IMdR Info
Lettre d'information
de l'Institut pour la Maîtrise des Risques
Sûreté de fonctionnement - Management - Cindyniques
n°37
1er trimestre 2018

*Spécial « Entretiens du risque 2017 »*

sommaire



## Edito

Les 6èmes Entretiens du risque réunirent près de 100 personnes au Carré des Sciences les 14 et 15 novembre sur le thème « **Le déni du risque : de l'attitude individuelle à la gouvernance des organisations** ». Ce thème émergea lors des Entretiens 2015 (*Explorer l'imprévisible : comment et jusqu'où ?*), après qu'André Claude Lacoste eut parlé de silence organisationnel.

Le déni est un terme polysémique ; ses synonymes sont : démenti, dénégation, refus, scotomisation. Le sujet est si difficile à appréhender que des conférenciers firent, qui une bibliographie, qui un brainstorming ; d'autres ignorèrent le sujet en réalisant parfois que leurs activités comportaient comme une dose de… déni !

Gérald Bronner et Etienne Klein introduisirent les rencontres. Selon Bronner, la perception des risques est bouleversée par la dérégulation du marché de l'information imposée par internet ; elle produit une démagogie cognitive. Ce marché devenu cacophonique produit des effets pervers : cadrage de l'information, surestimation des très faibles probabilités, fantasmes et amplifications de certains risques, déséquilibre entre les coûts pertes-bénéfices (vaccins)… Ainsi, la surestimation des événements à très faible probabilité, confirmée par des expériences en psychologie expérimentale, donne la priorité aux lanceurs d'alertes négatives sur les publications scientifiques ; les risques rares font plus de buzz que les risques avérés (inondations vs maladies cardiovasculaires) et nos cerveaux sont plus attentifs aux mauvaises nouvelles qui foisonnent sur internet. Ceci entraîne un traitement irrationnel du risque et de fait, notre esprit est aveugle quant aux coûts de son inaction ; cette cacophonie détourne notre attention de ce qui la mériterait (vaccination, consommation de sucre et obésité). Et finalement de souligner qu'il existe désormais un danger démocratique venant de nous-mêmes, d'autocontrôle permanent et de jugements, d'hystérisation des commentaires, de polarisation des points de vue.

Etienne Klein proposa une réflexion historique et philosophique sur « progrès » vs « innovation ». Quand nos sociétés croyaient au progrès, le temps était considéré comme constructeur et permettait de dessiner le futur grâce à une philosophie de l'Histoire. Aujourd'hui, le mot progrès a disparu, supplanté par le mot innovation. Désormais le temps est considéré comme destructeur, il faut donc innover pour compenser la détérioration du monde. Notre rapport au risque en est bouleversé et le futur est désormais colonisé par les fantasmes. Les principes remplacent les valeurs. Mais les premiers ne se discutent pas, alors que les secondes dépendent de leurs évaluateurs : aucun consensus ne peut donc être atteint, ce qui favorise la procrastination. La Science qui a remplacé le Religieux comme fondement de notre société est contestée, marginalisée d'autant que nous gérons nos connaissances comme des croyances ; comme si la ligne de démarcation entre le vrai et le faux était poreuse ! La recherche c'est le doute, pas la science. Le désir de véracité entraîne un déni de vérité, il installe un esprit critique généralisé et génère des théories du complot (B. Williams). Et Klein de conclure avec Einstein « Il n'existe pas de chemin qui mène de ce qui est à ce qui doit être ».

Bonne lecture et merci au comité de programme des rencontres et à sa présidente Myriam Merad !

**Denis MARTY**
*Président de la commission « Communication » IMdR*

# Les Entretiens du risque 2017 :« le déni du risque de l'attitude individuelle à la gouvernance des organisations »

## Session 1 « les mécanismes du déni »

*Pour la première session consacrée aux mécanismes du déni du risque, le choix a été fait d'examiner le sujet par les deux extrémités : l'amont scientifique présenté par un neurophysiologiste, Alain Berthoz, explicitant le fait que le déni est une forme de protection de l'individu, et l'aval présenté par un industriel Pierrick Le Masne du groupe ACCOR expliquant comment ressortir du déni par la grande porte en se réformant.*

Pour aborder ce sujet qu'il considère comme un défi, **Alain Berthoz** a commencé par faire une étude bibliographique sur le sujet. Le mot déni est un terme très polysémique et il est donc préférable de parler au pluriel de dénis plutôt que du déni. Il est déjà possible de dire qu'il ne s'agit pas d'un déficit de la cognition, mais d'un mécanisme, volontaire ou involontaire, d'inhibition en vue de se protéger. Contrairement aux animaux, l'homme a conscience qu'il va mourir, ce qui l'amène dans certains cas à dénier le réel. Aussi, dans la littérature, on parle beaucoup de déni en médecine : déni de la maladie pour permettre au malade qui ne peut l'affronter de la supporter, méthamphétamine pour dénier les limites du corps utilisée par les armées allemandes pendant la dernière guerre, etc.

Dans ses propres recherches sur la simplexité, art des êtres vivants à résoudre des problèmes complexes à l'aide de solutions apparemment simples, Alain Berthoz a mis en lumière des mécanismes du cerveau reposant sur la sélection des informations utiles et l'inhibition des autres. Le cerveau nous donne sa représentation du monde et impose ses règles d'interprétation. C'est un émulateur qui utilise son interprétation du passé pour bâtir des boucles internes de raisonnement qui ne prennent que très peu d'informations de l'extérieur. C'est une démarche typiquement Bayésienne. Elle intègre une dimension affective, et si l'enfant utilise des heuristiques à partir des informations de l'extérieur, l'homme adulte se contente de 5% d'informations externes, le reste étant construit par des boucles internes au cerveau. Ainsi la pensée automatique intuitive supplante l'observation, ce qui permet de gagner en rapidité mais peut conduire à des erreurs d'interprétation. L'observation de malades et de traumatisés permet de mieux comprendre le fonctionnement du cerveau lorsqu'une fonctionnalité n'est plus disponible comme le choix des informations utiles à une décision.

Ainsi, on peut dire que les différentes formes de déni font intrinsèquement partie des outils de fonctionnement du cerveau humain. Mais le déni n'est malheureusement pas toujours protecteur des autres, ainsi c'est le déni de l'identité humaine de la victime qui permet au terroriste de supprimer sans émotion des innocents.

**Pierrick Le Masne** : « Le déni du risque, et après comment rebondir ? »À la table ronde du congrès Lambda-Mu de Saint Malo Pierrick Le Masne avait expliqué comment le groupe ACCOR avait vécu l'arrivée de nouveaux acteurs (Google, Airbnb) dans l'hôtellerie : déni marqué par un processus de ricanement, remise en cause des statistiques, puis sidération. Ici, il présente la réaction de ce grand groupe après ce choc.

En prenant du recul, la conscience de devoir évoluer qui était niée est apparue progressivement : « À la fin, tu es las de ce monde ancien » (citation d'Apollinaire qui résume son état d'esprit).

