Porte-avions, marine militaire Pompiers Industrie pétrolière Bloc opératoire	Aviation civile Trains et métros Industrie nucléaire Biologie médicale Radiothérapie
Rationalité	La prise de risque est l'essence du métier. On recherche le risque pour survivre dans le métier.	Le risque n'est pas recherché, mais il fait partie du métier.	Le risque est exclu, autant que possible.
Trait de culture principal	Fighter spirit, culte des champions et des héros.	Culte de l'intelligence du groupe et de l'adaptation aux situations changeantes.	Culte de l'application des procédures et de la sécurité organisée par une supervision efficace.
Caractéristiques des accidents et des leçons tirées pour la sécurité	Multiples, arrivent çà et là, peu de victimes à la fois, peu de médiatisation. Ne marquent pas la profession. Seuls les succès sont vraiment analysés (malheur aux perdants) ; on apprend sur l'adversité à travers l'analyse des récits de héros qui ont survécu à des situations exceptionnelles.	Fréquents, nombres de victimes variables, parfois forte pression médiatique, mais toujours des enquêtes et analyses des accidents. On apprend des échecs passés surtout à mieux gérer la même situation dégradée à l'avenir (améliorer sa détection et sa récupération, actions centrées sur la gestion des conséquences).	Rares, beaucoup de victimes et dégâts collatéraux, forte pression médiatique. On apprend des échecs passés surtout à ne plus s'exposer à de telles conditions (meilleure prévention, actions centrées sur la suppression des causes).

	Modèle de la résilience	**Modèle des HRO *High Reliability Systems***	**Modèle de l'ultrasécurité**
Trait principal du modèle qui procure la sécurité	La compétence experte des acteurs et leur expérience accumulée sur le domaine technique.	La compétence du groupe à s'organiser (rôles), à se protéger mutuellement, à appliquer les procédures, à se méfier des simplifications trop routinières de la situation, à s'adapter, à percevoir les variations de contextes, *sense making.*	La compétence des superviseurs du système à éviter d'exposer les acteurs au front de ligne aux risques inutiles. La compétence des acteurs du front de ligne à appliquer les protocoles.
Formations types des opérateurs pour améliorer la sécurité	Apprentissage par les pairs, accumulation d'expérience professionnelle, « training for zebra », travail sur la connaissance de ses propres limites.	Entraînement au travail en équipe pour acquérir une connaissance des capacités du groupe, et une adaptabilité de l'application des procédures en fonction du contexte.	Entraînement au travail en équipe pour appliquer les procédures et répartir le travail même en cas d'événements anormaux.
Niveau de sécurité objectif de ces systèmes	Entre 10^{-2} et 10^{-4}	Entre 10^{-4} et 10^{-6}	Meilleur que 10^{-6}
Capacité de progrès à l'intérieur du modèle	Facteur 10	Facteur 10	Facteur 10

Quelques règles complémentaires pour passer à l'action

On vient de voir que construire la sécurité n'est pas simple. Il faut connaître les risques, construire des défenses, et surtout être réaliste et choisir le bon modèle de sécurité. Mais cela ne suffit pas. La sécurité ainsi pensée, aussi pertinente soit-elle, nécessite d'être mise en route et maintenue dans le temps au plus proche du terrain. Le management a un rôle essentiel à ce niveau, à la fois pour influencer les comportements (et pas simplement diriger) et pour bien comprendre ce qui n'est pas couvert par le plan de sécurité. Enfin, il faut aussi gagner la bataille du futur et pas seulement penser un système qui corrige les erreurs d'un passé révolu.

Le rôle du management : bien faire ce qu'on a décidé de faire, et bien savoir ce qu'on a décidé de ne pas faire

Établir une stratégie de sécurité, aussi bonne soit-elle, n'a de sens que si elle est comprise et relayée. Il faut que le management ait compris les objectifs (ce qui doit être obtenu) mais aussi les impasses volontaires et leurs raisons (ce à quoi on renonce pour des raisons d'arbitrages par rapport à d'autres avantages commerciaux ou de business que l'on veut préserver). L'éducation et la formation du *middle management*[63] et du management de proximité à ces deux enjeux sont au cœur d'une démarche réussie. La littérature fourmille de travaux sur ce domaine[64]. Une très bonne synthèse est présentée dans les cahiers de sécurité industrielle de l'Institut pour la culture de sécurité Industrielle ; elle inspire très largement la présentation de ce paragraphe.

Bien faire ce que l'on a décidé de faire : le rôle clé du *middle management*

La fonction traditionnelle d'un manager est de gérer, c'est-à-dire d'accomplir sa tâche le mieux possible, de planifier les activités ou de commander. Il convient cependant d'y ajouter une volonté d'influencer, de guider ou d'orienter ses collaborateurs. C'est cette dernière aptitude qui fait du manager un leader. Elle est fondamentale pour progresser en sécurité puisque dans ce domaine aussi, la mobilisation collective passe obligatoirement par l'existence d'un certain leadership du management, entendu comme la capacité du manager à influencer les comportements pour qu'ils deviennent plus sûrs.

D'une part, chacun gère ses priorités en fonction de son contexte de travail et des messages qu'il reçoit. On est généralement attentif à ce qui préoccupe son chef, même s'il ne demande pas explicitement des comptes : en d'autres termes, si le chef n'est pas intéressé par un domaine, il y a peu de chances que ses collaborateurs s'y intéressent !

D'autre part, ce n'est pas parce que la sécurité des personnes concerne naturellement chaque individu, son intégrité, sa santé, que sa mobilisation sera forcément spontanée. Pour cela, chacun doit être éclairé sur les enjeux, convaincu sur les objectifs, et le mouvement doit être coordonné. Bref, les propres comportements sécurité du management sont des messages qui pèsent beaucoup plus que les différents slogans affichés dans l'entreprise. Ils démontrent la valeur qui est réellement attribuée dans l'entreprise à la sécurité et déterminent fortement le degré de motivation du personnel à agir en sécurité.

63. Les *middle managers* sont des managers travaillant à un niveau intermédiaire de la hiérarchie, entre le niveau exécutif et le niveau des cadres de proximité ; typiquement ils dirigent une unité fonctionnelle, source Uyterhoeven HE (1972). General managers in the middle. Harvard Business Review 50: 75-85 et Thakur M (1998) Involving middle managers in strategymaking. Long Range Planning 31: 732-41.

64. Hopkins A (2005) Safety, culture and risk, first ed. CCH Australia Ltd, Australia.
Hopkins A (2007) Holding corporate leaders responsible. Keeping Good Companies 59: 340-4.

Le management a un rôle clé de traduction et de suivi du plan de sécurité. Cette compétence se décline selon sept principes fondateurs décrits dans l'encart ci-après.

ENCART : Sept principes pour un leadership en sécurité industrielle (source ICSI, 2011)[65]

Principe 1	**Créer la vision sécurité (en cohérence avec les valeurs et les principes de management)** • S'approprier et décliner la politique sécurité de l'entreprise • Placer la sécurité au rang qu'elle mérite au regard des autres enjeux • Imaginer la situation future que l'on veut à partir du diagnostic sécurité • Donner des objectifs spécifiques, mesurables et atteignables • Construire la vision collectivement • Définir, à partir de la vision, les principes de responsabilité et les attentes en termes de comportement
Principe 2	**Donner à la sécurité la place qui lui revient dans l'organisation et le management, et la piloter au quotidien** • Intégrer la sécurité à tous les niveaux de l'organisation • Clarifier les rôles et attributions de chacun • Définir un plan de progrès déclinant la vision • Repérer systématiquement les obstacles • Assurer les moyens adaptés
Principe 3	**Faire partager la vision sécurité : influencer, convaincre et favoriser la remontée de l'information** • Rappeler régulièrement les objectifs et les attentes en termes de comportement • Renouveler les messages • Communiquer clairement • Organiser et promouvoir l'observation et le repérage des situations à risque y compris la détection des signaux faibles • Instaurer un climat de confiance, privilégier la transparence • Faire émerger les bonnes pratiques, encourager et accompagner les initiatives • Rappeler que la sécurité est l'affaire de chacun
Principe 4	**Être crédible : exemplarité et cohérence** • Garantir une compétence suffisante de tous les acteurs pour permettre l'appropriation des objectifs de sécurité • Être compétent, équitable et intègre dans son jugement sécurité • Être exemplaire dans le respect des exigences sécurité et de ses engagements y compris en situation perturbée • S'impliquer personnellement dans le déploiement du Plan d'Action Sécurité • Être capable de se remettre en cause et de questionner l'attitude y compris de ses supérieurs • Argumenter ses décisions

65. ICSI, Leadership en sécurité, Cahiers de la sécurité industrielle, consulté le 29 décembre sur http://www.icsi-eu.org/francais/dev_cs/cahiers/CSI-LIS-pratiques-industrielles.pdf.

Principe 5	**Favoriser l'esprit d'équipe et la coopération transversale** • Développer les échanges pour résoudre les problèmes de sécurité • Assurer des moyens de coordination permettant une vision globale des risques • Favoriser le partage des outils et des méthodes • Rapprocher les fonctionnels de la sécurité des opérationnels du terrain • Veiller à ce que chacun se sente intégré et solidaire • Croiser les objectifs apparemment contradictoires • S'assurer que les pratiques traditionnelles de groupe ne s'opposent pas à la transparence et à la démarche de progrès collective
Principe 6	**Être présent sur le terrain pour observer, écouter, communiquer efficacement** • Organiser les visites de terrain • Organiser des rencontres régulières avec les différents métiers • Associer les entreprises prestataires aux visites de chantier, encourager et favoriser l'accès au terrain pour la direction des entreprises prestataires • Souligner ce qui va bien, rappeler les enseignements des accidents passés • Repérer les difficultés de mise en œuvre des consignes et rechercher collectivement des solutions • Faire un retour aux acteurs concernés des constats sur le terrain • Rencontrer les victimes d'accidents
Principe 7	**Reconnaître les bonnes pratiques et appliquer une sanction juste** • Mettre en exergue les bonnes initiatives en sécurité • Choisir des moments clés pour récompenser et sensibiliser • Communiquer à froid sur l'inacceptable et les règles de sanction (éventuellement graduées) qui en découlent • Analyser soigneusement le contexte (environnement technique et organisationnel, encadrement) avant toute sanction et veiller à demeurer équitable et juste • Savoir justifier la sanction en toute transparence

Bien comprendre les sacrifices de sécurité acceptés dans le plan d'action décidé

Le management doit aussi comprendre les mesures qui ont été écartées du plan de sécurité et les raisons (souvent stratégiques, financières, arbitrages pour d'autres priorités) qui sont derrière ces sacrifices.

Ces décisions fragilisent la sécurité et doivent être prises en compte par une stratégie dédiée consistant autant que possible à réduire l'exposition à ces risques pour lesquels il n'y a ni procédure, ni entraînement, et à en parler suffisamment en réunion pour que les opérateurs soient au moins capables de détecter ces situations, et quelques clés pour les éviter.

Par exemple, les avions automatisés modernes sont protégés contre le décrochage par des cocons électroniques qui reprennent la main sur l'équipage quand les caractéristiques du vol (par sa vitesse, ou l'attitude inusuelle de l'avion) franchissent les valeurs seuils de tolérance. Dans de très rares conditions, ces avions peuvent toutefois être privés de ce cocon électronique et l'équipage être confronté à une perte de contrôle

et un décrochage. L'aéronautique a fait le choix de ne pas entraîner complètement les équipages à ces cas exceptionnels (pour des raisons de temps, de coût, et de technique – les simulateurs ne savent pas mimer ces conditions). Il faut dans ce cas que chacun soit bien conscient de ce trou de compétence et apprenne à minimiser les expositions à ces conditions exceptionnelles, soit par anticipation stratégique pour éviter les conditions où ce type de décrochage peut se produire (pertes totales des informations de vitesse notamment), soit par réaction immédiate quand le signal d'alarme d'approche de ces conditions retentit.

Autre exemple, la plupart des établissements de santé n'intègrent pas dans leur cartographie de risques l'administration erronée de soins par des juniors en stages laissés seuls en garde à l'hôpital dans les services ou aux urgences, notamment la nuit, les jours de fêtes, au mois d'août ou le week-end. Les hôpitaux intègrent bien en général le risque d'erreur des juniors dans leur cartographie, mais en précisant qu'il est protégé par la supervision des seniors. Or on est ici dans le cas où il n'y a plus de séniors. Les hôpitaux écartent ce risque de leur analyse parce qu'il les obligerait à reconnaître une attitude quasiment illégale et inavouable puisqu'il est impensable de laisser des apprenants seuls dans les protocoles officiels[66, 67, 68]. Dans ce cas, les cadres doivent savoir que ce risque n'est pas protégé et doivent organiser le travail autant que faire se peut pour prendre en compte cette exposition : consignes plus claires d'appel, paroles sur ce thème réellement échangées avec les juniors, apprentissage des gestes génériques de mise en sécurité des patients…

Dernier exemple, la cartographie officielle des risques des pêcheurs professionnels au chalut en mer du Nord insiste considérablement sur les risques de collision avec des tankers ou des ferries[69, 70]. La réponse prévue à leur plan de sécurité consiste à protéger les zones de pêches autorisées en les gardant séparées et sans intersection avec les grandes voies maritimes et autoroutes de la mer, et consiste à doter ces marins de systèmes de détection des autres navires (ARPA-*Automatic-Radar Plotting Aid*). Cette cartographie du risque néglige pourtant deux facteurs qui

66. Bell CM, Redelmeier DA (2001) Mortality among patients admitted to hospitals on weekends as compared with weekdays. N Engl J Med 345: 663-8.

67. Aylin P, Yunus A, Bottle A, *et al.* (2010) Weekend mortality for emergency admissions: a large multicentre study. Qual Saf Health Care 19: 213-7.

68. Young J, Ranji S, Wachter R, et al. (2011) July effect: impact of the academic year-end change over on patient outcomes. Ann Intern Med 155: 309-15.

69. Morel G, Amalberti R. Chauvin C (2009) How good micro/macro ergonomics may improve resilience, but not necessarily safety. Safety Science 47: 285-94.

70. Morel G, Amalberti R, Chauvin C (2008) Articulating the differences between safety and resilience: the decision-making of professional seafishing skippers. Humanfactors 1: 1-16.

renvoient à des fondamentaux de l'économie d'un métier très compétitif et soumis à des quotas (premier venu, premier servi, premier payé) : « le poisson n'est pas abonné » aux zones réservées à la pêche, et les systèmes d'anticollisions émettent sur votre propre position (c'est leur rôle), pouvant ainsi attirer les autres pêcheurs vers votre lieu de pêche. Sans surprise, des pêcheurs travaillent assez souvent hors zones autorisées et coupent volontairement leur système d'anticollision pour ne pas être repérés, alors que ce cas est exclu de l'analyse des risques. Là encore, il faut veiller à bien ouvrir la parole sur ces pratiques parmi les marins (plutôt que de les traiter par une omerta) pour ne pas traiter une matrice de risques naïve.