L'arrivée d'Internet a déplacé la chaine de valeur des grands groupes hôteliers au profit des acteurs du monde internet. Ainsi GOOGLE réalise le premier chiffre d'affaire mondial dans le domaine de l'hôtellerie (400G€), mais cette constatation a été longue à être acceptée et assimilée.

Face à cette situation, il a fallu trouver une nouvelle manière de réagir, car on est passé d'une guerre de tranchée à une guerre de mouvement. Les réponses à trouver étaient d'un type nouveau comme en métaphore guerrière on est passé du bouclier au glaive.

Dans un premier temps, il y a eu un bouillonnement de nouvelles actions sans stratégie définie. De nombreuses initiatives ont été lancées et notamment une prolifération de nouvelles chaines d'hôtels explorant de nouvelles cibles. Dans un deuxième temps, il a fallu trier, ce qui veut dire arrêter certaines actions, décision encore plus difficile à prendre que de les démarrer.

Beaucoup de mesures symboliques ont été prises : changement de siège avec installation dans des bureaux paysagés afin de trouver de nouvelles relations au sein des équipes ; grande attention à la recherche de sens pour le travail de chacun, prise de décision moins structurée et plus au fil de l'eau ; importance donnée au shadow comex constitué de milléniums et qui filtre les idées avant passage en comex ; recherche d'opportunités dans les collaborations avec les sociétés du numérique vues au départ comme des risques.

Aujourd'hui des orientations stratégiques à moyen terme (cinq ans) réapparaissent avec trois grands axes : hôtellerie, voyages et services, et l'esprit de l'entreprise a changé.

**Jean-Paul LANGLOIS**
*Président de la session 1*

# Session 2 « les individus face au déni des risques »

*Après avoir examiné les différents mécanismes neurologiques pouvant conduire au déni ainsi que les capacités des individus à rebondir après avoir pris conscience d'une position de déni, la session 2 a exploré deux autres types de mécanismes du déni : l'une au cours de situations de travail et/ou en société (session 2.1.), l'autre en faisant face à des situations de risques extrêmes (session 2.2.).*

La session 2.1 a été illustrée par l'exposé de certains facteurs de perception des risques :

*a) ceux d'ordre à la fois cognitif et culturel*

**François Daniellou** considère que les organisations sécrètent souvent en elles-mêmes du déni, alimenté par :

- une confiance excessive dans les calculs capables de définir l'occurrence des événements redoutés et une croyance en la pertinence et l'efficacité des procédures mises en place. De ce fait, il se crée une illusion du contrôle des activités fondée sur la conformité aux procédures, en déniant le fait que la sécurité dépend en grande partie du professionnalisme des acteurs,

- une disposition implicite au silence organisationnel, processus de défense permettant de se protéger des contradictions pouvant exister au sein de l'organisation. Citons deux exemples - la déviance aux règles devient « normale » (trop de règles tuent la règle) – la rétention des informations remontantes, car le management intermédiaire est « cisaillé » entre les orientations des directions générales et les réactions des opérateurs.

*b) ceux liés à des mécanismes de mise à distance de la douleur qui pourrait être ressentie*

En exposant le cas des conducteurs de métro face aux accidents graves de voyageurs, **Laura Cottard** confirme l'importance de ce silence individuel et organisationnel utilisé comme stratégie pour « mettre à distance » leur participation involontaire à la mort d'un voyageur. Les conducteurs mettent en place des modalités défensives qui sont de deux natures :

- un travail psychique complexe pour s'éviter de penser à cet événement, mais travail perpétuel, car nombreuses sont les occasions de confrontation. C'est un refus de penser s'apparentant à de la dénégation,

- un renvoi à la fatalité comme moyen de défense contre un sentiment de culpabilité, car ils sont soumis à enquête judiciaire.

Ce mécanisme de mise à distance adopté par les conducteurs est renforcé par le silence de l'institution qui affiche une grande pudeur sur ce sujet. La parole est discrète au cours des formations, ou à l'issue d'un accident. Il n'existe donc pas d'espace collectif pour débattre de cette situation.

Pour expliquer ces mécanismes de mise à distance de la douleur, les deux exposés pourraient se résumer en une phrase prononcée par François Daniellou : quand une situation est difficile à supporter et que l'on ne peut la changer, l'inconscient va modifier la perception de la situation pour la rendre supportable. En conclusion, les deux orateurs ont regretté l'absence d'espaces de discussions qui seraient un moyen de renforcer les pratiques du métier et d'acquérir une culture de sécurité, source de comportements plus sûrs.

La session 2.2. a exploré les facettes du déni du risque face à deux contextes de risque extrême :

*c) celle où l'individu cherche à se surpasser, à vivre ses propres limites dans le but de vaincre un environnement particulièrement hostile afin d'assurer sa mission,*

**Aude Villemain** évoque son expérience, vécue à la fois comme chercheur et comme équipière d'un raid polaire, (chargé de ravitailler tous les six mois une base franco-italienne basée dans l'Antarctique). Ce raid doit s'effectuer dans un délai d'acheminement très court et dans un environnement particulièrement hostile, les températures avoisinant les - 60 degrés. Elle note que pour les « raiders », le risque est banalisé. Ils sont conscients des difficultés à éviter, mais ne les considèrent que comme des problèmes à gérer. Dans leur univers, ils côtoient les risques (pannes, sorties de route, crevasses, gel du fuel…), sans utiliser de procédures, ne reçoivent pas de formation spéciale, mais ne comptent pas de morts.

Ce qui les guide, les mobilise, c'est l'appel du grand blanc, l'osmose avec l'environnement, l'exploit à accomplir, la virilité, la recherche de sensations auxquels il faut ajouter le sentiment de puissance, de liberté, d'absence de contraintes hiérarchiques, de réglementations et de procédures. Ils apprécient donc d'avoir à gérer des difficultés plutôt que d'avoir à appliquer des règles. Ayant vécu une situation critique engageant leur processus vital, ils s'en sont sortis grâce à leur autonomie, à l'acquisition d'une conscience collective partagée. Cela leur a permis de dépasser un possible enfermement dans leur processus habituel de pensée. Aussi, dans ces conditions extrêmes, le déni du risque s'est transformé en défi.

d) *et celle de surfeurs de haut niveau recherchant à la fois à maintenir leur entraînement et à capter des sensations malgré un environnement de requins.*

**Laurence Baillif** a abordé l'attitude de surfeurs confrontés au risque lié à la présence de requins dans la baie de Saint-Paul, sur l'île de La Réunion. Depuis 2011, plusieurs surfeurs ont été victimes d'attaques, dont certaines mortelles. Avec 18 attaques, la crise des requins-bouledogues devenait depuis cette date le cauchemar de l'île, mettant en péril les activités touristiques et économiques. Au début des attaques,

les baigneurs et surfeurs étaient considérés par certains habitants comme des imprudents responsables de leur sort, ce qui a conduit le préfet à interdire le surf. Mais, les activités nautiques devenant une tradition réunionnaise et le surf ayant acquis un haut niveau de notoriété permettant aux athlètes de figurer parmi les meilleurs de l'olympisme, la situation devenait dramatique. Comment accepter cette interdiction, si l'on veut devenir champion olympique ? Allait-on obliger les surfeurs à basculer dans le déni du risque, alors qu'ils restent conscients du risque et prêts à accepter des règles de prudence ? Plusieurs décisions ont alors été prises par les pouvoirs publics, visant à gérer les risques de sécurité pour permettre à l'île d'assurer la protection de l'environnement, la poursuite des activités touristiques et la pratique du sport. Une analyse cindynique a fait apparaître qu'aucun arbitrage n'avait été réalisé entre ces objectifs souvent contradictoires et devant impliquer tous les partenaires. Les décisions n'ayant pas été prises après une analyse plurielle et transversale, elles ne pouvaient qu'être propices à l'émergence de plusieurs formes de déni. Et pour les réduire, un mode de gestion discuté avec l'ensemble des acteurs impliqués a été proposé.

Chargée de faire le point sur l'ensemble de la journée, **Claude Hansen** a constaté que l'émotion était allée croissante depuis le matin, illustrant le fait que le déni était un moyen de lutter contre l'emprise de cette émotion sur une pensée rationnelle. Le déni de peur irrationnelle, lorsqu'il est refoulé, se transforme en anxiété ou en angoisse se manifestant par des symptômes. L'ouverture à l'idée de l'angoisse permet de se poser les questions sur ses effets : tentatives de déculpabilisation, tentation d'irresponsabilité et réflexion sur la morale civique dont nous avons besoin pour passer du déni au défi.

Les interventions du lendemain devaient permettre d'approfondir et de corriger ces points…

**Guy PLANCHETTE**
*Président de la session 2*

## Session 3 « les collectifs et les organisations face au déni du risque »

**Etienne Klein** a ouvert la journée avec un exposé intitulé « Perception des risques et innovation ». Il a proposé une réflexion historique et philosophique sur les mots « progrès » et « innovation ». Quand on croyait au progrès, le temps était considéré comme constructeur. Mais le mot progrès a disparu du langage politique et le mot innovation l'a définitivement supplanté. Désormais, le temps est considéré comme destructeur et il faut innover pour compenser la détérioration du monde.

**Marie-Valentine Florin**, Directrice de l'*International Risk Governance Center* (IRGC), Ecole Polytechnique Fédérale de Lausanne a présenté une conférence intitulée « La gouvernance des risques face au déni : une perspective internationale ». Elle a véritablement traité du déni du risque, certains participants estimant que sa présentation aurait pu servir de conférence introductive aux rencontres. Elle a cité des éléments contribuant à créer des situations de déni du risque : les biais cognitifs, les prises de risques induites par des biais dans la communication ou la visualisation, les conséquences des risques systémiques, les risques percevables mais non perçus ou perçus comme non-significatifs. L'innovation technologique réelle résulte d'un équilibre délicat entre des réglementations sur les risques qui favorisent ou contraignent l'innovation, des incitations économiques et l'acceptation publique. Marie-Valentine Florin pointe deux domaines à surveiller en se demandant s'il n'y a pas déni en ce qui les concerne : l'internet des objets et les véhicules autonomes. Elle conclut que, pour réconcilier les nécessités d'innovation technologique, de réduction du poids des réglementations et de gestion anticipative des risques, au-delà de la communication et de l'éducation, une approche de gouvernance des risques adaptative permet de répondre au besoin de flexibilité et d'anticiper, prévenir et gérer des situations de déni délibéré ou inconscient.

**Marianne Abramovici**, Maître de conférences à l'université de Paris-Est/Marne-la-Vallée a présenté « Les paradoxes de la gestion des risques en innovation ». Après avoir rappelé le concept de « destruction créatrice » de Schumpeter, elle a montré les deux visages du management de l'innovation : innovation incrémentale et innovation de rupture. La première limite la prise de risque tandis que la seconde assume le risque et donne toute sa dimension au processus de destruction créatrice. Le « *Design Thinking* » permet de penser l'usage et la méthode DKCP permet de penser la rupture.

**Patrick Couvreur**, Professeur à l'université Paris-Sud, membre de l'Académie des sciences mais aussi membre des académies des technologies, de médecine et de pharmacie, a présenté une communication sur les « Nanotechnologies pour la conception et le développement de nouveaux médicaments ». En associant un principe actif à un nano-vecteur, le franchissement de certaines barrières biologiques peut être facilité, le métabolisme et l'élimination du médicament freinés et sa distribution modifiée pour l'amener à son site d'action. Au-delà d'un exposé très scientifique difficile à suivre pour un profane en la matière, les échanges ont abordé le risque pris lors des essais cliniques à une époque où le moindre problème est médiatisé. Tout médicament a des effets secondaires et le professeur Couvreur a souligné que l'aspirine n'obtiendrait plus aujourd'hui l'autorisation de mise sur le marché.

**Roland Nussbaum**, Directeur de la Mission Risques Naturels (MRN) pour la Fédération Française de l'Assurance a présenté une communication « Déni des risques naturels et assurance : observations de praticiens ». Après avoir rappelé les rôles de la MRN et de l'Observatoire National des Risques Naturels (ONRN), Roland Nussbaum a présenté des exemples d'influence de l'assurance sur l'attitude individuelle face aux risques naturels et des exemples d'influence de l'assurance sur la gouvernance des organisations.

**Marie-Hélène Vergote**, Maître de conférences à l'université de Bourgogne, Agrosup Dijon, a relevé le défi de porter un regard cindynique sur la session 3. Je la cite : « Les présentations des intervenants de la matinée n'ont pas démenti l'adage selon lequel les acteurs qui travaillent sur les risques font des cindyniques comme Monsieur Jourdain : sans le savoir ! [...] Dans l'épistémologie cindynique, le déni figure bien parmi les problèmes récurrents. Même si le terme n'apparaît pas en tant que tel, le déni est présent sans ambiguïté. Ainsi, dans les systèmes sociotechniques, le déficit culturel dit « culture d'infaillibilité » figure parmi les dix déficits systémiques de base recensés comme sources de danger.[...] En matière d'appréhension des nouvelles technologies et innovations, du fait des inégalités qu'elles génèrent, la mobilisation du principe de précaution par leurs détracteurs révèle surtout l'absence d'espaces de discussion et plus particulièrement de négociations sur les valeurs. Ainsi, si les risques sociotechniques demeurent l'enjeu phare de la maîtrise des risques et sont de ce fait sortis du champ du déni, il faut admettre que le rapport d'aversion croissante au risque de nos sociétés est un fait… peut-être un danger ? Les cindyniques sont aussi là pour appréhender ce problème. »

**Philippe LE POAC**
*Président de la session 3*

## Session 4 « Aspects culturels dans la maîtrise des risques »

Cette session avait pour objectif de montrer comment un contexte culturel pouvait avoir une influence sur les attitudes de déni du risque.