Ces trois exemples résument assez bien les quatre raisons les plus fréquentes d'écarter un risque (identifié) du plan de sécurité : trop gênant pour le *business model*, trop rare, trop coûteux à gérer, trop incorrect pour être avoué.
Règle pratique : il est toujours utile en fin de construction d'un plan de sécurité de balayer les domaines que l'on a sacrifiés en s'aidant des catégories précédentes pour mieux les repérer et les classer. Les risques ainsi identifiés doivent donner lieu à un traitement particulier qui est plus celui de l'information et de la conscience partagée qu'ils existent, qu'il faut savoir les identifier, et tout faire pour éviter leur rencontre.

Penser futur et non passé

Les techniques de gestion des risques sont essentiellement construites sur le rétroviseur. Elles lisent le passé pour se prémunir de l'avenir, et misent sur la stabilité du monde pour conserver la valeur des leçons tirées des erreurs du passé. L'évolution est intégrée sous forme d'une évolution plutôt que d'une révolution et les inférences sont plutôt linéaires en matière de risques.
Hélas, le monde n'est pas aussi linéaire ; il évolue par fractures et mutations brutales parfois après deux ou trois décades de stabilité. Ce sont le plus souvent les innovations techniques qui déplacent brutalement les métiers. En très peu de temps, un système technique donné peut devenir totalement obsolète et ses règles de sécurité avec. Ainsi, en moins de 15 ans, cette bascule s'est appliquée par exemple au remplacement de la photographie argentique par le numérique, à la fin des télévisions à tubes, à l'explosion des technologies nomades. Mais les révolutions ont aussi atteint plusieurs grands systèmes industriels : passage progressif du forage et de l'exploitation des puits de pétrole à l'exploitation massive du pétrole dans les schistes bitumineux, passage progressif d'une régulation du trafic aérien essentiellement humaine à une régulation automatisée (*data-link*), arrivée de nouvelles techniques et matériels de constructions allégées permettant des ouvrages d'art construits deux fois plus vite avec des caractéristiques jamais réalisées jusque-là en hauteur et sur sols fragiles, arrivée de nouvelles motorisations pour les automobiles, passage de la chirurgie invasive à la chirurgie percutanée ou par voie naturelle non invasive, fin annoncée de la transfusion sanguine remplacée par la production de sang par des cultures de cellules souches…

Le point essentiel à retenir est que la technique ne change jamais seule. Elle change l'organisation du système, son modèle de business, ses acteurs aussi (de nouveaux venus profitent du saut technologique pour remplacer les anciens, exemple de l'industrie de la photographie numérique), en bref, tout le modèle et donc toute sa cartographie de risque et les défenses à construire.
Il faut donc en permanence regarder à l'horizon, et en permanence requestionner le modèle de sécurité que l'on a construit sur les bases du passé. Dans cette mouvance accélérée des technologies, les méthodes prospectives peuvent s'avérer plus efficaces pour éviter les accidents de demain que les méthodes rétrospectives.

Penser sécurité dans un système en mutation rapide : l'exemple de la médecine.
La médecine est entrée en rapide mutation avec une crise majeure inscrite dans la durée, s'étalant au moins sur les 10 ans qui viennent (horizon 2020, 2025). Cette situation s'applique à beaucoup de secteurs de l'industrie et des services : qu'il s'agisse de grands secteurs comme l'industrie nucléaire dans le post-Fukushima, la banque et la finance internationale en recherche d'un nouveau modèle, l'aéronautique en pleine recomposition mondiale, l'industrie pétrolière en butte à l'épuisement des ressources… ou de plus petits secteurs à haut danger comme la pêche professionnelle menacée tous les jours dans sa survie.
Quatre types de forces agissent simultanément sur tous ces secteurs :
– une arrivée d'innovations de rupture portant à la fois sur le fond et sur l'organisation : en médecine : chirurgie minimale invasive par les voies naturelles, génomique et médecine personnalisée, complétées par une série d'autres découvertes (chimiothérapie orale…) raccourcissant de façon spectaculaire la durée des séjours à l'hôpital, et imposant de ce fait un autre modèle d'hôpital à court terme (moins d'hôpitaux plus techniques, moins de lits, complété par un « hôpital à la maison »). L'équivalent dans l'industrie pourrait être la mutation de l'industrie pétrolière classique de forage vers l'exploitation intensive des schistes bitumineux… ;
– une transformation sociologique de l'offre et des professions : réduction drastique du nombre de chirurgiens au profit de professions interventionnelles utilisant des techniques légères de chirurgie (cardiologues, radio-imageurs, gastroentérologues, ophtalmologistes) avec pour conséquence la remise en cause de la position historique des blocs opératoires, et la sortie possible de l'hôpital vers les cabinets de ville d'une partie de ces interventions. On assiste aussi à une féminisation massive des acteurs de santé et des médecins du secteur des soins primaires, avec plus de regroupement dans des maisons de santé placées dans les petites villes, un travail à temps partiel de chacun, et en conséquence la constitution de déserts médicaux dans le milieu rural, aboutissant à l'institution de télémédecine et de délégations de tâches du médecin vers les soignants locaux, et des soignants vers les patients et leur entourage à la maison. Dans l'industrie, des équivalents seraient par exemple représentés par l'arrivée croissante des métiers liés aux énergies nouvelles, qu'il s'agisse de solaire, d'éolien ou de piles à combustible pour les transports du futur (quel sera notre besoin résiduel en ingénieurs en motorisation thermique classique à l'horizon 2025 ?) ;

– une demande de sécurité sans limite avec une formidable pression à la transparence et à la supervision externe ;
– et évidemment une crise financière sans précédent confrontant plus que jamais le modèle de sécurité au modèle économique.

Et la culture de sécurité dans tout ça ?

> Le lecteur d'un ouvrage sur la gouvernance du risque et de la sécurité s'attend à ce que cet ouvrage parle de culture de sécurité, et même que ce sujet soit assez central. Vous aurez remarqué que ce n'est pas le cas. L'idée n'est pas de nier ni de rejeter l'intérêt du concept, mais de le repositionner à sa juste valeur dans l'échelle de sa contribution à la sécurité. Et quand on fait ce travail, on observe d'abord une variation très grande sur l'usage et le contenu du concept de culture de sécurité dans la littérature, et on est assez tenté de conclure que la culture est effectivement profondément liée au modèle de sécurité, mais rarement un concept sur lequel on peut agir en premier et directement pour améliorer cette sécurité. L'unité de temps de changement est longue, très longue, et le processus d'amélioration de la culture demande une vraie persévérance pour lire les bénéfices.

Le thème de la culture et des climats de sécurité est un des plus populaires sujets de publication dans les journaux scientifiques spécialisés dans les risques industriels (et les risques des Services publics, transports, médecine). La plupart des articles et des livres proposent des outils d'évaluation de la culture, notamment des questionnaires.
Mais qu'apprend-on réellement de ces concepts pour améliorer la sécurité d'un système ? La question mérite d'être posée car la réponse est plutôt hésitante.

Cultures et climats (de changement, d'efficience, de sécurité), une multitude d'ambiguïtés et de confusions

Sept caractéristiques dominent la littérature sur les cultures ; ce sont presque autant d'interrogations de fond sur l'intérêt du concept pour faire évoluer la sécurité.

1. Les cultures renvoient à des valeurs (idées importantes) **et des normes** (attentes de comportements) (i) **morales,** partagées par tous les individus d'une communauté donnée (codes sociaux, rapports hommes-femmes, rapports à la vérité), (ii) **éthiques** (conditions inacceptables du succès ou de l'échec dans cette communauté), **et** (iii) **sociales** (définition de la réussite, distances hiérarchiques, rapport à l'incertitude, rôles et expertise).

2. La notion de culture s'est d'abord appliquée à caractériser des communautés nationales ou d'entreprises bien avant d'être déclinée sur le registre spécifique de la culture de sécurité. Dans le cadre des cultures nationales, le travail du psychosociologue Geert Hofstede[71] fait souvent référence. Il distingue cinq dimensions dont la combinatoire permet de classer les cultures nationales les unes par rapport aux autres (sans jugement de valeur). Les cinq dimensions sont (a) le degré de distance hiérarchique, (b) le besoin de réduction de l'incertitude, *degré de tolérance qu'une culture peut accepter face à l'inquiétude provoquée par les événements futurs* (c) l'individualisme versus le collectivisme, (d) la dimension masculine macho versus féminine, et (e) l'orientation à court ou à long terme ; liens aux *traditions si l'orientation est à court terme, valeurs d'économie et persévérance si l'orientation est à long terme.* D'autres contributions importantes ont été proposées pour caractériser les cultures d'entreprises (ou cultures d'organisation, *corporate culture*), particulièrement la contribution de O'Reilly, Chatman et Caldwell[72] qui distinguent sept dimensions : innovation, stabilité, respect des personnes, orientation vers le résultat, attention aux détails, solidarité du groupe, compétitivité et volonté de gagner (*aggressiveness*). Enfin, il apparaît difficile de ne pas citer la contribution majeure du sociologue Edgar Schein[73] qui distingue trois niveaux dans une culture d'entreprise : un niveau visible (*artifacts*) qui montre les comportements et les rituels observables (c'est typiquement le niveau que reflète la notion de climat d'une entreprise), un niveau des valeurs conscientes (*values*) qui portent les croyances partagées sur l'entreprise, ses points forts, ses points faibles, ses ennemis, ses amis, et enfin un troisième niveau (*organization's tacit assumptions*) fait de valeurs tacites, inconscientes ou tabous que les acteurs partagent sans pouvoir les évoquer (*unspoken rules*), par exemple, « *on pratique dans cet hôpital l'euthanasie des patients en fin de vie pour réguler la charge de travail du personnel* ».

Au départ, aucune de ces approches ne visait explicitement un classement de valeur des nations ou des entreprises, mais toutes ont été rapidement réutilisées par d'autres auteurs pour qualifier les « bonnes cultures » et les « mauvaises ». C'est à partir de ce moment que les difficultés de tous ordres ont commencé.

Évidemment, le premier problème quand on veut classer une culture par rapport à une autre est de préciser le résultat souhaité : on peut en effet classer les nations ou entreprises selon leur performance commerciale, leur capacité de changement, leur sécurité, et sur bien d'autres critères encore. Sans surprise, les classements relatifs aux traits d'une « bonne culture » vont ainsi différer selon le critère retenu. Pire, une bonne culture dans un registre particulier (la capacité de changement, ou l'efficience) peut s'avérer être une culture peu performante dans un autre registre (la sécurité par exemple). On a donc un premier niveau de difficulté : une culture n'est jamais bonne pour tous les bénéfices que l'on pourrait escompter sur toutes les dimensions. Choisir de parler de « bonne

71. Hofstede G (1983) Culture's consequences: international differences in work-related values. Administrative Science Quarterly (Johnson Graduate School of Management, Cornell University) 28: 625-29.

72. O'Reilly C, Chatman A, Caldwell D (1991) People and organizational culture: a profile comparisons approach to assessing person-organization fit. Academy of Management Journal 34: 487-516.

73. Schein, Organizational culture and leadership, John Wiley & sons, 1985, Ed 2010.

culture » de sécurité peut donc conduire des entreprises à adopter des traits culturels contraires voire handicapants pour d'autres aspects clés des défis qu'elles doivent relever pour survivre.

3. La notion de culture de sécurité n'est pas homogène dans ses « gènes ». Sous le même vocable, le terme renvoie à des approches théoriques très différentes.

- Helmreich[74], Flin[75], Guldenmund[76] et bien d'autres auteurs (les plus nombreux en rapport aux autres approches listées après) ont abordé le sujet de la culture de sécurité par le prisme des théories psychosociologiques sur les petits groupes et sur le rôle des leaders et managers de proximité, en privilégiant le regard des opérateurs de base sur leur environnement de travail. De nombreux questionnaires ont été développés sur cette base, tant sur la mesure de la culture que sur celle du climat de sécurité. Ce sont sans aucun doute ces questionnaires, facilement disponibles, qui ont rendu ces approches particulièrement populaires dans le monde de l'industrie dans le cadre de « diagnostics de culture de sécurité et diagnostics facteurs humains et organisationnels[77] ». Les points identifiés en relation avec une bonne culture de sécurité par ces « diagnostics par questionnaires » sont : un style de leadership démocratique, le respect des rôles de chacun (de la hiérarchie) et des procédures, l'absence de culture de censure, une capacité à signaler ses erreurs/événements/incidents sans être puni, le sentiment d'écoute de la hiérarchie, un bon niveau de solidarité et d'entraide dans le groupe, un faible nombre d'accidents du travail…
- D'autres auteurs ont concentré les définitions d'une bonne culture de sécurité sur les suites données par le management (*middle* et *top management*) au traitement des incidents et des accidents (Westrum[78], Reason[79]) en insistant sur le besoin d'une analyse approfondie ; certains ont même encore plus insisté sur le régime de sanction à associer à ces mêmes évènements indésirables, pointant le besoin impératif de préserver une capacité au système d'échapper à la justice quand on parle d'erreurs humaines – forcément involontaires – (concept de *just culture*[80, 81]).
- C'est un cadre théorique très élargi des théories organisationnelles qui a inspiré les approches sur les cultures de gouvernance et la macro-organisation du système, finalement assez loin des perspectives centrées sur les petits groupes et les

74. Helmreich RL, Merritt AC (1998) Culture at work: national, organizational, and professional influences. Aldershot, United Kingdom: Ashgate.

75. Flin R, O'Connor P, Crichton M (2008) Safety at the sharp end: a guide to non-technical skills. Aldershot, UK: Ashgate.

76. Guldenmund F (2007) The use of questionnaires in safety culture research – an evaluation. Safety Science 45: 723-43.

77. Daniellou F, Simart M, Boissière I. Human and organizational factors of safety :state of the art, ICSI, http://www.foncsi.org/media/PDF/CSI-HOFS.pdf.

78. Westrum R (2004) A typology of organisational cultures. Qual Saf Health Care 13: 22-7.

79. Reason JT, Carthey J, de Leval MR (2001) Diagnosing vulnerable system syndrome: an essential prerequisite to effective risk management Qual Health Care 10 (suppl 2): i21-5.

80. Marx D (2001) Patient safety and the just culture, a primer for health care executives. MERS-TM: Columbia University New York.

81. Dekker S (2008) Just culture, balancing safety and accountability. Aldershot, UK: Ashgate.

opérateurs. Ces travaux ont irrigué les connaissances sur les cultures d'entreprise, en reliant par exemple le niveau de qualité de production, la capacité innovante (climat de créativité[82]) et différentes familles de cultures : cultures de clan, cultures de changement, cultures pariant sur la hiérarchie, et cultures rationnelles[83] et en évaluant les spécificités et les marges de progrès de chaque type de culture.