Sur la base d'exemples relatifs aux inondations et aux feux de forêts dans la région PACA, **Christine Voiron**, géographe a montré que le concept de géo-gouvernance apportait une aide à l'appropriation d'une culture du risque. Cette approche permet d'élargir le champ de vision du risque, de le spatialiser et de stimuler les dynamiques futures de prise en compte des risques. Elle permet également de fournir des outils de médiation en rendant intelligible la complexité territoriale par le biais d'ateliers d'information et d'échanges avec la population à partir de cartes. Contribuant ainsi à la diffusion d'une culture de « terrain » et de « proximité », la géo-gouvernance rend le risque moins abstrait. En introduisant une démarche participative, elle permet aux parties prenantes d'un territoire d'avoir un regard concret et documenté sur le risque face à certaines attitudes de déni ou à d'autres trop rigides et excessives.

L'exemple des situations conflictuelles autour du projet de la nouvelle gare de Stuttgart illustre, lui, l'impact d'une culture sur le comportement des populations. En 2010, le projet a fait l'objet de manifestations massives de la part de citoyens « indignés », car jugé trop cher, trop compliqué,... Cependant, malgré une victoire du parti vert aux élections et une guerre d'expertise, un processus de dialogue lancé par le gouvernement aboutit à un vote citoyen en faveur du projet. **Félix Heidenreich** de l'Université de Stuttgart y voit l'influence d'une culture du « tout est possible » liée au succès de l'industrie locale et aux progrès technologiques déniant les risques afférents au projet.

En prenant l'analogie avec le nœud gordien, **Jean Caire** (Département Maîtrise des Risques Entreprise (MRE) de la RATP) nous renvoie à la perception du risque en cyber-sécurité dans les entreprises, oscillant entre l'exagération affichée par certaines sociétés de services informatiques et le déni de directions générales qui n'ont pas encore été piratées. Et pourtant les menaces sont multiples et les outils d'attaque sont mis quasi gracieusement à disposition de prédateurs anonymes qui peuvent, comme des exemples récents l'ont montré, porter des coups aux conséquences onéreuses, sinon fatales. Face au déni, il convient de modéliser le cyber-risque en distinguant ses composantes dont chacune devrait faire l'objet d'un traitement particulier en permettant d'impliquer et de responsabiliser les parties prenantes concernées dans leurs rôles respectifs.

Pour **Laurent Magne** de la direction des risques du groupe EDF, le déni du risque est un paradoxe quasi culturel présent dans toutes les organisations. Il est plus souvent la règle que l'exception : le risque ne serait-il pas alors de nier ce déni ?

Face à des facteurs de déni individuels et collectifs nombreux qui sont susceptibles d'être aggravés par les facteurs organisationnels, Laurent Magne propose plusieurs parades : un dispositif de gestion des risques incarné à tous les niveaux d'organisation de l'entreprise ; l'entretien d'une capacité de questionnement et l'ouverture au regard externe ; la définition de priorités claires, renforcées par l'exemplarité ; l'acceptation d'un contrôle indépendant effectif, reconnu et valorisé. Ces propositions, illustrées par de nombreux exemples, ont apporté à ces entretiens du risque 2017 une trame opérationnelle particulièrement appréciée.

**Jean-François RAFFOUX**
*Président de la session 4*

# Synthèse des rencontres

Après deux journées denses de partage de savoirs et d'expériences sur les mécanismes individuels, collectifs, organisationnels, voire sociétaux en jeu dans l'émergence et le maintien du déni des risques, de nombreux constats mettent en évidence l'intérêt porté au sujet.

Cette 6ème édition des Entretiens du risque a permis de rendre possible la création d'espace de partage des vécus et des pratiques en la matière et de rendre ainsi compte des freins et des bonnes pratiques culturelles et sectorielles (exemple : énergie, BTP, transport, etc.) visant à sortir de l'aveuglement volontaire ou involontaire et dont certaines formes peuvent être dangereuses pour les tiers, l'environnement et les biens.
Le déni des risques est souvent pointé comme une cause explicative de dysfonctionnement de la prévention des risques, pointant de ce fait les carences et les responsabilités individuelles ou collectives sur lesquelles il est supposé difficile d'agir. Bien que le déni des risques puisse avoir une fonction positive pour les individus et les organisations, il est sans conteste difficile en pratique d'apprécier le moment où il met en danger les Hommes, les organisations et les biens. La question portant sur le rôle et la fonction attendus des préventeurs, et par là même de la prévention des risques, apparaît alors comme au centre des questionnements.

À ce titre, si l'innovation doit permettre d'améliorer les conditions de vie des sociétés de manière durable, la prévention des risques n'a-t- elle pas pour fonction de penser ce qu'est un projet responsable de société ?

La difficulté à dégager une vision claire de ce qu'est un projet responsable pour une société rend difficile l'appréciation des conséquences de l'arbitrage conscient ou inconscient de ce qu'est un mal pour un bien (*e.g.* ignorer volontairement une catégorie de risque) et un bien pour un mal (*e.g.* se focaliser sur des risques négatifs en inhibant les capacités d'innovation sociales). Il est peut-être temps de repenser le cadre de l'éthique et de l'analytique de la prévention des risques en la matière.

Nos conférenciers ont ainsi été féconds en matière de partage de solutions et de propositions pragmatiques que nous pouvons résumer en ces termes :

- la nécessité de resituer le projet de prévention des risques dans son contexte. C'est en revenant au cadre et au cadrage de ce qui fait risque ainsi qu'à la connaissance de ce qui fait système qu'il est possible de sortir des clivages culturels et des illusions de métiers ou d'organisation
- la plus-value apportée par la caractérisation et l'explicitation des biais individuels, organisationnels et sociétaux (*e.g.* biais de responsabilité, des très faibles probabilités, de l'amplification sociale, la dépendance au ressentir, le mythe de toute puissance, le biais de complexité, l'effet du rex positif et négatif, etc.)
- le besoin de développer et de déployer des méthodologies et des approches pour penser le complexe par la simplexité (*e.g.* cindynique, géo-gouvernance, méthodologie IRGC, etc.)
- la nécessité de déployer de nouvelles formes de régulation des risques. L'hybridation des formes de régulation au sein des organisations et sur les territoires entre celles basées sur les règles et celles prônant le participatif et le délibératif
- la mise en place de conditions organisationnelles et de gouvernance permettant l'expression du courage institutionnel et d'œuvrer à expliciter les causes profondes du déni organisationnel, de la censure dont l'auto-censure. Le travail sur la mémoire et la culture et la mise en perspective historique des leçons des accidents offrent des perspectives de recherche et opérationnelles qui ne manqueront pas d'être fructueuses.

Plus largement, nous devons œuvrer à requestionner les limites de nos paradigmes et de nos concepts en matière de maîtrise des risques pour faire face aux nouveaux défis qui se présentent à nous en vue d'accompagner un déploiement responsable des technologies. Le prochain congrès Lambda Mu s'inscrit dans cette perspective.

**Myriam MERAD**
*Présidente du comité de programme*

# Systèmes socio-techniques et terrorisme : le face à face !

## Conférence donnée par Jean-Louis NICOLET le 6 février

Depuis 1970, le terrorisme frappe et provoque morts, blessés et dégâts considérables à travers le monde. Selon le recensement établi par le « *National Consortium for the Study of Terrorism* » plus de 150 000 actes de terrorismes ont été commis au cours de ces 46 dernières années dans le monde. La courbe de la figure n°1 montre l'évolution de ce phénomène ; La figure n°2 donne l'évolution du nombre de morts et de blessés par an dans le monde au cours de cette même période ; La figure n°3 montre l'évolution du nombre d'actes de terrorisme commis par Al Qaïda et par Daech (EI).

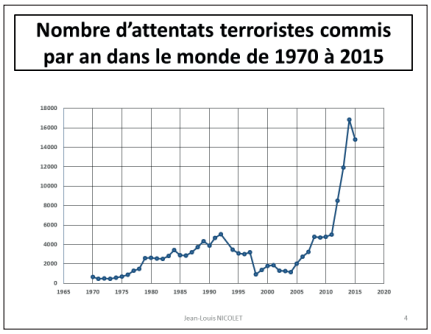


*Fig. 1*

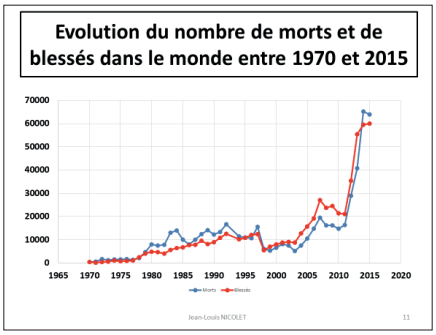


*Fig. 2*

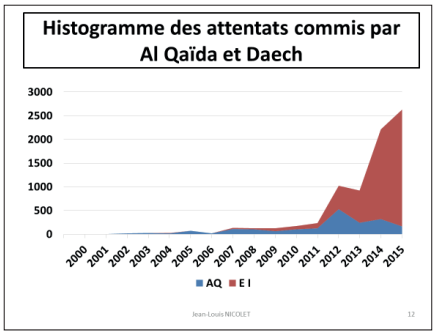


*Fig. 3*

Les cibles publiques c'est-à-dire des systèmes ouverts sont touchées en priorité. Pensons aux attentats de Madrid, de Londres, du Bataclan, de Nice… En moins de quinze ans nous sommes passés d'un terrorisme importé à celui d'une implantation locale, d'une structure de type Al-Qaïda à une « ubérisation » micro cellulaire du type Daech. L'accroissement exponentiel du risque qualifié de « terroriste », à multiples facettes, doit nous amener à réfléchir à la sûreté et la sécurité des systèmes socio-techniques que nous concevons et exploitons au quotidien afin qu'ils soient à même de résister aux attaques de deux nouveaux acteurs que sont **les Terroristes** et, pire, les **Janus**.

Pour décrire les scénarios auxquels nous allons avoir à faire face, Jean Louis Nicolet a retenu trois catastrophes survenues à un même système socio-technique, le transport aérien.

**La chute du « Rio – Paris ».** Il est 2 h du matin. Dans le cockpit, le second copilote prend la place du commandant qui vient de quitter le cockpit pour se reposer. L'avion approche d'une zone de forte perturbation. À 2 h et 10 mn le pilote automatique de l'appareil se désengage. Après quelques secondes d'étonnement, le copilote annonce « j'ai les commandes ». Pendant plusieurs minutes il va s'efforcer de stabiliser l'appareil qui oscille de droite à gauche, en tirant sur le manche pour prendre de la hauteur et passer au-dessus de la perturbation. Concentré sur le pilotage de l'avion, il a du mal à comprendre pourquoi les ordinateurs se sont brusquement arrêtés. N'arrivant pas à stabiliser l'avion, les deux pilotes réveillent le commandant qui les rejoint aussitôt. Pendant plusieurs minutes les trois hommes vont essayer de comprendre ce qui se passe afin de rétablir la situation, mais en vain. Après une chute de 35 000 pieds, l'Airbus A 330-203 s'écrase dans l'Atlantique avec ses 258 occupants. La séquence accidentelle a durée 4 mn et 28 s. Le dépouillement des boîtes noires montrera que de nombreuses causes matérielles, informationnelles, humaines sont à l'origine du drame, à savoir notamment le givrage des trois tubes Pitot, des erreurs de diagnostic, une ergonomie peu adaptée, une formation insuffisante… Pendant les quelques minutes qu'a duré cette séquence accidentelle, l'équipage a tout fait pour rétablir la situation. Leur seul objectif était de poursuivre leur route et arriver sain et sauf à destination. Aucun d'entre eux n'a voulu que l'avion décroche pour aller s'abîmer dans les flots. Fondamentalement ils étaient tous les **Amis du système**.

**L'attentat du 11 septembre 2001.** Depuis deux ans, quinze hommes préparent aux Etats-Unis, dans le plus grand anonymat, ce qui va être le plus incroyable attentat commis jusque-là. Ce matin-là, les quatre équipes qui se sont rendues séparément sur les trois aéroports choisis montent à bord de leurs vols respectifs et rejoignent leurs sièges comme des passagers normaux. Quelques minutes après le décollage de chaque appareil, ils prennent en otages les passagers, maîtrisent et tuent les pilotes et coupent les transpondeurs. Seuls maîtres à bord, ils changent de cap et se dirigent sur

leurs cibles respectives : les Twins, le Pentagone et la Maison Blanche ou le Congrès. Seules trois équipes les atteindront : les deux tours du World Trade Center et une aile du Pentagone. La quatrième cible ne sera pas atteinte du fait de la révolte des passagers, ayant conduit au crash de l'appareil. Bilan : 2 900 morts, 6 000 blessés, 93 pays concernés. Contrairement aux pilotes du « Rio – Paris » les quinze hommes montés à bord des quatre appareils ne sont pas les amis du système, mais des terroristes. Leur but n'est pas de conduire en toute sécurité les passagers à destination. Leur seul objectif est d'atteindre et de détruire les cibles désignées par Ben Laden, le chef d'Al Qaïda. Mais à y regarder de plus près, force est de constater que dans tout le système aérien (aéroports, tours de contrôle, procédures, dispositif d'interception de vols anormaux…) une seule chose a changé : **l'objectif que les quatre pilotes ont en tête**. Ce changement d'objectif va transformer les quatre avions, systèmes sûrs, pratiques, confortables, rapides en des armes redoutables. Ce nouvel acteur, **le Terroriste, devient l'ennemi des systèmes socio-techniques** que nous concevons et exploitons pour nos besoins quotidiens car il cherche à les détruire de l'extérieur ou en y entrant par infraction ou par ruse. À la suite de ces événements dramatiques, les systèmes de protection des postes de pilotage ont été repensés pour éviter toute intrusion de terroristes ou d'hommes mal intentionnés. Des procédures de contrôle des passagers et des bagages ont été mises en place pour éviter que des engins explosifs ne soient introduits à bord des appareils. Certains systèmes de défense en profondeur ont été revus et corrigés.