- Toujours dans le cadre des théories organisationnelles centrées sur le risque, on citera bien sûr l'approche des HRO (*High Reliability Organizations*), qui se singularise en qualifiant une bonne culture de sécurité avant tout comme la capacité d'adaptation du groupe à des situations non standard, en soulignant l'importance du leadership, de l'expertise et du rôle de chacun, et surtout de la résilience, voire de l'improvisation, deux idées fort peu présentes (voire contradictoires) dans tous les courants précédents. Le diagnostic de culture HRO procède beaucoup moins par questionnaire, et beaucoup plus par audit des organisations.
- D'autres enfin ont massivement (exclusivement ?) assimilé culture de sécurité à culture de qualité dans une perspective de meilleures production et performance du système ; on pense au Toyotisme[84] et au *Lean management*. Encore une fois, on se trouve assez loin des théories précédentes avec une culture donnant la priorité aux organisations centrées sur le flux, un rôle clé au management de proximité pour réduire les erreurs génératrices de baisse de performance, et gérer en premier la qualité dans la ligne production en ne regardant par contre que très marginalement la question des accidents graves.

Cette liste est loin de refléter toutes les contributions et courants théoriques existants sur le domaine de la culture de sécurité : théories différentes, messages différents, focus différents. La plupart du temps, les lecteurs et utilisateurs occasionnels ne peuvent pas connaître toute cette déclinaison et se trouvent prisonniers d'un point de vue, d'une logique, sans comprendre les contradictions qui pourraient exister à mélanger dans leur propre société une approche centrée par exemple sur la ligne de production autour d'une culture de type Toyotisme ou *Lean management*, et en même temps dire que leur objectif est d'être une organisation HRO, et toujours en même temps, de dire dans d'autres cénacles que l'objectif prioritaire de l'entreprise est de faire évoluer la culture et d'adopter un climat propice au changement pour supporter les virages à venir imposés par de nouvelles conditions socioéconomiques.

Bref, le mot « changer de culture de sécurité » peut facilement cacher de sévères ambiguïtés et de fortes déceptions s'il est vraiment décliné sans précaution jusqu'aux opérateurs. Heureusement… ou malheureusement, l'emploi du mot se trouve souvent limité à un discours de bienséance pour l'extérieur, mais sans grande conséquence sur l'intérieur, et souvent sans utilité réelle. Ceci dit, toute entreprise a une culture, et il est

82. Ekvall G (1991) The organizational culture of idea-management : a creative climate for the management of ideas. In: Managing Innovation, sous la dir. de Henry J and Walker D, London: Sage, p. 73-9.

83. Un bon résumé de toute cette approche dans Braithwaite JJ, Hyde P, Pope C (2010) Culture and climate in health care organizations. Palgrave MacMillan.

84. Liker J (2003). The Toyota Way: 14 management principles from the world's greatest manufacturer, First edition. McGraw-Hill.

peut-être plus important pour l'intervention de sécurité de connaître cette culture dans toutes ses contradictions.

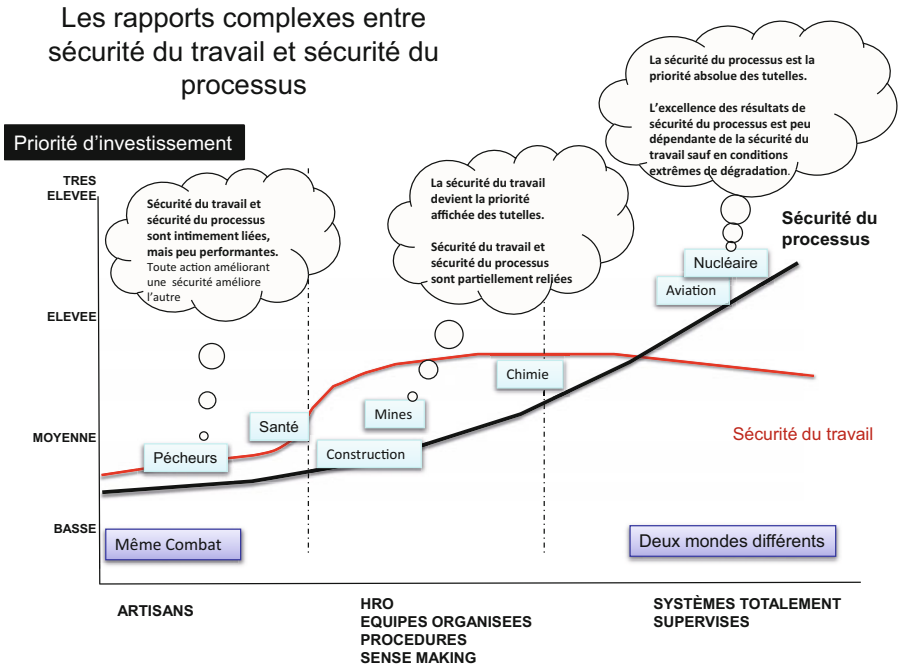
Cultures et taux d'accidents en aviation civile. *Helmreich a montré, en reprenant les travaux d'Hofstede au début des années 2000, que les équipages des pays fortement collectivistes et présentant une forte distance hiérarchique (Amérique centrale, Asie centrale) avaient un taux d'accidents d'avions de ligne deux fois et demi supérieur au taux des pays occidentaux caractérisés par des cultures plus individualistes et sans distance hiérarchique. Dans un premier temps, l'interprétation est allée naturellement vers l'idée d'un classement de valeur des cultures et vers l'idée qu'il fallait faire adopter par tous les traits des cultures occidentales associés aux meilleurs résultats de sécurité. Pourtant très rapidement, cette hypothèse n'a plus été aussi explicite. La raison éthique était importante (ne pas choquer ces pays, ni leurs valeurs nationales), mais la vraie raison était encore plus triviale : l'étude ne faisait que révéler une évidence : la conception d'un système complexe (comme un avion) est profondément culturellement marquée ; il est bien plus facile aux usagers partageant cette culture de se servir du produit correctement : les avions modernes automatisés exigent une collaboration très directe entre membres d'équipage et une capacité d'étonnement et de remise en cause mutuelle et constante des subordonnés sur les gestes et décisions de leur chef ; les pays qui ont des rapports hiérarchiques plus distants ont forcément du mal à fonctionner dans ce moule. En quelque sorte, il n'y a pas de « bonne culture » mais il y a des mauvais « mariages ».*

4. Un lien mal compris entre deux productions de la culture de sécurité : la sécurité des travailleurs et la sécurité du site et du produit. Assez curieusement, la littérature a développé deux cadres parallèles d'application aux diagnostics de culture de sécurité dans les entreprises : la sécurité au travail, et la sécurité du site et du produit. On peut aujourd'hui dresser un constat en trois points sur cette ambiguïté :

– les priorités respectives données à ces deux domaines dépendent de la maturité et des priorités publiques de tutelles dans les différentes familles d'industries et de Services publics. Les deux courbes de priorité se croisent. Pour les activités les plus immatures et les moins sûres (métiers artisanaux, médecine), la priorité publique va plutôt à la sécurité de la production (sécurité du patient par exemple) ; dans les industries à fort niveau de main-d'œuvre, un peu plus matures que les artisans et dotées de tutelles puissantes, la priorité va plutôt à la sécurité du travail (baisser le taux d'accidents du travail). Mais paradoxalement, pour les industries les plus sûres (en termes d'accidents industriels), la priorité rebascule sur la sécurité du processus ; ces industries plus sûres (en matière de risque d'accident) montrent souvent des performances à peine moyennes en matière de sécurité du travail (et en tout cas inférieures aux industries du groupe précédent) ;

85. Helmreich R (1993) Attitudes towards automation across five cultures – NASA report/University of Texas/FAA - Aerospace Crew Research.

– en dehors d'idées générales, on ne sait pas très bien quels sont les liens théoriques entretenus entre ces deux espaces de sécurité. Le lien est à l'évidence un cas complexe, puisque l'excellence dans un de ces deux domaines est rarement associée à l'excellence dans l'autre ;
– l'ambiguïté se poursuit dans l'emploi de bien des outils de mesure des cultures et des climats de sécurité, particulièrement les questionnaires, souvent validés pour un seul de ces deux domaines, mais employés sans précaution pour mesurer l'autre domaine.



5. On peut changer rapidement un climat de sécurité, mais on ne sait pas changer rapidement une culture de sécurité. La notion de climat de sécurité, inspiré du premier niveau de Schein (*opus cité*) porte sur les éléments objectifs (sur des faits), alors que la notion de culture de sécurité porte sur des éléments subjectifs (des valeurs). On sait éventuellement faire changer assez vite les éléments du climat de sécurité par des actions dédiées sur le management, l'organisation, mais on ne sait pas faire changer aussi vite par action directe les valeurs qui caractérisent une culture. Ceci dit, on peut infléchir significativement la culture en changeant autoritairement les fondamentaux du système technique et en introduisant des modifications majeures dans l'économie du système, mais évidemment cela dépasse les capacités d'une intervention ponctuelle dans une entreprise d'un secteur industriel ou de service (type hôpital ou banque). En bref, l'économie de marché dicte la culture plutôt que l'inverse. Les leviers du changement sont systémiques et non pas locaux.

Le changement de culture en aviation civile : un levier systémique bien avant le levier facteurs humains. L'aviation de ligne a longtemps été la terre des héros, avec des commandants de bord maîtres après Dieu, décidant à leur guise de leur route et des dérogations jugées pertinentes aux procédures. L'installation du contrôle aérien après la Seconde Guerre mondiale a représenté une première limite à cette autonomie, mais c'est surtout l'immense standardisation mondiale de la supervision du système de vol, l'arrivée des avions automatisés gommant les différences de doigté entre pilotes, et l'enregistrement de tous les actes de l'équipage dans le cockpit (analyse systématique des vols) qui ont définitivement fait basculer dans les années 1980 la culture de l'aviation civile vers le modèle ultrasûr. La mise en place des formations au travail en équipage dans les années 1990, et les initiatives très médiatisées sur le signalement volontaire sans blâme sont venues après, et ont plus été des accompagnements au changement que la vraie raison du changement de culture (aujourd'hui marquée par des acteurs équivalents, avec une grande transparence des incidents et un travail des équipages centré sur la coordination et le suivi des procédures).

6. Il n'y a pas une culture idéale, il y a des cultures adaptées à chaque cas. Cette vision s'est progressivement imposée comme la seule résistant aux faits. Toute normativité en la matière s'avère contreproductive. On a vu dans les paragraphes précédents qu'il existe plusieurs modèles de sécurité et non un seul. Assez logiquement, ces différents modèles de sécurité, qui reflètent des arbitrages différents entre flexibilité, compétitivité, adaptabilité et performance de sécurité, renvoient à des réglages différents de la culture de sécurité.

7. L'évolution des valeurs qui caractérisent une culture demande du temps, beaucoup de temps. Certains parlent de levier générationnel. Aucun outil classique de matrice de risque et de plan d'action de sécurité ne porte sur des horizons temporels aussi longs.

Au bilan, mesurer la culture de sécurité d'une unité de production est utile et fait intégralement partie d'une démarche de diagnostic. Elle nécessite une connaissance assez approfondie des théories qui sont derrière les outils de mesure pour ne pas faire de contresens. Elle ne saurait par contre suffire en elle-même. Son interprétation est toujours relative car elle dépend des enjeux locaux (qu'il faut avoir bien analysés et bien compris). Finalement, cette mesure permet surtout de situer la marge de progrès de l'entreprise en matière de sécurité.

> Si l'on doit procéder à une intervention de sécurité locale et limitée dans le temps dans une entreprise, plutôt que de croire que l'on va changer sa culture, on doit inverser le raisonnement et déduire (de la mesure de sa culture) la marge de progrès réellement réalisable par cette entreprise compte tenu de sa culture.

Ce diagnostic vient conforter l'identification du modèle de sécurité qui caractérise le mieux le milieu (et les besoins) de l'entreprise que l'on audite. En bref, on ne change

pas une culture d'entreprise par une intervention ponctuelle motivée par une demande de sécurité. Aucune action n'a ce pouvoir. Mais on peut comprendre et identifier la culture en place pour évaluer quelles marges de progrès dans les résultats autorisera cette culture (approche réverse).
Si l'ambition est plus grande et prétend vouloir changer la culture d'une profession, il faut disposer de leviers systémiques, changer la demande du *business model* à l'échelon de la profession, agir au moins au niveau régional, sinon national ou international, et persister sur le long terme (intervention longue impérative avec des dispositifs réglementaires à la clé).

Dans la mesure où la culture de sécurité est plutôt une conséquence de l'économie de la profession et de son modèle de sécurité qu'une cause de ce modèle, il est légitime que ce paragraphe vienne plutôt en dernier qu'en premier dans ce texte.

4

Facteurs humains et organisationnels (FHO) : une évolution considérable des enjeux

Bien que ce livre se concentre sur la sécurité des systèmes complexes, il m'est apparu utile de le terminer par une présentation des grandes fractures historiques et la succession des principes guidant les démarches FHO dans les entreprises (facteurs humains et organisationnels).

Ma perception de l'histoire de l'industrialisation me conduit à différencier cinq étapes successives et importantes dans la prise en compte des facteurs humains et organisationnels (FHO). Cette connaissance enrichit et module nécessairement la stratégie de prise en charge systémique de la sécurité.

L'ouvrier productif

La première étape est datée de la fin du XIX^e^/début du XX^e^ siècle et de la montée en puissance de d'industrialisation intensive. Elle combine trois concepts fondamentaux visant à « **disposer d'ouvriers plus productifs** ».
C'est d'abord **le Taylorisme**[1] qui prône une productivité accrue en prenant mieux en compte les caractéristiques humaines (essentiellement physiques) et les exigences du travail à réaliser. Cette double connaissance permet d'établir un compromis optimal de productivité pour chaque situation de travail (essentiellement des travaux répétitifs et physiques), maximisant l'efficience, sans entamer ni dégrader inutilement la capacité des ouvriers sur la durée. L'idée d'une ***organisation scientifique du travail***, analysable,

1. Taylor F. The principles of scientific management. Harper & Row, 1911, Reprint Norton Library, 1967.

enseignable et généralisable, constitue indiscutablement la première cible historique des FHO[2].
Ce Taylorisme s'est adapté mais il n'a pas disparu, surtout dans les activités manuelles (il s'applique forcément moins bien aux activités intellectuelles). Un poste sur cinq d'ouvriers reste Taylorisé sous une forme moderne. Le Toyotisme[3] émergeant de la fin des années 1970 n'est qu'une relecture moderne des concepts de Taylor. Le contrôle qualité a été placé au centre du dispositif, le personnel mieux intégré, le travail posté par équipe tournante s'est généralisé, les tâches ont été enrichies (elles sont par exemple moins monotones sur les chaînes de fabrication, avec des véhicules qui se suivent tout en exigeant du même poste de montage des actions différentes pour des finitions différentes), la chaîne préserve aussi un peu plus de temps aux ajustements personnels (temps de rattrapage…) tout en restant cadrée par les enveloppes du temps collectif. Mais dans le fond, ce sont toujours les idées de rationalisation du temps des gestes à faire qui restent centrales. La remontée brutale du taux de TMS (troubles musculosquelettiques ou *Repetitive Strain Injury*) dans la fin des années 1990[4] nous montre à quel point certains principes de base du Taylorisme ont déjà été oubliés, alors qu'ils auraient dû rester partie intégrante de nos savoirs académiques. Bien sûr l'intense polémique humaniste des années 1980 a fait beaucoup pour condamner Taylor, sans doute excessivement, mais c'est bien la très grande difficulté technique et méthodologique de portage du Taylorisme vers les tâches complexes et intellectuelles de notre société moderne qui a tué définitivement cet enseignement dans les universités, et particulièrement dans les cursus en ergonomie des universités.

Le deuxième pas de cette période initiale est assurément **la prise en compte du contexte et de la motivation**, et plus particulièrement du contexte psychologique de travail. Les travaux de Elton Mayo[5,6] étalés de 1927 à 1932 à l'usine Hawthorne constituent le fondement de cette approche. Mayo intervient une première fois dans un atelier de montage de la *Western Electric Company* (assemblage de matériel pour les radios) dont les lignes de production sont féminisées, et démontre la pertinence d'une approche des conditions de travail dans la productivité. Il crée un atelier expérimental avec une meilleure lumière et des meilleures conditions de travail. La production augmente. Mayo va revenir dans cette usine quelques mois après, sur le même atelier, et tester une idée assez géniale : il supprime dans l'atelier expérimental les améliorations des

2. Le Fordisme n'était pas très loin à la même époque du Taylorisme, avec une standardisation poussée à l'extrême sur les chaînes de Ford, compensée par un salaire supérieur versé aux ouvriers (« five dollars day »).

3. Préconisé par l'ingénieur Ohno sur les chaînes de Toyota, le Toyotisme vise l'objectif des 5 zéros : zéro stock, zéro défaut, zéro papier, zéro panne, zéro délai.

4. Pascarelli E, Quilter D (1994) Repetitive strain injury. John Wiley and sons.

5. Mayo E. The human problems of an industrial civilization. Contributors: first published 1933, reprint in Thompson K. The early sociology of management and organizations – Routlege London. Publication Year: 2003.

6. Gillespie R (1991) Manufacturing knowledge: a history of the Hawthorne Experiments. Cambridge: Cambridge University Press, and Sonnenfeld JA (1985) Shedding Light on the Hawthorne Studies. Journal of Occupational Behavior 6.

conditions de travail réalisées précédemment. La production augmente encore plus. La preuve est faite que la production est très largement guidée par l'intérêt porté aux travailleurs, qui se transforme en motivation supplémentaire. Cette ligne de travail va inspirer la sociologie du travail et créer de nombreuses ramifications et développements qui sont toujours d'actualité.

Le troisième pas de cette première période reste le **temps de la sélection**. Très tôt la sélection par les diplômes ou par les tests psychologiques recherchant des habiletés particulières est apparue une troisième voie prometteuse et naturellement complémentaire à la formation et l'organisation pour réduire la variabilité naturelle des sujets et pour permettre une meilleure adaptation au travail, y compris dans les réponses aux conditions dégradées. La création par G. Stanley Hall, John Wallace Baird, et Ludwig Reinhold Geissler du *Journal of Applied Psychology* en 1916, presque entièrement dévolu à ce sujet de la sélection, reste un marqueur historique de cette montée en puissance de la sélection.
Jusqu'aux années 1960, ces fondamentaux des approches des facteurs humains et organisationnels vont peu changer. Les connaissances ergonomiques et sur les conditions de travail vont s'accumuler sans révolution.

Pour résumer cette première période.
- L'accent est mis sur la productivité des opérateurs.
- Le savoir-faire principal FHO à cette phase est dans la conception de la situation de travail pour une meilleure productivité : analyse de la demande, de la connaissance des capacités des opérateurs et de leur sélection, et des solutions d'améliorations de conditions de travail.
- La sécurité est seulement prise en compte comme une variable d'accompagnement de la productivité (un travailleur bien sélectionné, bien formé et bien motivé a moins de problèmes de santé, produit plus et cause moins d'accidents).
- L'application scientifique des concepts (d'analyse, de contexte, et de sélection) est d'abord motivée pour des améliorations rapides et certaines de la productivité.
- Le management n'est pas une cible de cette première période.

L'usine sûre

La deuxième étape accompagne la **montée en puissance des industries à risques** à la fin des années 1960**.**
Cette étape va être très productive jusqu'au début des années 1990, et dominée par la volonté de **contrôler un risque** qu'on sait croissant dans les installations industrielles (essentiellement chimiques et nucléaires).
L'accident de l'usine de Seveso en Italie en 1976 dû à une surchauffe d'un réacteur chimique causant un épandage de dioxine va fortement accélérer le besoin d'établir

une science de la fiabilité et de la sécurité (*Reliability engineering and system safety*[7,8]). La survenue de l'accident nucléaire de Three-Miles Island en 1979 finit de convaincre la communauté sur la priorité de cette approche et met un accent particulier sur la composante humaine de la fiabilité, sans que les principes généraux de l'approche ne changent.

L'idée fondatrice de ces approches **calculatoires du risque** est que le risque est le produit de la fréquence (des événements) par la gravité des conséquences. Cette équation de base reste le fondement des méthodes d'évaluation du risque (*System-Risk Assessment*, SRA), et par extension des méthodes d'évaluation de la fiabilité humaine (*Human-Risk Assessment*, HRA[9]).

De nombreux outils de mesure et de décision (quoi prioriser dans un plan d'action sécurité) vont être développés dans les années 1980 ; certaines déclinaisons vont être nettement plus prospectives pour la phase de conception (HAZOP par exemple), d'autres vont ajouter des dimensions au processus calculatoire de base (l'AMDEC considère le risque comme le produit de la fréquence, la gravité, et la détectabilité).

Le retour d'expérience va apparaître comme essentiel pour nourrir ces modèles calculatoires.

Pour résumer cette phase.

- Le contexte a basculé dans des industries à risques ; le procédé utilisé dans l'usine peut créer du dommage collatéral bien au-delà du poste de travail de proximité.
- La sécurité est devenue le premier centre d'intérêt de la démarche FHO. L'analyse des erreurs prend le pas sur toutes les analyses de conditions de travail.
- Le regard est toujours centré sur l'outil de production interne.
- La priorité de l'analyse est centrée sur le procédé, ses défaillances, et les procédures de contrôle : on cherche des solutions sûres aux dysfonctionnements imaginés ou déjà vus, qu'ils soient d'origine technique (pas de procédure, ou procédure incorrecte) ou humaine (erreur), mais l'analyse reste technocentrée.
- L'analyse est calculatoire et se nourrit du retour d'expérience.
- Le risque est tel que la sécurité n'est plus une variable concurrentielle entre exploitants. Tous doivent arriver à l'excellence. Le rôle des tutelles et des règlements devient majeur, et s'applique à tous.
- Mais cette phase est encore ouvertement positive et pleine d'espoir : on croit à l'excellence de sécurité : on peut faire mieux, on peut imaginer de meilleurs procédés, de meilleurs outils. L'application des concepts de fiabilité conduira de façon certaine à la résolution des problèmes identifiés. Le chemin est long, mais il sera parcouru, et les accidents disparaîtront.

7. Lewis E (1987) Introduction to reliability engineering. John Wyley and sons
8. Frankel E (1988) System reliability and risk analysis. Kluwer
9. Bell J, Holroyd J (2009) Review of human reliability assessment methods, report HSE, http://www.hse.gov.uk/research/rrpdf/rr679.pdf

Le produit sûr, les enjeux de sécurité portés par la conception et l'usage

La troisième étape accompagne la montée en puissance **des transports publics** à la fin des années 1980 et pendant les années 1990 : avions automatisés, TGV, métros guidés…

Pour la première fois, l'analyse prioritaire porte sur les qualités du produit commercial (la sécurité du train, de l'avion) plus que sur le site de conception et de production. Le regard est décentré sur la conception et l'usage. Les problèmes de sécurité de l'usine deviennent secondaires ; les problèmes d'usage et de qualité du produit deviennent la priorité.

Cette décentration est à la fois le produit et la conséquence de deux révolutions :

- une révolution technique avec l'introduction massive de l'informatique et de l'électronique permettant de reconcevoir la conception et l'usage dans un environnement modélisé et supervisé[10]. Il en résulte un changement radical des interfaces, des précisions extrêmes dans la performance de guidage et de flux (séparations verticales et horizontales des avions) et une place à redéfinir pour les opérateurs. Une nouvelle discipline scientifique naît avec le *Cognitive Engineering*[11]. L'électronique a aussi introduit la possibilité d'un cocon infranchissable et protecteur des erreurs de l'opérateur. Au-delà des apports dans le poste de pilotage, la notion d'exploitation en réseau et de sécurité du réseau, inexistante dans la phase précédente, devient une préoccupation centrale ;
- une révolution dans la distribution des rôles et responsabilités. La conception du produit influence les clients bien au-delà de l'outil, ils imposent des règles d'usage avec de plus en plus d'impact sur l'organisation de leur société. Par exemple, l'automatisation des avions et du contrôle a changé profondément les règles professionnelles et les règles de gestion des compagnies (changement de carrières, de formation, de profil de recrutement). Plus le système devient complexe, plus les constructeurs finissent par créer le système d'exploitation tout entier, ses standards, ses règles d'emploi et d'usage, et joue de toute leur influence sur les règlements, au lieu de simplement vendre un outil pour des exploitants. On a vu au chapitre 3 que le constructeur finit par exporter toute sa culture y compris sa vision de la sécurité, du collectif et de l'organisation de l'exploitation par la chaîne hiérarchique. Il faut dire que les exploitants n'ont pas vraiment beaucoup de choix : les offres sont alignées entre très peu de constructeurs mondiaux, et les vrais acheteurs sont des banques qui se décident sur des critères macroéconomiques et relouent les produits aux exploitants.

Mais bien sûr, *in fine*, le concepteur n'est pas l'utilisateur. Un copartage de la gestion du risque s'installe. La dissémination mondiale des produits se heurte à des cultures

10. Boy GA (2011) Handbook of human-machine interaction - A human-centered design approach. Ashgate, UK.

11. Sarter, N., Amalberti, R. (Ed.). Cognitive engineering in the aviation domain. Hillsdale-New Jersey: Lawrence Erlbaum Associates, 2000.

différentes qui vont alimenter longtemps les débats FHO : quelle tolérance sur les écarts d'usage des produits donnés par un constructeur, quel degré d'appropriation et de particularisation du produit conçu par le bureau d'étude doit être laissé à l'exploitant…
L'introduction du CRM en aéronautique (*Crew-Resource Management*[12]) pour accompagner, former et sécuriser le travail en équipe et du modèle des plaques (fromage Suisse) de Reason (*op cité*) pour couvrir le besoin naissant de sécurité systémique symbolise les deux contributions les plus marquantes de cette phase pour les FHO.

Pour résumer cette phase.

- La sécurité du produit livré et son usage prennent le pas sur les procédés de production à l'intérieur de l'usine.
- Sur un plan technique, la révolution informatique permet automatisation et supervision centralisée d'un réseau.
- La sécurité repose sur la conception, l'exploitation et l'usage. L'usage ouvre de nouveaux champs de développement, notamment sur l'organisation sûre des collectifs (formations des équipes, équipages) et des organisations techniques (options d'organisations sous-optimales et erreurs latentes de la chaîne de commande de l'exploitation). L'analyse reste quand même centrée sur les acteurs de premières lignes et le management de proximité. Les FHO n'ont pas encore accès aux dirigeants, mais accèdent aux *middle managers*.
- Le savoir-faire FHO progresse particulièrement à cette phase ; on lui doit les contributions sur le travail collectif, la fiabilité du collectif, la culture de sécurité, la fiabilité de la chaîne hiérarchique. La conception crée l'usage et modèle le client, y compris économiquement, mais les FHO restent assez extérieurs à cette dimension économique très importante laissée à l'appréciation des grands cabinets d'audits.
- Bien sûr, les acquis de la phase précédente (montée en puissance des tutelles, études de fiabilité) restent d'actualité.

La fin du rêve, l'impossible sécurité

La quatrième étape correspond à l'effondrement d'un mythe auquel tout le monde voulait croire : on pensait jusque-là que la science appliquée aux interventions de sécurité pourrait contrôler le risque et répondre à la demande et aux inquiétudes de la société.
La déception s'installe dans la deuxième partie des années 1990. L'industrie commence à percevoir toute l'ironie d'un effort considérable consacré à la sécurité. On ne peut jamais échapper à la pression et aux investissements croissants en matière de sécurité. Le momentum de la demande sociale est infini, de plus en plus exigeant, au point qu'il n'y a pas à attendre de retour sur bénéfice des efforts consentis par l'entreprise en matière d'investissements de sécurité. C'est même l'inverse : plus elle s'améliore, plus

12. Kanki B, Helmreich R, Anca J (2010) Crew resource management. Academic Press, 2nd ed

il lui faut consacrer de l'investissement sur la sécurité au détriment d'autres investissements sur la production.
Les principaux traits de cette phase ont déjà été décrits dans les chapitres 1 et 2.
Pour la première fois aussi, le lien s'établit fortement entre des univers de sécurité jusque-là séparés : sécurité industrielle d'un côté, sûreté des installations (vulnérabilité au terrorisme notamment) et sécurité environnementale. Les grandes perturbations du climat et de la planète politique alimentent et majorent le risque pris dans l'implantation des usines, la conception et l'usage des systèmes complexes, surtout organisés en réseaux supervisés. La cartographie des risques devient transversale à tous ces thèmes.
Le terrorisme et les menaces (épidémies…) deviennent planétaires. La confiance dans un futur dessiné sous forme d'une progression linéaire et constante de sécurité s'évanouit.
Il n'y a pas de limite à la sécurité, et plus on sécurise, plus la demande est forte, et plus la sanction est lourde pour les accidents résiduels. **La sécurité n'est pas qu'une question scientifique ; elle apparaît surtout une affaire de perception sociale.**
En même temps, cette perte de confiance dans la science va ouvrir l'émergence du **principe de précaution**[13] et des approches de réparation des victimes sur des critères de moins en moins scientifiques.
On assiste à une mise à distance de la maladie et de la mort qui paradoxalement augmente les inquiétudes et les demandes. Toute atteinte prématurée (ou menace) provoque l'indignation sociale.
Cette prise de conscience va irriguer la médecine du travail moderne, ouvrir des horizons de réparation jusque-là inconnus, avec la prise en compte des nuisances chroniques (dossier de l'amiante) qui ont le potentiel de raccourcir l'espérance et la qualité de vie, domaines qui sont infiniment plus subjectifs et complexes à calculer que la blessure directe sur le poste de travail. La sécurité était un devoir pour l'industrie avec une exigence de moyens ; elle devient un droit pour le citoyen, avec une obligation de résultats, et se trouve exigible et monnayable quasiment sans limite haute de réparation financière.
Paradoxalement aussi, les derniers grands progrès de confort de la société et du travail (35 heures en France par exemple) font apparaître de nouvelles difficultés considérables d'adaptation des travailleurs, victimes du manque de temps, d'une intensification de leur activité et de la perte d'une certaine humanité des rapports sociaux. Les démarches FHO doivent gérer souffrance au travail et suicide chez ces professionnels pourtant infiniment mieux traités que leurs ancêtres, mais la souffrance ne contient pas l'histoire des autres ni la relativité des situations… elle n'est que personnelle et ancrée sur ses propres douleurs.
Le coût social de cette sécurité conduit à des crises sociétales en série : crise assurantielle, crise de compétitivité, crise de responsabilité, débats de fonds sur le maintien des industries à risque sur le sol des pays les plus sensibles. Elle favorise aussi massivement les transferts de responsabilité, notamment par une sous-traitance renforcée.