**Le crash du vol de la Germanwings dans les Alpes.** Au cours du vol Barcelone-Düsseldorf, le copilote arrache l'avion de la piste. Il est 9 h. Le commandant assure les communications avec le centre de contrôle de Marseille. À 9 h 30 mn 08 s le commandant qui a un besoin pressant demande au copilote de prendre en charge les communications avec Marseille. Il se lève, déverrouille la porte et sort. Aussitôt le copilote prend la place du commandant et ferme la porte avec le verrou de sécurité. Dorénavant plus personne ne pourra entrer dans le cockpit, car le verrou ne peut être enlevé que de l'intérieur. C'est l'arme de défense ultime face aux terroristes. À 9 h 30 mn 53 s le copilote, resté seul dans le cockpit, modifie la consigne relative à l'altitude de l'avion. De 38 000 pieds, il la ramène à 100. Le dépouillement des boîtes noires, après le crash, montrera qu'il avait simulé cette manœuvre lors du vol aller Düsseldorf – Barcelone. Quelques instants plus tard, l'avion commence à descendre et le régime des moteurs à diminuer. À 9 h 33 mn 47 s le contrôle de Marseille voyant l'avion à une altitude de 30 000 pieds et continuant à descendre essaye d'entrer en contact avec l'équipage, mais le copilote ne répond pas. À 9 h 34 mn 31 s, le commandant de retour des toilettes, demande l'accès au poste de pilotage mais ne reçoit pas de réponse du copilote. Toutes les tentatives pour ouvrir la porte et accéder au cockpit seront vaines. Jusqu'au crash final, le copilote restera enfermé, seul dans le cockpit, pilotant son suicide et entraînant volontairement dans la mort l'équipage et tous les passagers, soit cent cinquante personnes. À 9 h 49 mn 30 s l'avion explose au contact du sol. Nous sommes là face à notre troisième acteur que nous avons appelé Janus, à l'image du dieu romain. Dans un premier temps, il est **l'Ami du système** qu'il connaît donc parfaitement. Puis un jour, pour une raison ou une autre, médicale comme ici, idéologique, il bascule, il se radicalise… Il devient alors **l'Ennemi du système** et va décider de le détruire avec une très grande efficacité, car le maîtrisant parfaitement.

L'apparition de ces deux derniers acteurs, **le Terroriste** et **le Janus,** rend la plupart de nos systèmes socio-techniques vulnérables, car la plupart des systèmes de défense en profondeur mis en place ont généralement été conçus pour faire face aux défaillances non volontaires des Amis du système. De plus comme nous l'avons vu, avec le crash de la Germanwings, un système de défense en profondeur efficace pour lutter contre des terroristes peut s'avérer une arme efficace à la disposition d'un Janus déterminé. Une nécessité s'impose : nous devons revoir dans leur ensemble tous les systèmes de défense en profondeur mis en place sur nos sites industriels, sur nos systèmes socio-techniques, qu'ils soient ouverts ou fermés, publics ou privés mais avec un triple regard : celui de **l'Ami du système, du Terroriste et du Janus.** Puis en fonction des risques mis en évidence, prendre les décisions qui s'imposent. Tout incident, toute séquence accidentelle devra aussi faire l'objet de ce triple regard.

Après un large échange entre participants, l'IMdR envisage de créer un groupe de travail pour mieux appréhender les risques que ces deux derniers acteurs peuvent faire courir à la plupart de nos systèmes socio-techniques.

---

*"Systèmes socio-techniques et terrorisme : le face à face ou l'Ami, l'Ennemi et le Janus"*
**Jean-Louis NICOLET** - Editions L'Harmattan, 2017, 298 p. - ISBN : 978-2-343-12557-2

# Le programme 2018 - 2019 des projets IMdR au service des entreprises

Cela fait de nombreuses années que l'IMdR réalise des projets où les efforts humains et financiers sont mutualisés. Ces projets sont en outre une opportunité d'échanges entre grandes entreprises de secteurs industriels différents, préoccupés par les mêmes problèmes de maîtrise des risques et de sûreté de fonctionnement.

Cette structure de projet (que nous devons au CNES et qui a été perfectionnée au début des années 2000 grâce aux apports du CEA, d'EDF, du JRC Ispra et de Renault) est très populaire, très efficace, et on peut affirmer que la plupart des projets (plus d'une centaine à ce jour, y compris les projets européens) ont généralement donné satisfaction aux souscripteurs. Les projets les plus populaires sont sans aucun doute les projets « avancés », les applications des nouvelles méthodes à des données de souscripteurs ou les états de l'art. On peut aussi signaler que parmi les bénéfices pour les entreprises, les échanges, le *benchmarking*, le « débroussaillage » de sujets nouveaux sont des points importants que les grandes entreprises nous encouragent à poursuivre. Les meilleurs projets sont ceux qui sont construits par nos groupes de travail et de réflexion (GTR). Ils sont proches des préoccupations des entreprises. Ils sont plus faciles à initier car l'accès aux souscripteurs potentiels est direct.

Aujourd'hui l'innovation est considérée comme essentielle pour la survie des entreprises. Les projets proposés par l'IMdR pour les prochaines années vont dans ce sens. Ils proposent des orientations pour faire mieux en maîtrise des risques et en sûreté de fonctionnement. Notre programme s'appuie sur les réflexions de nos GTR et sur les résultats de nos projets passés, sur nos journées d'échanges et sur nos congrès (λμ et Entretiens du risque). Nous pouvons proposer cette année **un programme de projets 2018-2019 cohérent** que l'on peut découper en quatre grandes classes :

- généralités et concepts,
- modélisation et propagation des incertitudes,
- analyse et traitement des données incertaines,
- aide à la décision en contexte incertain.

Notre programme répond à des enjeux industriels, à des besoins opérationnels identifiés. Il est volontairement innovant, tout en privilégiant l'application sur des cas réels. Nous espérons qu'il vous conviendra et que vous le soutiendrez, nombreux, en souscrivant aux différentes propositions.

**Généralités et concepts**

Le premier concept est le déni du risque. On peut dénier le risque, c'est-à-dire le refuser comme vrai ou possible pour différentes raisons: parce que cela contrarie nos objectifs, parce que sa probabilité est infinitésimale, parce que nous ne le percevons pas comme étant un risque, parce que nous prenons sciemment le risque pour l'exploit ou la compétitivité… Ce point a été traité dans le cadre des Entretiens du risque 2017 (Merad *et al*, 2017).

Cette réflexion nous oblige à étudier plus profondément les concepts de vulnérabilité par la fiche FP7 (FP = Fiche Projet) *« Recherches sur le concept de vulnérabilité relatif aux systèmes et ouvrages socio-techniques »* : Quelle(s) définition(s) ? Quelles vulnérabilités : physique, matérielle, sociale, économique, démographique… ? Quels sont les situations à risque, leurs enjeux, l'obligation et la capacité de résilience, les facteurs d'influence ? Les études existantes relatives au risque sismique sont certainement un bon point de départ.