13. Le principe de précaution est formulé pour la première fois dans la déclaration de Rio en 1992, et s'applique au départ uniquement pour les risques environnementaux. Il va être rapidement étendu à tout le domaine des grands risques médicaux. Lire par exemple Gollier C, Treich N (2003) Decision making under uncertainty : the economics of the precautionary principle. Journal of risk and uncertainty 27 : 77-103, ou Guilhou X, Lagadec P (2002) La fin du risque zéro. Ed Organisations.

La transparence, concept fort de cette « impossible sécurité », s'avère un terrible outil à domestiquer.
Le système sociétal entre en irrationalité complète, au point de faire investir progressivement dans l'industrie plus de ressources sur un savoir-faire de gestion des crises et d'effets collatéraux économiques, que sur la prévention proprement dite des accidents et les dégâts directs qu'ils peuvent provoquer.

Pour résumer cette phase.

- L'amélioration de la sécurité produit toujours plus de demande de sécurité.
- Le « dernier accident » coûte infiniment plus cher en image et en réparation que les accidents du passé, quand ils étaient le fruit d'une industrie qui n'avait pas fait d'efforts substantiels.
- Malgré, ou peut-être à cause des progrès, les travailleurs sont plus en souffrance que dans les phases précédentes.
- On quitte brutalement l'idée qu'il pouvait exister une maîtrise et une réduction totale des risques, pour accepter l'idée d'un pilotage dynamique de risques, ou l'on doit échanger au mieux les risques sur différentes dimensions (accident, économie, production, ressources humaines, stratégie de concurrence) afin de survivre aux crises qui seront inéluctables (sur une dimension ou sur une autre).
- Cette phase impacte considérablement les FHO. Elle n'apporte pas de vrais nouveaux modèles de sécurité, sinon ceux de la gestion des crises, mais elle oblige à penser l'usage de tous les modèles disponibles d'une façon plus systémique, à transversaliser les approches, à regarder de plus haut les situations, à prendre en compte la gouvernance, et surtout à fournir un conseil qui n'est plus optimal sur une dimension, mais un conseil qui est optimal sur les équilibres, les compromis et les sacrifices les plus payants. Autrement dit, une approche FHO moderne ne répond pas exclusivement à la question qui lui est posée, particulièrement en matière de sécurité ; la démarche doit relever du ***management total***, et resituer – voire modérer – la réponse locale en tenant compte des effets collatéraux sur les autres dimensions contradictoires de l'activité de l'entreprise.

Par exemple, la sécurité du patient (erreurs médicales) n'est qu'un des grands risques que doit savoir gérer un établissement médical. On sait que toute action sur ce risque particulier agit sur les autres risques de l'établissement, souvent en les augmentant, ce qui explique en retour que les mesures préconisées soient finalement rarement suivies à fond par la gouvernance de la clinique [la gouvernance doit aussi gérer le risque économique (taux d'occupation, facturation, impayés…), le risque ressource (trouver des docteurs et personnels compétents pour rester ouvert 24 heures/24), le risque de non-conformité (feu, bâtiment, locaux…), le risque stratégique (taille critique, politique d'alliance, d'achat, d'actionnaires…]. Une bonne intervention FHO doit résoudre la question posée, tout en identifiant clairement les effets collatéraux sur les autres risques, de sorte à préparer une décision comprise et maîtrisée dans ses effets et ses coûts collatéraux par la gouvernance, sinon l'intervention est vouée à l'échec.

L'incertain comme futur risque : les risques futurs au centre du présent

Nous sommes entrés dans une **cinquième étape pour les FHO**.
Elle se caractérise par un regard tourné vers les risques futurs (« qui n'existent pas encore et que l'on veut éviter ») alors que toutes les phases précédentes étaient tournées vers un risque passé que l'on essayait de réduire.
Le grand débat sur les menaces écologiques illustre à merveille ce nouveau glissement. L'épuisement du pétrole, l'évolution des facteurs bioclimatiques et le réchauffement de la planète sont autant de thèmes pour lesquels le risque est immense (la fin annoncée de nos sociétés), mais où les hypothèses contradictoires et l'incertain dominent les acquis scientifiques.
Le nouveau regard de la médecine du travail sur les effets sur les générations absentes (futures) de l'exposition à des nuisances chroniques de la génération présente est une autre illustration de cette évolution. Les effets génétiques sur les futures générations sont particulièrement redoutés, avec l'exposition chronique à des substances chimiques. Mais là encore, la science est largement démunie. Le maniement du principe de précaution n'est pas si facile ; les atermoiements de l'initiative européenne REACH[14] sur l'étude systématique de la toxicité de toutes les nouvelles molécules soulignent bien cette difficulté.
Plus globalement, une société déjà largement sécurisée porte son regard et ses exigences sur un horizon temporel de plus en plus éloigné, et focalise ses efforts – par écho aux fondements biologiques individuels – pour survivre le plus longtemps possible et pas simplement résister à la contrainte de l'instant. On sait aussi que cette « fuite » de l'horizon sécurité est particulièrement fragile et serait rapidement réajustée en cas de menace à court terme.

Pour résumer cette cinquième phase.

- Le débat se déplace vers **faire survivre la société** sur le long terme et assurer sa sécurité future. La résilience de la société devient plus importante que la sécurité de l'individu.
- Le débat part de grandes peurs instrumentalisées, de questions quasi générales sur les conditions de survie de la société, et voudrait irriguer en retour des contraintes immédiates de fonctionnement, de production et de structuration de l'industrie.
- Le besoin est externe à l'industrie, virtuel, immense, infini, et surtout mal défini, mais la pression sociétale fait qu'on ne peut l'éviter.
- L'incertain fait plus peur que les risques importants connus. L'avenir détermine le présent.

14. REACH (Registration, Evaluation, Authorisation and restriction of CHemicals) est un règlement européen entré en vigueur le 1er juin 2007, destiné à encadrer l'enregistrement, l'évaluation et l'autorisation des substances chimiques, ainsi que les restrictions applicables à ces substances.

- Les méthodes concrètes de réponse manquent, et la culpabilité certaine puisque les efforts, encore moins que dans la phase précédente, ne seront jamais à la hauteur du péril.
- En quoi cette dernière évolution impacte-t-elle les FHO ? Dans l'immédiat, ces grandes peurs ne sont pas incarnées dans de nouvelles méthodes, mais l'existence des peurs influence les analyses et les réponses. Ce n'est plus tant l'arbitrage entre dimensions de risques qui compte dans cette nouvelle évolution (comme c'était le cas dans la phase d'avant), que l'arbitrage sur des dimensions d'incertitude et le changement que l'on doit porter dans le regard sur les systèmes de retour d'expérience. La mise en place et l'écoute des dispositifs des signaux à bas bruits (souvent rares et peu écoutés, voire écartés par les REX actuels), l'écoute dans la presse des souffleurs d'alertes (*whistle blowers*) et leur potentielle influence sur les futurs choix d'organisation du travail entrent totalement dans le champ des FHO modernes.

Conclusion

Ces cinq phases décrites sont comme cinq pierres laissées sur un chemin en construction.

Mais ce n'est pas la construction d'une théorie totale de la sécurité dont il s'agit, encore moins de la construction d'une théorie totale des FHO ; c'est la construction continue de la société, de ses perceptions collectives sur son niveau de sécurité, et de l'innovation technologique qui est au centre du processus, rendant obsolètes certaines pratiques, et obligeant mécaniquement des ajouts et des développements FHO pour répondre aux nouvelles situations et produits mis sur le marché.

Il nous appartient de capitaliser les savoirs acquis sur toutes ces phases, sans en oublier aucun car l'industrie possède des pans entiers qui relèvent encore de chaque phase. Il nous appartient aussi d'élever notre regard à une altitude suffisante pour percevoir la globalité des phénomènes, aborder les problèmes d'une façon systémique, et relativiser les trop nombreuses querelles de paroisse sur des détails de méthodes ou les batailles de mots sur les concepts, souvent sans grande importance sur le long terme.

5

Conclusion : Les règles d'or en matière de sécurité systémique

Dans ce jeu complexe de forces contraires en interactions, la connaissance approfondie de tous les enjeux du système (de sécurité mais aussi commerciaux) et de son histoire est essentielle pour piloter la sécurité et réaliser les compromis et les arbitrages raisonnables.
On ne peut vraiment prendre de bonnes décisions locales qu'à partir d'un critère global d'échanges entre ces forces contraires ; aucune décision en gestion des risques n'a de chance d'être efficace sans une vision systémique.

L'entreprise, un système de tensions contradictoires imposant des arbitrages sur la sécurité

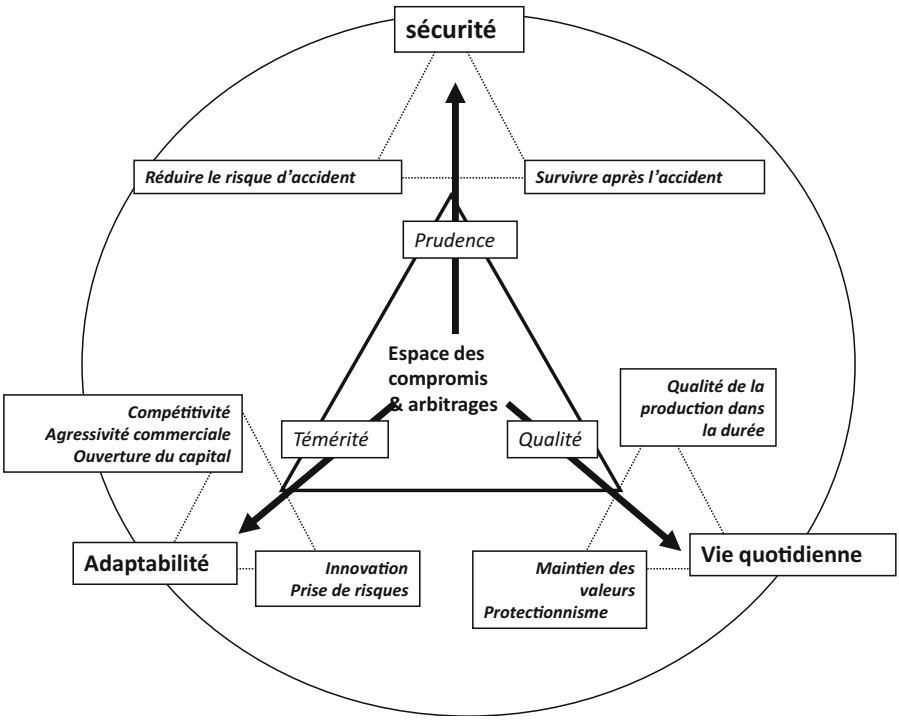
La gouvernance de l'entreprise est soumise en permanence à des tensions pour survivre économiquement. Elle doit se prémunir de quatre risques :

- **ne pas gagner le marché**
  - Pas de produits vendables, concurrence, innovation
  - Commercialisation difficile, diffusion insuffisante, récession économique
- **ne pas pouvoir produire en temps, avec la qualité attendue et au coût attendu**
  - Qualité de la chaîne de production, image de l'entreprise
  - Qualité de la maintenance
  - Paix sociale
- **ne pas maîtriser l'accompagnement financier du business plan d'innovation, de production et de commercialisation**
  - Modèle d'entreprise, choix de l'entité sociale
  - Cash, liquidités, emprunt, dettes, placements
  - Partenariats, alliances… dépendances

- **ne pas maîtriser la sécurité de la production et du produit vendu**
  - Drames humains, Image de l'entreprise
  - Exposition aux sanctions des tutelles

La gestion de ces risques est distribuée dans des directions différentes : commerce, recherche, production, sécurité.
Chacune des directions essaie d'optimiser sa feuille de route, souvent au détriment des autres directions (enjeux de partage des ressources) et justifie ses choix par des risques menaçant la survie à court ou moyen terme.
Dans ce jeu interne, on sait que les arbitrages vont se faire spontanément avec trois constantes :

- **la distance temporelle au bénéfice et au risque**
  - On privilégie le bénéfice immédiat au bénéfice hypothétique à long terme
  - On sacrifie le risque à long terme contre la maîtrise du risque à court terme
- **la fréquence *versus* la gravité**
  - On sacrifie la maîtrise de la gravité hypothétique contre la maîtrise des nuisances fréquentes avérées
- **la saillance et l'émergence *versus* rationalité**
  - Priorité des arbitrages internes en réponse aux jugements externes des menaces (presse, tutelles, marché, finances)



Spontanément, ce jeu de l'arbitrage est peu favorable aux solutions de sécurité : elles prétendent réduire des risques potentiels mais non immédiats, avec des coûts assez élevés (parfois leur coût propre, notamment en personnels, immobilisation pour formations, et souvent pour le frein à la production qu'elles représentent : plus de procédures et d'administration) ; leurs meilleurs avocats sont indiscutablement l'accident passé… et les tutelles externes (quand elles existent) qui exigent une conformité réglementaire. Mais même ce chemin réglementaire est un piège potentiel pour l'arbitrage interne en faveur de solution de sécurité, car il conduit souvent la direction générale à n'attendre que cette mise en conformité et la surveillance d'indicateurs remis aux tutelles (dont la priorité va d'abord à la protection contre les accidents du travail), et à être moins favorable si les moyens manquent à des actions plus systémiques et plus sur le fond.
Enfin, le message de la direction de sécurité est également brouillé par la démarche qualité sur la ligne de production (dont la direction est souvent confondue avec celle de la sécurité) : cette qualité (aux enjeux immédiats d'image) est souvent considérée comme une priorité de plus haut niveau que la sécurité (aux enjeux différés). Elle donne alors l'illusion qu'on écoute et priorise les propositions de la direction de qualité et sécurité, alors qu'elle ne porte que sur un point peu en lien avec la sécurité.

Au final, le réglage final des priorités internes de l'entreprise navigue forcément dans un espace de compromis limité bordé :
- d'un côté par le souci de réduire l'exposition aux risques ;
- d'un autre côté, par le souci d'accepter l'exposition au risque pour des bénéfices secondaires considérés supérieurs.

L'art de l'intervention de sécurité est triple :
- établir et faire valoir une vision systémique du risque de l'entreprise ;
- savoir ne pas reculer dans les compromis sur la sécurité au-delà d'un certain seuil ;
- savoir gérer les sacrifices consentis qui ne font pas partie du plan retenu de priorités.

Les dimensions d'échanges du compromis et de l'arbitrage du risque au sein de la direction de la sécurité

On vient de voir les principales dimensions d'échange du risque dans l'entreprise. Voyons maintenant comment évaluer les marges de compromis dans le dossier de l'intervention/plan de sécurité pour qu'il prépare efficacement les arbitrages possibles lors des discussions à l'échelon stratégique.

Les trois dimensions essentielles du compromis et de l'arbitrage de sécurité

- Le cycle de vie du système. Tous les systèmes industriels et de services naissent et meurent. L'ambition de toute intervention de sécurité est de prolonger la vie du système en lui assurant les meilleures conditions de vieillissement (*healthy life*, santé économique et physique). Cette ambition se décline différemment selon la phase du système. La pression à la sécurité augmente en fin de cycle quand le système a épuisé progressivement ses marges de progrès économiques. En conséquence, les règles d'arbitrage sur les actions de sécurité (par rapport aux contraintes économiques) varient selon la phase du cycle. Les données du marché et les prises de risques sont prioritaires sur les données de sécurité pendant une longue partie du cycle (le modèle de sécurité doit alors accepter les prises de risques et en réduire les conséquences négatives), mais le paradigme s'inverse en fin de cycle où la réduction de l'exposition au risque par les actions redevient prioritaire sur le modèle économique.
- Le guidage de l'opérateur. Si l'on veut conserver un rôle effectif de l'opérateur dans la gestion de la sécurité, il faut privilégier quatre traits de sécurité dans l'organisation du travail, chacun de ces traits ayant des réglages propres ajustés au niveau de sécurité du système : (a) quel que soit le niveau de sécurité, ne pas compter les erreurs, mais plutôt compter les récupérations ratées, (b) pour les systèmes les moins sûrs, ne pas miser sur la prévention et le seul respect des procédures mais privilégier les stratégies de récupération et d'atténuation dans l'effort de formation, d'analyse des accidents et de construction des procédures ; il faut accepter que les incidents vont se répéter (et non pas que l'on va pouvoir les prévenir à l'avenir) et progressivement doter le système d'une résilience interne pour mieux traiter ces incidents, (c) pour les systèmes les plus sûrs, concevoir un système de normes et de contraintes compatibles avec la performance désirée de l'entreprise. Toute exigence excessive (sans doute satisfaisante pour les tutelles et dans le jeu de conformité administrative) se traduira par des violations immédiates que l'entreprise tolérera et qui feront entrer le système dans une perte de contrôle progressive et silencieuse, (d) pour tous les systèmes, concevoir des postes de travail compréhensibles intuitivement par les opérateurs, sans excès de mobilisation de ressources cognitives, permettant la réalisation en routine de la majorité du travail courant et libérant ainsi l'attention de l'opérateur sur les points décisifs pour la sécurité : anticipation, orientations stratégiques, choix et décisions.
- Le modèle économique du système. Tous les systèmes n'ont pas le même enjeu de sécurité. Les systèmes publics ont des exigences évidemment différentes des systèmes artisanaux, et les systèmes instables et fortement innovants ont encore d'autres contraintes. Ces différents systèmes de travail renvoient à différents systèmes de sécurité, qui eux-mêmes ont des réglages internes de compromis et d'arbitrages différents entre sécurité et autres dimensions de l'entreprise. Il faut savoir reconnaître le type de système sur lequel on intervient et appliquer les règles d'arbitrages *ad hoc*. Dans un système artisanal, on acceptera la recherche volontaire d'exposition à

des nouveaux risques en jouant la carte de sécurité *via* les actions sur la compétence des acteurs ; dans un système industriel classique relevant du modèle des HRO, on privilégiera les actions de sécurité sur le collectif et sur les procédures en laissant librement le système s'exposer aux risques et travailler dans ces conditions assez instables. Dans un système public ou ultrasûr, le modèle de sécurité devient la priorité sur le modèle économique, et on développera intensivement la supervision et l'exclusion de l'exposition aux risques.

Un exemple de construction de l'arbitrage en médecine : l'analyse de la valeur[15]**.**
Pourquoi penser amélioration de la valeur plutôt que démarche d'amélioration classique de la qualité ? La réponse est simple : quelques rares exemples mis à part, l'amélioration de la qualité n'a pas tenu ses promesses dans le domaine de la santé. Les résultats sont mal compris, décevants et se heurtent trop souvent à d'autres réalités concurrentes, budgétaires ou tout simplement prioritaires dans la délivrance du soin. L'hôpital doit en effet résoudre en permanence un système de forces contradictoires entre amélioration de la qualité des soins, augmentation du volume de soins et diminution des coûts. Certains hôpitaux arrivent mieux que d'autres à maîtriser cette équation impossible. La solution semble clairement organisationnelle.
L'amélioration de la valeur répond à cette demande. C'est la recherche active du meilleur compromis entre ces trois systèmes de tensions. La qualité peut et doit s'améliorer, mais ne peut le faire concrètement qu'en acceptant de ne pas dégrader les autres dimensions, ou mieux encore, en améliorant aussi ces autres dimensions.
À noter que cette approche n'est pas contradictoire avec le fait que certaines améliorations de la qualité, qui n'apportent pas d'économie, peuvent être importantes et protégées ; mais elles sont relativement rares en comparaison des solutions de qualité qui demandent des arbitrages.
La sécurité des patients liée aux erreurs et multiples défauts d'organisation qui éloignent les professionnels des meilleures pratiques (faillites diverses dans les prises en charge et les coordinations interprofessionnelles), apparaît comme un domaine typique sur lequel l'amélioration de la valeur a un grand impact, à la fois sur le volume de soin (le soin mal fait prolonge l'hospitalisation et surcharge le système de santé), le coût et, bien sûr, *in fine*, la qualité et la sécurité.
La démarche d'amélioration de la valeur consiste à faire un compromis entre l'importance attendue pour le patient, la lourdeur de la mise en œuvre, l'impact sur le coût (espéré positif mais souvent négatif) et le modèle de retour sur investissements.

15. Ovretveit J, Staines A (2011) L'amélioration de la valeur dans les services de santé. Paris: Springer Verlag France.

Ovretveit J (2009) Saving through quality productivity improvement? A review of evidence of quality improvements reducing costs to health service providers. The Health Foundation: London.

Deux exemples de méthodes disponibles pour calculer ce compromis :

1. Le modèle d'analyse de rentabilité « coût – dépense – économie » prend en compte :
– le coût occasionné par le problème de qualité, à savoir, l'estimation du coût annuel pour l'organisation d'un déficit de qualité ;
– les dépenses consenties pour réduire le problème, à savoir, l'estimation des ressources que l'organisation devrait investir pour réduire le problème de 50 %, en incluant les dépenses liées à la mesure du problème et de son évolution ;
– les économies/pertes nettes à un an et pour les années suivantes, à savoir, coût annuel occasionné par le problème, duquel est déduite l'estimation des dépenses pour une année d'activité d'amélioration, montrant combien l'organisation pourrait économiser à une échéance de 1 an et pour les années suivantes.
Exemple : intervention visant à réduire les escarres dans un hôpital de 600 lits :
– coût du gaspillage = $3 millions, si réduction de 50 % = $1,5 million ;
– dépenses consenties pour une réduction de 50 % = $150 000 : temps de l'équipe $30 000, formations $70 000, matelas $50 000 ;
– économies nettes de la première année : $600 000 (en supposant qu'il faut 6 mois pour concevoir un plan et qu'il se met sur pied durant les 6 mois suivants).
– Économies annuelles pour les années suivantes : $1,4 million.

2. La méthode du « coût d'obtention de la qualité » consiste à limiter le déploiement de la qualité aux seuls domaines dans lesquels elle a une chance réelle d'avoir des gains. Elle repose sur un estimé de la somme des différents coûts réels potentiellement induits par la démarche de la qualité :
– coûts de la prévention : coûts occasionnés par les activités visant à prévenir les défaillances de qualité ;
– coûts de l'évaluation de la qualité : coûts de la mesure et de l'inspection des produits ou services pour assurer la conformité aux standards de qualité (maîtrise de la qualité) ;
– coûts de défaillances internes (coûts des défaillances du produit ou de la prestation avant qu'ils ne soient fournis au client) ;
– coûts des défaillances externes (coûts induits par les défaillances après réception du service par le client).
Cinq points nécessaires pour construire et réussir une démarche d'amélioration de la valeur :
– une vision pour le système médical, comprise de tous, patients et professionnels ;
– une stratégie ciblée porteuse de sens ;
– un crescendo sur 10 à 20 ans pour assurer le parcours organisationnel nécessaire pour atteindre le but avec son bénéfice maximal : RIEN NE PEUT ÊTRE OBTENU À TRÈS COURT TERME dans les deux premières années, il FAUT SAVOIR INVESTIR ET DURER DANS LA MÊME STRATÉGIE en acceptant que les premières années (0-3 à 5 ans) coûtent, puis que le bénéfice augmente progressivement ;
– une identification des processus, de leurs buts et de leurs interactions ;
– un vrai leadership, reconnu et pérenne.

Deux exemples particulièrement étudiés pour leur valeur pédagogique :

1. Le canton de Jonkoping en Suède est un exemple connu dans le monde entier pour la qualité des soins dispensés à ses patients : adhésion complète de la population et des professionnels, réduction spectaculaire du nombre d'EIG, efficacité, proximité et soutien pour tous :
– la vision commune de la démarche est simple et ambitieuse (le slogan fédérateur) : « une vie attractive et bonne pour tous dans le canton » (*nda*, cette vision ne fait même pas mention du fait médical) ;
– la stratégie d'amélioration de la qualité est vue comme un parcours d'apprentissage plutôt que comme une méthode toute faite. Une veille à l'égard des nouveaux outils et des nouvelles méthodes systématiquement étudiées et testées, adoptées seulement si elles s'insèrent avantageusement dans la vision et dans la culture ;
– la durée est prise en compte avec la stabilité et la continuité au sein des équipes ;
– chaque cible visée est priorisée, analysée pour sa valeur ajoutée, connue de tous, de la secrétaire au patron, et valorisée ;
– les processus sont identifiés et le soutien de leur pilotage assuré y compris financièrement. Le directeur général est personnellement impliqué dans le pilotage, tout comme le directeur de l'innovation et le directeur médical.

2. Le système des hôpitaux d'Intermountain dans l'Utah aux États-Unis (*non profit organization*) offre un autre exemple mondialement connu de réussite dans l'analyse de la valeur :
– la vision proposée et partagée par tous est celle de « l'excellence clinique » ;
– tous les processus sont priorisés pour ne garder que ceux qui ont la meilleure preuve clinique (EBM) tout en ayant la meilleure valeur économique. Huit spécialités ont analysé et produit leurs *guidelines* dans ce sens après un long processus d'apprentissage de la méthode ;
– chaque programme clinique fait l'objet d'un projet de déploiement complet avec des compétences dans tous les secteurs, bien sûr médicaux, mais aussi administratifs, informatiques, statistiques. Les résultats sont suivis et commentés en continu chaque mois pour décider de corrections ou d'améliorations (y compris dans le déploiement de nouveaux emplois ou ressources si nécessaire) ;
– le partage d'information est au cœur de l'engagement des professionnels et des patients (informatisation, dossier médical informatisé, PC dans chaque chambre de patient, application intranet pour suivre les résultats cliniques, processus et *outcomes*) ;
– le système a mis plusieurs années à s'organiser dans ce sens, mais le bénéfice actuel est tout simplement remarquable : des ressources (moyens humains et techniques) très supérieures à la moyenne des hôpitaux américains, pour une valeur et un service rendu au patient très supérieurs, et un système financier sain, dégageant des profits réinvestis sur l'innovation.

10 règles d'or pour réussir une intervention de sécurité systémique

Le balayage des différents points importants pour une approche systémique du risque dans l'entreprise conduit à proposer 10 règles de base pour gérer avec efficacité le plan de sécurité, son déploiement, les sacrifices que l'on peut consentir et ceux pour lesquels on ne peut pas faire l'impasse. Les 10 règles se déclinent aux trois échelles du système : macro (le système), méso (l'entreprise, l'hôpital) et micro (le poste de travail).

Au niveau MACRO

1. Ne pas devancer la demande de sécurité, et vouloir accélérer la sécurisation d'un système : chaque système a un cycle de vie ; ses besoins de sécurité changent à chaque étape ; inutile de vouloir répondre au-delà de la demande, car on ne ferait qu'accélérer le parcours vers la fin du cycle.
2. Prendre en compte l'espace complet des contraintes de l'entreprise. Établir une juste estimation du besoin de sécurité. Le modèle économique et particulièrement le besoin de l'exposition au risque guide le modèle de sécurité que l'on va choisir. Sauf à avoir l'ambition de changer de modèle économique, il faut privilégier les moyens d'optimisation internes au modèle choisi avant de prendre sur étagères des solutions de sécurité dans d'autres modèles. L'analyse élargie systémique de la situation et de la cartographie des risques peut amener à considérer des priorités ou des solutions de sécurité jusque-là ignorées parce que hors champ (par exemple agir sur l'obésité en privilégiant une politique de santé publique et d'éducation alimentaire, plutôt qu'une priorité centrée sur la prise en charge médicale).
3. Survivre aux accidents est aussi important que savoir les éviter. Le plan de sécurité ne peut pas s'arrêter à la prévention des accidents. Tout comme la gestion de l'erreur au niveau individuel doit laisser une large place à la détection et à la récupération, la gestion de la sécurité d'un système complexe doit réserver une place à la gestion de l'accident (crise), et à la survie de l'entreprise après l'accident.

Au niveau MÉSO

4. Concevoir une intervention « totale » aux niveaux macro, méso et micro : Aucun plan de sécurité ne peut se limiter à des solutions de sécurité portées uniquement par les acteurs de première ligne. Il faut toujours envisager une part de la cartographie des

risques et de l'intervention de sécurité spécifique à l'engagement de la direction exécutive, du *top* et *middle management*[16, 17].

5. Soigner particulièrement la déclinaison du plan avec le *middle management* : faisabilité, engagement, formation. Bien se rappeler que gérer les risques revient à gérer toutes les sources de problème qui peuvent tuer l'entreprise. La sécurité, comprise comme l'évitement des accidents, n'est qu'un aspect de ces risques, aux côtés des risques économiques, d'image, de manque de savoir-faire innovant… Dans la majorité des cas, ce sont même ces autres risques qui sont les plus immédiatement perçus comme menaçant l'entreprise. Il faut savoir accepter cette priorité relative, tout en maintenant une vigilance et une défense éclairées des aspects purement sécurité. On s'attachera particulièrement à bien faire ce qui est possible de faire, et encore plus à bien cerner tout ce que l'on a (temporairement) renoncé à faire, afin de renforcer les protections sur ces derniers points. Le management a un rôle clé dans ces deux fonctions. En effet, le bénéfice du plan de sécurité, même négocié à la baisse, ne sera obtenu qu'avec la complicité et l'engagement total du management. Le plan de sécurité doit décliner comment on va convaincre ce *middle management*, qu'est-ce qu'on va lui expliquer sur les aspects sacrifiés, et comment ce management envisage de convaincre et relayer à son tour les cadres de proximité et les opérateurs de premières lignes. La partie relative à l'information des cadres et opérateurs sur ce que l'on a décidé de ne pas faire dans le plan de sécurité est aussi stratégique que la partie de conviction sur bien faire ce que l'on a décidé de faire.