La résilience quantifiée sur la base d'une analyse de risque quantitative est à la mode. Dans certains pays (Etats-Unis, Royaume Uni) des études sont développées (Barker Kash *et al*, 2017 ; Linkov, 2017). En Europe un groupe de réflexion se constitue. Il est vrai qu'actuellement les décideurs se mobilisent sur l'après-événement. Il ne s'agit plus seulement de s'intéresser à la gestion de crise, mais bien d'adapter, d'anticiper les effets de l'évènement indésirable, de restituer et de retrouver l'état initial avant l'événement fâcheux, voire un état amélioré. La fiche projet FP11 *« Méthodes de caractérisation et de quantification de la résilience - Etat de l'art »* a pour objectif de définir les différentes notions apparaissant dans la problématique de la résilience des systèmes socio-techniques, de faire l'état des travaux actuels des outils existants et des applications traitées à ce jour. Ces fiches FP7 et FP11 pourraient se voir fusionnées dans un plus grand projet.

Un autre sujet concerne la différence de traitement entre un évènement interne (généralement traitée de façon sévère) et une agression naturelle extrême, « mieux » acceptée (IMdR, 2016 ; Dube *et al*, 2017). C'est ce que propose la fiche FP9 *« Identification des différences de traitement des événements internes, agressions internes et agressions naturelles extrêmes, lors de l'évaluation du niveau de risque d'une installation industrielle »*. Il s'agit de formaliser le processus de traitement, de caractériser les différences de traitement des évènements internes et des

agressions externes, d'examiner leur prise en compte dans les processus de décision et bien sûr de traiter un exemple relatif à une agression naturelle extrême.

**Modélisation et propagation des incertitudes**

Les réseaux probabilistes nous semblent un outil d'avenir. Les réseaux bayésiens ont déjà démontré leur intérêt par leur intégration des incertitudes et leur structure « base de connaissances », et se développent dans de nombreux domaines de la maîtrise des risques (prospective, diagnostic, pronostic, analyse de dégradation, maintenance, aide à la décision, analyse de risque,…). Ces méthodes de réseaux probabilistes (réseaux bayésiens, crédaux, évidentiels (VBS, *Valuation Based Systems*),…) se sont développées à partir des années 1990 et nous paraissent séduisantes, notamment parce qu'elles sont supportées par une représentation graphique, qu'elles sont adaptées au contexte d'incertitude, qu'elles généralisent des méthodes utilisées couramment par l'ingénieur ou le chercheur. La fiche FP5 *« Représenter et propager l'incertitude à l'aide de réseaux »* propose un état de l'art et des applications démonstratives dans trois domaines : l'analyse de risque, la fiabilité multi-états et le facteur humain.

De nombreux progiciels de traitement des incertitudes sont maintenant présents, libres d'accès ou commerciaux. Mais que valent-ils ? La fiche FP8 *« Comparaison de logiciels de traitement des incertitudes »* propose une comparaison de ces progiciels, d'une part de leurs descriptifs, d'autre part d'une comparaison des résultats obtenus par le traitement de deux exemples industriels par ces progiciels (dont l'un est analytique). Cette comparaison ne peut qu'être utile pour donner une appréciation de la qualité et de la convivialité, mais surtout pour mettre en évidence les éventuels points faibles et les perspectives de R&D.

Une dernière fiche projet concernant les signatures sera prochainement proposée. La signature d'un système cohérent à n composants ayant des durées de vie indépendantes et identiquement distribuée (iid) est un vecteur dont la composante i est la probabilité P (T=Xi : n) où T est le temps à la défaillance du système et Xi la durée de vie du composant i (Samaniego, 2017). Hormis la conférence (Marichal, Mathonet, Paroissin, 2017), à notre connaissance, peu de publications proviennent de nos universitaires ou de nos industriels. Il nous parait important de se pencher sur ce concept dont les applications en ingénierie semblent multiples : comparer différentes conceptions, tester l'utilité de redondances, détecter l'éventuel vieillissement d'un système. Ce concept semble bien adapté aux systèmes électroniques, au secteur de l'automobile. D'après les documents publiés, le concept de signatures est utile pour tout système où la fiabilité est un enjeu important.

**Analyse et traitement des données incertaines**

Le projet P17-3 « Rénovation du site internet FIDES » est déjà en cours. Il consiste à rénover et actualiser les fonctions du logiciel FIDES, facilitant l'accès aux données de fiabilité électronique et leur traitement.

À la suite du projet HUMS (*Health and Usage Monitoring Systems* ; IMdR, 2017), on peut penser que le retour d'expérience sera profondément impacté. On va passer d'une période au trop peu de données à une période de trop plein de données. Ceci va bouleverser tous les usages en aval de la collecte des données de retour d'expérience et en particulier l'analyse de fiabilité. La fiche projet FP 10 *« Big data in reliability »* se propose d'évaluer l'impact sur le retour d'expérience, en particulier sur l'analyse de la qualité des données (leur justesse et leur pertinence), mais aussi l'impact sur les méthodes. Inévitablement les défaillances devraient décroître, les données seront essentiellement des données de dégradation qu'il conviendra d'analyser. Les modèles de sûreté de fonctionnement en aval (les modèles systèmes) vont eux aussi être impactés. Dans un premier temps, la fiche projet se limite à l'estimation de la fiabilité. Il conviendra d'examiner l'impact du *big data* sur le processus d'analyse des dégradations et des défaillances et l'impact sur les compétences à mettre en œuvre. Cette fiche projet a déjà le nombre requis de souscripteurs. Le projet est donc lancé. Son cahier des charges est en cours de rédaction.

Dans l'éventualité où ce projet ne pourra pas évoquer l'analyse de dégradation, une fiche de projet spécifique sur *l' « analyse de dégradation et modélisation d'une cinétique »* sera rédigée. Elle sera centrée sur le traitement des données de dégradation, leur analyse, les modèles permettant d'estimer une cinétique : modèles physiques, régression, processus gamma, processus Wiener,…) (Mercier, 2017; Giorgio *et al*, 2017), et des exemples applicatifs liés à la maintenance préventive.

Une journée scientifique sur la *cybersécurité* est en préparation. Elle sera organisée en 2018. Le congrès λμ21 de Reims (octobre 2018) sera focalisé sur la transformation numérique.

Le retour d'expérience textuel est de plus en plus utilisé pour l'analyse de défaillance et pour l'analyse des situations d'incident- accident. Toute donnée est précieuse et les textes associés aux données structurées du retour d'expérience sont riches d'enseignements. On ne peut plus négliger cette information essentielle. La fiche FP12 *« Méthodes statistiques de traitement et d'interprétation d'un retour d'expérience en langage naturel »* rédigée sur la base des travaux (Blatter, Raynal, 2016 ; Tanguy, 2017; Tissot, 2017) se propose d'étudier l'apport des méthodes statistiques, notamment les méthodes de sémantique latente (LSA : *Latent Semantic Analysis* ; LSI : *Latent Semantic Indexation*), le *topic modeling*, l'analyse distributionnelle (*word embeddings*, ou

plongements lexicaux), au traitement et à l'interprétation du retour d'expérience. En particulier l'apport aux experts de retour d'expérience et aux opérationnels devra être évalué.

**Aide à la décision dans un contexte incertain**

Le projet P17-2 *« Comprendre le jugement et la perception des risques dans la prise de décision : comprendre le choix des individus ou des collectifs confrontés à des situations de risque »* est d'ores et déjà lancé. Le cahier des charges est rédigé. Il n'est guère trop tard pour souscrire. Deux contextes structurent ce projet : le comportement individuel de l'expert - ingénieur (comment va-t-il permettre de construire une décision collective ?), puis la perception collective (comment se construit-elle ?).