6. Établir une juste analyse des coûts économiques des incidents/accidents. L'analyse systémique de sécurité et les arbitrages qui vont avec obligent à adopter un grand réalisme. Trois sous-dossiers doivent accompagner l'analyse des risques pour se préparer

---

16. Lire par exemple :

Carthey J, de Leval MR, Reason JT (2001) Institutional resilience in healthcare systems. Qual Health Care 10: 29-32. Exposé de la méthode CAIR d'audit des directions d'hôpitaux et de cliniques sur leur management de la sécurité et de la qualité.

La méthode se base sur l'exploration par questionnaire de 3 dimensions (the three Cs') :

– commitment : engagement par les directeurs à considérer la sécurité du patient comme une priorité, mesuré sur l'analyse des décisions prises, les arbitrages réellement effectués en faveur de la sécurité, et la présence des directeurs dans les réunions parlant de sécurité ;

– compétence : la compétence des directeurs en matière de sécurité des soins, leur formation ;

– cognizance : connaissance du risque : quelles actions (tableaux de bord, gestion de crise) la direction a-t-elle pour connaître le risque lié au soin : signalement non punitif, solutions pour analyser collectivement le risque. Quel est le temps réservé à la lecture et à l'analyse de ces actions dans les comités de directions ?

17. Un autre article illustre parfaitement cette approche système appliquée par les autorités de santé d'Écosse. L'action prend le nom de NINEWELLS HOSPITAL et s'étale sur 3 ans. Elle compte quatre piliers essentiels : (1) imposer la sécurité du patient comme une priorité stratégique, (2) imposer la sécurité du patient comme un sujet auquel on consacre les mêmes temps et investissements que pour les autres sujets habituels dans les staffs de gouvernance, (3) concevoir une organisation pérenne centrée sur la sécurité du patient dans la santé et dans les hôpitaux, avec (4) une résonance institutionnelle particulière dans la formation (postes de professeurs, cursus actifs…). Les réformes exécutées ont été suivies par la mesure du taux d'événements indésirables par une méthode imposée à tous les établissements de santé. Les résultats montrent notamment une réduction de la mortalité, et une réduction des infections sur voies veineuses centrales.

Haraden C, Leitch J (2011) Scotland's successful national approach to improving patient safety in acute care. Health Affairs 30 (4): 755-63.

aux arbitrages et préserver le maximum d'actions sur cette dimension de la sécurité : l'un calculant le coût de la non-qualité et des sinistres, un second proposant une évaluation de l'impact sur l'image commerciale de la non-qualité et des performances de sécurité médiocres, un troisième calculant l'impact potentiel de ce que l'on ne va vraisemblablement pas faire, faute de moyens ou par le fait des arbitrages liés à d'autres priorités.

Au niveau MICRO

7. Établir une juste analyse des causes des accidents et incidents. Une approche systémique réussie impose d'être honnête et complet dans l'analyse des causes d'accidents et des décisions de correction. Il s'agit notamment de ne pas simplifier excessivement la causalité en se limitant aux erreurs patentes des opérateurs ; il faut considérer au même rang de priorité les actions sur les erreurs latentes liées à l'organisation. Au-delà de ces actions sur les erreurs latentes ou patentes, il faut aussi réserver une place privilégiée dans la cartographie aux risques d'accidents associés aux mauvais couplages entre structures sans que nécessairement chaque structure ait commis des erreurs (au travail sur les interfaces).
8. Préserver une juste autonomie des acteurs. La robustesse ou résilience finale du système repose toujours sur la capacité adaptative résiduelle des acteurs. Il faut veiller à ne pas se corseter de procédures inutiles, chaque procédure réduisant un peu plus la capacité adaptative du système.
9. Établir une juste politique d'incitation/contrôle-sanction. La lutte contre l'erreur et contre les violations conduit au souhait d'une transparence maximale tout en préservant un régime de sanctions pour les cas les plus inacceptables. Le consensus entre partenaires sociaux sur ce régime de la transparence et de la sanction est essentiel pour le succès du plan de sécurité. En quoi le système va récompenser les acteurs qui signalent, qui va être concerné (la direction et le management doivent l'être tout autant que les acteurs de premières lignes), quels sont les critères réels de l'inacceptable, particulièrement en conditions économiques dégradées où l'entreprise doit prendre plus de risques pour survivre ? Tous ces points doivent être présents et discutés dans le plan de sécurité.
10. Établir une juste information. La transparence ne doit pas concerner seulement la déclaration des événements indésirables. Elle doit concerner toute l'information des travailleurs sur les stratégies poursuivies par l'entreprise, tant d'un point de vue économique qu'en termes de politique de sécurité.

La sécurité d'un système n'est jamais un travail achevé ; c'est toujours un état transitoire, perçu favorablement ou défavorablement par les tutelles, les clients et l'entreprise elle-même.

Piloter la sécurité n'est jamais une recette (boîte à outil disponible, mais qui ne règle pas les problèmes). Sa maîtrise relève d'abord de la capacité à se réinterroger en tant que gestionnaire de risque, et à percevoir les équilibres qu'il faut préserver pour survivre aujourd'hui, et ceux qui peuvent évoluer pour laisser plus de chance à l'entreprise de survivre demain.

Références

- Allwood CM (1984) Error detection processes in statistical problem solving. Cognitive science 8: 413-37
- Allwood C, Montgomery H (1982) Detection errors in statistical problem solving. Scandinavian Journal of Psychology 23: 131-13
- Amalberti R, Wioland L (1997) Human error in Aviation. Key note address at the International Aviation Safety Conference 1997 (IASC-97), Rotterdam Airport. In: H. Shoekkha ed, Aviation Safety, VSP BV: The Netherlands, p. 91-108
- Amalberti R (1998) Automation in Aviation: A human factors perspective. In D. Garland, J. Wise., J. Hopkins (Ed.), Aviation Human Factors (Hillsdale-New Jersey: Lawrence Erlbaum Associates), 173-92
- Amalberti R (2001) La maîtrise des situations dynamiques. Psychologie Française 46-2 : 105-17
- Amalberti R, Fuchs C, Gilbert C (2001) Risques, erreurs et défaillances. Grenoble: MSH Vol 1
- Amalberti R, Fuchs C, Gilbert C (2002) Conditions et mécanismes de production des défaillances, accidents, et crises (Vol. 2). Grenoble: MSH-CNRS
- Amalberti R, Fuchs C, Gilbert C (2003) La mesure des défaillances et du risque (Vol. 3). Grenoble: MSH-CNRS
- Amalberti R. (2001). The paradoxes of almost totally safe transportation systems. Safety Science 37: 109-26
- Amalberti R (2009) Quel futur et quelle stratégie de sécurité pour un système devenu ultrasûr ? Transfusion Clinique et Biologique 16: 80-5
- Amalberti R, Brami J (2011) Tempos management in primary care: a key factor for classifying adverse events, and improving quality and safety, BMJ Quality & Safety Online First, published on 2 September 2011 as 10.1136/bmjqs.2010.048710
- Amalberti R (2001) La conduite des systèmes à risques. Paris: PUF, 2e ed, traduit en espagnol : Amalberti R (2009) *El control de los sistemas de alto riesgo,* Madrid: Modus Laborandi
- Amalberti R (2001) La conduite des systèmes à risques. Paris: PUF, 2e ed
- Amalberti R, Deblon F (1992) Cognitive modelling of fighter aircraft's control process: a step towards intelligent onboard assistance system. International Journal of Man-Machine studies 36: 639-71
- Amalberti R, Auroy Y, Berwick D, Barach P (2005) Five system barriers to achieving ultrasafe health care. Ann Intern Med 142, 9: 756-64
- Amalberti R, Vincent C, Auroy Y, de Saint Maurice G (2006) Framework models of migrations and violations: a consumer guide. Quality and Safety in Healthcare 15 (suppl 1): i66-71
- Amalberti R (2006) Optimum system safety and optimum system resilience: agonist or antagonists concepts? In: Hollnagel E, Woods D, Levison N. Resilience engineering: concepts and precepts, Aldershot, England: Ashgate: 238-56
- Amalberti R (2002) Use and misuse of safety models in design. Lecture Notes in Computer Science 2485: 1-21
- Amalberti R, Barach P. Improving healthcare: understanding the properties of three contrasting and concurrent safety models. Submitted

- Aslanides M, Valot C., Nyssen AS, Amalberti R (2007) Evolution of error and violation description in french air force accident reports: impacts of human factors education. Human Factors and Aerospace safety 6: 51-70
- Aylin P, Yunus A, Bottle A, *et al.* (2010) Weekend mortality for emergency admissions: a large multicentre study. Qual Saf Health Care 19: 213-7
- Bainbridge L (1987) Ironies of automation. In: New technology and human errors, sous la dir. de Rasmussen, Duncan & Leplatedts. Wiley publ., p. 271-86
- Bell CM, Redelmeier DA (2001) Mortality among patients admitted to hospitals on weekends as compared with weekdays. N Engl J Med 345: 663-8
- Bell J, Holroyd J (2009) Review of human reliability assessment methods, report HSE, http://www.hse.gov.uk/research/rrpdf/rr679.pdf
- Besnard D, Greathead D, Baxter G (2004) When mental models go wrong : co-occurrences in dynamic, critical systems. Int J Human-Computer Studies 60: 117-28
- Barber N (2002) Should we consider non-compliance a medical error? Qual Saf Health Care 11: 81-4
- Bell CM, Redelmeier DA (2001) Mortality among patients admitted to hospitals on weekends as compared with weekdays. N Engl J Med 345: 663-8
- Bell J, Holroyd J (2009) Review of human reliability assessment methods, report HSE, http://www.hse.gov.uk/research/rrpdf/rr679.pdf
- Besnard D, Greathead D, Baxter G (2004) When mental models go wrong : co-occurrences in dynamic, critical systems. Int J Human-Computer Studies 60: 117-28
- Boy GA (2011) Handbook of human-machine interaction - A human-centered design approach. Ashgate, UK
- Braithwaite JJ, Hyde P, Pope C (2010) Culture and climate in health care organizations. Palgrave MacMillan
- Brami J, Amalberti R (2009) Les risques en médecine générale. Springer Verlag France: Paris
- Broadbent D (1958) Perception and Communication. London: Pergamon Press
- Cellier JM, de Keyser V, Valot C (1996) La gestion du temps dans les environnements dynamiques. PUF: Paris
- Chateauraynaud F, Torny D (1999) Les sombres précurseurs : une sociologie pragmatique de l'alerte et du risque. Paris, EHESS
- Classen D, Resar R, Griffin F, et al. (2011) Global trigger tool shows that adverse events in hospitals may be in times greater than previously measured. Health affairs 30: 581-9
- Cooper D (2009) Behavioral safety interventions. Professional Safety: 37
- Cullen D, Bates D, Small S, *et al.* (1995) The incident reporting system does not detect adverse drug events: a problem for quality improvement. Jt Comm J Qual Improv 1: 541-8
- Daniellou F, Simart M, Boissière I. Human and organizational factors of safety :state of the art, ICSI, http://www.foncsi.org/media/PDF/CSI-HOFS.pdf
- de Kersasdoué J (2007) Les prêcheurs de l'apocalypse, pour en finir avec les délires écologiques et sanitaires. Paris: Plon
- De Keyser V (1996) Les erreurs temporelles et les aides techniques. In: La gestion du temps dans les environnements dynamiques, sous la dir. de Cellier JM, De Keyser V, Valot C. Paris: PUF, p. 287-310
- de Montmollin M. L'ergonomie de la tâche, Peter Lang, Berne, 1986

- De Saint Maurice G, Auroy Y, Vincent C, Amalberti R (2010) The natural life span of a safety policy: violations and migration in anaesthesia, Qual Saf Health Care 19: 327-31
- De Tersac G, Mignard J (2011) Les paradoxes de la sécurité, le cas d'AZF. Paris: PUF
- Dekker S (2004) Ten questions about human error. A New View of Human Factors and System Safety. Aldershot, England: Ashgate
- Dekker S (2007) Just culture, balancing safety and accountability. Aldershot, UK: Ashgate
- Doireau P, Wioland L, Amalberti R (1997) La détection des erreurs par des opérateurs extérieurs à l'action : le cas du pilotage d'avion. Le Travail Humain 60: 131-53
- Dorner D (1997) The logic of failure: recognizing and avoiding error in complex situations. Perseus Books
- Duncker K (1945) On Problem Solving. Psychological Monographs 58: 270
- Endsley M (1995) Toward a theory of situation awareness in dynamic systems. Human Factors 37: 32-64
- Endsley MR, Garland DJ (2000) Situation awareness analysis and measurement. Mahwah, NJ: Lawrence Erlbaum
- Ekvall G (1991) The organizational culture of idea-management : a creative climate for the management of ideas. In: Managing Innovation, sous la dir. de Henry J and Walker D, London: Sage, p. 73-9
- Evans SM, Berry JG, Smith BJ, *et al.* (2006) Attitudes and barriers to incident reporting: a collaborative hospital study. 15: 39-43
- Falzon P, Amalberti R, Carbonell N (1986) Dialogue control strategies in oral communication. In: The future of command languages: foundations for Human Computer communication, sous la dir. de D. Hopper et IA Newman. North Holland: Elsevier Science Publisher, p. 73-98
- Fioratou E, Flin R, Glavin R (2012) No simple fix for fixation errors : cognitive processes and their clinical implications. Anesthesia 65: 61-9
- Flin R (2007) Measuring safety culture in healthcare: a case for accurate diagnosis. Safety Science 45: 653-67
- Flin R, O'Connor P, Crichton M (2008) Safety at the sharp end: a guide to non-technical skills. Aldershot, UK: Ashgate
- Frankel E (1988) System reliability and risk analysis. Kluwer
- Gerstein M, Ellsberg M, Ellsberg D (2008) Flirting with disaster: why accidents are rarely accidental. Sterling Publishing
- Ghaferi A, Birkmeyer J, Dimick J (2009) Variation in hospital mortality associated with inpatient surgery. N Engl J Med 361: 1368-75
- Gibson J (1979) The ecological approach to visual perception. Boston: Houghton-Mifflin
- Gibson J, Crooks L (1938) A theoretical field analysis of automobile-driving. American Journal of Psychology 51: 453-71
- Gilbert C, Amalberti R, Laroche H, Pariès J (2007) Toward a new paradigm for error and failures. Journal of Risk Research 10: 959-75
- Gillespie R (1991) Manufacturing knowledge: a history of the Hawthorne Experiments. Cambridge: Cambridge University Press, and Sonnenfeld JA (1985) Shedding Light on the Hawthorne Studies. Journal of Occupational Behavior 6
- Gollier C, Treich N (2003) Decision making under uncertainty : the economics of the precautionary principle. Journal of risk and uncertainty 27 : 77-103, ou Guilhou X, Lagadec P (2002) La fin du risque zéro. Ed Organisations

- Guilhou X, Lagadec P (2002) La fin du risque zéro. Ed Organisations
- Grote G (2012) Safety management in different high-risk domains – All the same? Safety Science, in press, 2012
- Guldenmund F (2000) The nature of safety culture: a review of theory and research. Safety Science 34 (1-3): 215-57
- Guldenmund F (2007) The use of questionnaires in safety culture research – an evaluation. Safety Science 45: 723-43
- Hale A, Swuste A (1998) Safety rules: procedural freedom or action constraint? Safety science 29: 63-177
- Haraden C, Leitch J (2011) Scotland's successful national approach to improving patient safety in acute care. Health Affairs 30 (4): 755-63
- Hayes J, Flower L (1980) Identifying the organization of writing processes. Cognitive processes in rriting. L. Gregg, Steinberg, E. Hillsdale, Lawrence Erlbaum Associates
- Helmreich R (2000) On error management: lessons from aviation. Br Med J 320: 781-5
- Helmreich RL, Merritt AC (1998) Culture at work: national, organizational, and professional influences. Aldershot, United Kingdom: Ashgate
- Helmreich R (1993) Attitudes towards automation across five cultures – NASA report/ University of Texas/FAA - Aerospace Crew Research
- Heinrich HW (1931) Industrial accident prevention. New York: McGraw-Hill
- Hoc J M (1988) Cognitive psychology of planning. London: Academic Press
- Hoc JM, Amalberti R (2007) Cognitive control dynamics for reaching a satisficing performance in complex dynamic situations. Journal of cognitive engineering and decision making 1: 22-55
- Hofstede G (1983) Culture's consequences: international differences in work-related values. Administrative Science Quarterly (Johnson Graduate School of Management, Cornell University) 28: 625-29
- Hollnagel E (2004) Barriers and accident prevention. Aldershot, UK: Ashgate
- Hollnagel E (2009) The ETTO principle. Efficiency-Thoroughness Trade-Off, Ashgate Publishing
- Hollnagel E, Woods D, Levison N (2006) Resilience engineering: concepts and precepts. Aldershot, England: Ashgate
- Hopkins A (2005) Safety, culture and risk, first ed. CCH Australia Ltd, Australia
- Hopkins A (2007) Holding corporate leaders responsible. Keeping Good Companies 59: 340-4
- Hughes T (1983) Networks of power-electrification in Western countries. Baltimore: John Hopkins Univ Press
- ICSI, Leadership en sécurité, Cahiers de la sécurité industrielle, consulté le 29 décembre sur http://www.icsi-eu.org/francais/dev_cs/cahiers/CSI-LIS-pratiques-industrielles.pdf
- Jha A, Hupeerman G, Teich J, *et al.* (1998) Identifying adverse drug events. JAMIA 5: 305-14
- Johnson C (2004) Human Error and the Failure of Imagination, In: Human Error, Safety and Systems Development, sous la dir. de CW Johnson, P. Palanque, Préface. Kluwer Academic Press
- Johnson C (2003) Failure in safety-critical systems: a handbook of accident and incident reporting. University of Glasgow Press, Glasgow, Scotland

- Johnson C, Holloway C (2004) Systemic failures and human error in Canadian aviation reports between 1996 and 2002. In: HCI in Aerospace 2004, sous la dir. de Pritchett A et Jackson A, Eurisco, Toulouse, p. 25-32
- Kahneman D, Slovic P, Tversky A (1982) Judgement under uncertainty: heuristics and biases, Cambridge, Ma: Cambridge University Press
- Kanki B, Helmreich R, Anca J (2010) Crew resource management. Academic Press, 2nd ed
- Klein G, Zsambok CE (1997). Naturalistic Decision Making. Mahwah, NJ: LEA
- Lawton R, Parker D (2002) Barriers to incident reporting in a healthcare system. Qual Saf Health Care 11: 15-8
- Lewin Kurt (1935) A dynamic theory of personality. Mc Graw-Hill
- Lewis E (1987) Introduction to reliability engineering. John Wyley and sons
- Liker J (2003). The Toyota Way: 14 management principles from the world's greatest manufacturer, First edition. McGraw-Hill
- Marc J, Amalberti R (2002) Contribution de l'individu au fonctionnement sûr du collectif : l'exemple de la régulation du SAMU. Le Travail Humain 64: 201-20
- Marx D (2001) Patient Safety and the "Just Culture": a primer for health care executives. New York, NY: Columbia University
- Maturana H, Varela F (1992) The tree of knowledge, the biological roots of natural understanding. Shambala publications
- Mayo E. The human problems of an industrial civilization. Contributors: first published 1933, reprint in Thompson K. The early sociology of management and organizations – Routlege London. Publication Year: 2003
- McCammmon I (2004) Heuristics traps in recreational avalanche accidents: evidence and implications. Avalanche News: 68
- Miller GA (1956) The magical number seven, plus or minus two: some limits on our capacity for processing information. Psychological Review 63: 81-97
- Morel G, Amalberti R, Chauvin C (2008) Articulating the differences between safety and resilience: the decision-making of professional sea fishing skippers. Human factors 1: 1-16
- Morel G, Amalberti R, Chauvin C (2009) How good micro/macro ergonomics may improve resilience, but not necessarily safety. Safety Science 47: 285-94
- Morel G, Chauvin C (2007) A socio-technical approach of risk management applied to collisions involving fishing vessels. Safety science 44: 599-619
- Morineau T, Hoc JM, Denecker P (2003) Cognitive control levels in air traffic radar controller activity. Int Journal of Aviation Psychology 13 : 107-30
- Newell A, Simon H (1972) Human problem solving. Englewoods Cliffs, NY, Prentice HAll
- Noizet A, Amalberti R (2000) Le contrôle cognitif des activités routinières des agents de terrain en centrale nucléaire : un double système de contrôle. Revue d'Intelligence Artificielle 14(1-2): 73-92
- Norman D (1981) Categorization of action slips. Psychological review 88: 1-15
- Norman D (1983) Some observations on mental models. In: Mental models, sous la dir. de G. Stevens et S. Gentner. Hillsdale, NJ : LEA
- Norman D (1988) The design of everyday things. New York : Double Day Curency, pour un développement du concept inspiré de Gibson).
- Norman D A, Shallice T (1986) Attention to action: willed and automatic control of behavior. Consciousness and self-regulation. Davidson GS, Shapiro D. New York, Plenum Press 4: 1-18

- Ochanine D (1981) L'image opérative, actes d'un séminaire et recueil d'articles. Université Paris V
- O'Hara K, Payne S (1998) The effects of operator implementation cost on planfulness of problem solving and learning, Cognitive Psychology 35: 34-70
- O'Hara K, Payne S (1999) Planning and the user interface : the effect of lockout time and error recovery cost. International Journal Human Computer Studies 50: 41-59
- O'Reilly C, Chatman A, Caldwell D (1991) People and organizational culture: a profile comparisons approach to assessing person-organization fit. Academy of Management Journal 34: 487-516
- Ostberg G (2009) Some intangibles in human handling of risks, Lund University, Sweden RISC-Research Paper No. 3, http://www.wisdom.at/Publikation/pdf/RiskBerichte/RRR_GOestberg_SomeIntangibles_09.pdf
- Ovretveit J, Staines A (2011) L'amélioration de la valeur dans les services de santé. Paris: Springer Verlag France
- Ovretveit J (2009) Saving through quality productivity improvement ? A review of evidence of quality improvements reducing costs to health service providers. The Health Foundation: London
- Pascarelli E, Quilter D (1994) Repetitive strain injury. John Wiley and sons
- Perrow C (1984) Normal accidents: living with high-risk technologies. Basic Books: NY
- Piaget J (1974) La prise de conscience. Paris: PUF
- Plat M, Amalberti R (2000) Experimental crew training to deal with automation surprises. In: *Cognitive Engineering in the Aviation Domain*, sous la dir. *de* NSR Amalberti, Hillsdale- New Jersey: Lawrence Erlbaum Associates, p. 287-308
- Polet P, Vanderhaegen F, Amalberti R (2003) Modelling the border-line tolerated conditions of use. Safety Science 41: 111-36
- Rasmussen J (1997) Risk management in a dynamic society. Safety Science 27: 183-214
- Rasmussen J. (1983) Skills, rules, knowledge: signals, signs, and symbols, and other distinctions in human performance models. IEEE Transactions on Systems, Man and Cybernetics 13: 257-66
- Reason J. Human error, Cambride University Press, 1990, traduit en Français PUF, Paris, 1993 ; traduit en espagnol, Modus Laborandi, 2009.
- Reason J (1997) Managing the risks of organizational accidents. Aldershot, England: Ashgate
- Reason JT, Carthey J, de Leval MR (2001) Diagnosing vulnerable system syndrome: an essential prerequisite to effective risk management Qual Health Care 10 (suppl 2): i21-5
- Resar R, Rozich J, Classen D (2003) Methodology and rationale for the measurement of harm with trigger tools. Qual Saf Health Care 12: 39-45
- Ricci M, Goldman AP, de Leval MR, *et al.* (2004) Pitfalls of adverse event reporting in paediatric cardiac intensive care. Archives of Disease in Childhood 89: 856-85
- Rizzo A, Bagnara S, Visciola M (1987) Human error detection process. International Journal Man-Machine Studies 27: 555-70
- Roussel P, Moll MC, Guez P (2007) Étape 2 : Identifier les risques *a priori*. Risques & Qualité en milieu de soins IV 4: 239-47
- Roussel P, Moll MC, Guez P (2008) Étape 3: Identifier les risques *a posteriori*. Risques & Qualité en milieu de soins V-1: 46-58

- Rozich JD, Haraden CR, Resar RK (2003) Adverse drug event trigger tool: a practical methodology for measuring medication related harm. Qual Saf Health Care 12: 194-200
- Sarter N, Woods D (1992) Pilot interaction with cockpit automation: operational experiences with the flight management system. International Journal Aviation Psychology 2(4): 303-21
- Sarter N., Amalberti R. (Ed.). Cognitive engineering in the aviation domain. Hillsdale- New Jersey: Lawrence Erlbaum Associates, 2000
- Schein, Organizational culture and leadership, John Wiley & sons, 1985, Ed 2010
- Shiffrin R, Schneider W (1977) Controlled and automatic human information processing: perceptual learning, automatic attending and a general theory. Psychological Review 84: 127-90
- Simon H (1982) Models of bounded rationality, vol. 1. MIT Press
- Sjohania K, Sampson M, Ansari M, *et al.* (2007) How quickly do systematic reviews go out of date? A survival analysis. Ann Int Med 147: 224-33
- Taylor F. The principles of scientific management. Harper & Row, 1911, Reprint Norton Library, 1967
- Tengs T, Adams M, Pliskin J, *et al.* (1995) Five-hundred life-saving Interventions and their cost-effectiveness. Risk analysis 15, 3: 369-90
- Thakur M (1998) Involving middle managers in strategymaking. Long Range Planning 31(5): 732-41
- Uyterhoeven HE (1972). General managers in the middle. Harvard Business Review 50: 75-85 et Thakur M (1998) Involving middle managers in strategymaking. Long Range Planning 31: 732-41
- Valot C, Amalberti R (1992) Metaknowledge for time and reliability. Reliability Engineering and Systems Safety 36: 199-206
- Vincent C, Stanhope N, Crowley-Murphy M (1999) Reasons for not reporting adverse incidents: an empirical study. J Eval Clin Pract 5: 13
- Westrum R (2004) A typology of organisational cultures. Qual Saf Health Care 13: 22-7
- Wickens C (1984) Varieties of attention. New York: Academic Press
- Wilson R (1979) Analyzing the daily risks of life. Technology Review 81: 40-6
- Wioland L, Amalberti R (1996, November 12-15). When errors serve safety: towards a model of ecological safety. In: First Asian conference on Cognitive Systems Engineering in Process Control (CSEP 96), sous la dir. de E. Hollnagel. Kyoto, Japan: 184-91
- Woods DD (2005) Creating foresight: lessons for resilience from Columbia. In: Organization at the Limit: NASA and the Columbia Disaster, sous la dir. de W.H. Starbuck and M. Farjoun, Blackwell, p. 289-308
- Woods DD, Hollnagel E (2006) Joint cognitive systems: patterns in cognitive systems engineering. BocaRaton, FL: 2006, Taylor & Francis.
- Young J, Ranji S, Wachter R, et al. (2011) July effect: impact of the academic year-end change over on patient outcomes. Ann Intern Med 155: 309-15
- Zangh J, Norman DA (1994) Representation in distributed cognitive tasks. Cognitive Science 18: 87-122

Du même auteur

Livres et direction d'ouvrages de l'auteur en lien avec le thème

Livres d'auteurs

- Amalberti R. La conduite de systèmes à risques. Paris: Presses Universitaires de France (1996, 2e édition 2001).
- Amalberti R (2009) El control de los sistemas de alto riesgo, Madrid : Modus Laborandi, 2009 (traduction de la conduite des systèmes à risques, PUF)
- Brami J, Amalberti R (2009) Les risques en médecine générale, Springer Verlag France
- Amalberti R, Brami J. Audits de risques au cabinet de ville, Springer, à paraître, Septembre 2012

Livres coédités

- Amalberti R, de Montmollin M, Theureau J (1991) Modèles en analyse du travail (Vol. n° 171) Liège: Mardaga
- Amalberti R, Mosneron-Dupin F (1997) Démarches facteurs humains dans les études de fiabilité. Toulouse: Octarès
- Amalberti R (1998) Notions de sécurité écologique: le contrôle du risque par l'individu et l'analyse des menaces qui pèsent sur ce contrôle. Grenoble: MSH
- Sarter N, Amalberti R (2000) Cognitive engineering in the aviation domain. Hillsdale-New Jersey: Lawrence Erlbaum Associates
- Amalberti R, Masson M, Merritt A, Pariès J (2000) Briefings [Human Performance and limitations]. Paris: IFSA Dédale (3rd edition), traduit en anglais et espagnol
- Amalberti R, Fuchs C, Gilbert C (2001) Risques, erreurs et défaillances. Grenoble, MSH, Vol 1
- Amalberti R, Fuchs C, Gilbert C (2002) Conditions et mécanismes de production des défaillances, accidents, et crises (Vol. 2). Grenoble: MSH-CNRS
- Amalberti R, Fuchs C, Gilbert C (2003) La mesure des défaillances et du risque (Vol. 3). Grenoble: MSH-CNRS
- Vallery G, Amalberti R (2006) L'analyse du travail en perspective: influence et évolutions, Toulouse: Octarès

Direction de collection

Collection Progrès en sécurité des soins, Springer

Index