La journée scientifique *« Gestion des actifs industriels et management de leur fiabilité »* (IMdR, 2017) est très importante. Elle se situe dans le cadre de la maintenance prévisionnelle, de l'élaboration et de l'utilisation de la norme ISO 55000 relative à l'*asset management*. Cette journée a fait le lien avec les approches technico-économiques en sûreté de fonctionnement (coût global, soutien logistique, gestion du cycle de vie, *Risk Informed Asset Management*, *big data* en fiabilité et en maintenance, maintenance prévisionnelle).

Enfin une fiche projet FP13 *« Guide pratique d'orientation pour l'application des normes actuelles de management des risques et de sûreté de fonctionnement »* s'intéresse aux nombreuses normes existantes en maîtrise des risques et sûreté de fonctionnement. L'objectif est de permettre de disposer d'un outil permettant :

- d'avoir une connaissance des (principales) normes en vigueur : description, appréciation et impact de l'application pour les organisations,
- de connaître les tendances pour préparer le futur dans les différents domaines de la sûreté de fonctionnement (y compris la sécurité) et du management des risques.

Cette proposition a pour objectif premier d'actualiser les résultats d'un précédent projet et de fournir une approche globale pour inclure le management des risques. Ce projet permettra de donner une vision globale sur les normes (aspect cartographie) et de fournir un guide opérationnel pour la constitution d'un référentiel normatif d'une organisation.

**André LANNOY**

***Références***


- Barker Kash, Morshedlou Nazanin, Sansavini Giovanni (2017), *Trading off vulnerability and recoverability in network resilience*, MMR 2017, Grenoble, juillet 2017.

- Blatter Christian, Raynal Céline (2016), *Méthodes d'analyse textuelle pour l'interprétation des rex humain, organisationnel et technique*, Congrès λμ 19, Saint-Malo, 21-23 octobre 2014.

- Dube D., Parry G., Lewis S., True D., Ferrante F., Chapman J., (2017), *Enhanced guide on integrated risk informed decision making*, 2017 International Topical Meeting on PSA and Analysis (PSA 2017), September 2017.

- EPRI (2015), 3002003116 – *An Approach to Risk Aggregation for Risk-Informed Decision Making*, 29 April, 2015, www.epri.com

- Eurocodes (conception et dimensionnement des structures) – EN 1990 à EN 1999.

- Giorgio M., Mele A., Pulcini G. (2017), *A noisy gamma degradation process with degradation dependent non-gaussian measurement error*, MMR 2017, Grenoble, juillet 2017.

- IMdR (2016), Projet IMdR P14-1, *Méthodes de traitement des risques associés aux événements internes et aux agressions naturelles extrêmes*, janvier 2016.

- IMdR (2017), Projet IMdR P15-2, *HUMS (Health and Usage Monitoring Systems)*, mai 2017.

- ISO 55000 : 2014, *Gestion d'actifs – Aperçu général, principes et terminologie*, janvier 2014.

- Jouniaux Pierre, Dechy Nicolas *et al* (2016), *Détection, pertinence et amplification des signaux faibles dans le traitement du retour d'expérience*, Congrès λμ 19, Saint-Malo, 21-23 octobre 2014.

- Linkov Igor (2017), *The risk of not being resilient*, journée IMdR du 11 avril 2017, ENGREF, Paris.

- Marichal J-L, Mathonet P., Paroissin C. (2017), *Probability signatures of multistate systems made up of two-state components*, MMR 2017, Grenoble, juillet 2017.

- Merad Myriam *et al* (2017), *Le déni du risque: de l'attitude individuelle à la gouvernance des organisations*, 14 et 15 novembre 2017, Paris.

- Mercier S. (2017), *Probabilistic construction and properties of gamma processes and extensions*, MMR 2017, Grenoble, juillet 2017.

- Samaniego F.J., *System signatures: a 30- year perspective*, MMR 2017, Grenoble, juillet 2017.

- Tanguy Ludovic (2017), *Quel TAL pour le retour d'expérience? Réflexions sur les besoins et les solutions actuelles*, Journée IMdR (16 mai 2017), *Des méthodes aux applications du TAL dans le retour d'expérience*.

- Tissot Claire (2017), *Text mining sur des données d'accidentologie*, Journée IMdR (16 mai 2017), *Des méthodes aux applications du TAL dans le retour d'expérience*.

# Nous avons lu

## *«Qualité et Sécurité en Etablissement de Santé - Panorama de la gestion des risques en France – 2017»*
## Sous la direction d'Eric BERTRAND et Joël SCHLATTER
## LEH Edition, 2017


Cet ouvrage très complet a captivé notre attention alors que nous n'avons jamais été un professionnel de santé.

La première partie, la plus importante en nombre de pages (plus de 220), est intitulée « Thématiques ». Elle aborde tous les aspects de la qualité et de la sécurité dans les établissements de santé : les droits des patients, les outils de la gestion des risques au service du management médical, la perception des risques en établissement de santé et certification, la contribution de la qualité de vie au travail à la gestion des risques des établissements de soins, la vulnérabilité des professionnels de santé, les « événements indésirables graves », les risques épidémiques et biologiques en établissements de soins, l'accréditation pour les laboratoires de biologie médicale, la gestion du risque d'engagement de responsabilité civile médicale (point de vue du courtier d'assurance), la formation à la qualité et sécurité en matière de santé et de e-santé à l'échelle européenne.

Certains chapitres constituent des synthèses qui pourront servir de références bien au-delà des établissements de santé. Jean-François Bossu dans un chapitre « La systémique et le risque » promeut la pensée systémique et présente les mérites de l'ingénierie système. Les risques liés à la protection des données de santé sont détaillés dans le chapitre « Les risques du SI de santé » de Jean-François Goglin et le chapitre « Cybercriminalité des établissements de santé : mythe ou réalité ? » de Laure Zicry. Il est rappelé que le règlement général sur la protection des données (RGDP) entrera en vigueur le 24 mai 2018. Règlement européen et non directive, il s'appliquera uniformément dans l'ensemble des Etats membres de l'Union Européenne sans avoir à être transposé dans les droits nationaux.

Le Président de l'IMdR n'a pu qu'être sensible au chapitre « Du facteur humain aux cindyniques » dans lequel Sylvie Garandel présente des pistes développées dans le cadre du groupe de travail et de réflexion (GTR) de l'IMdR intitulé « Management des risques, cindyniques et nouvelles approches systémiques dans le secteur de la santé ».

La seconde partie, la plus courte (une centaine de pages) détaille les retours d'expérience en gestion des risques dans différents secteurs des établissements de santé : psychiatrie, endoscopie, gériatrie, radiologie et médecine nucléaire, pédiatrie, service d'urgence, transfusion sanguine, actes pharmaceutiques.

Au total, ce livre sera utile, bien entendu, pour tous les professionnels de la santé voire les professionnels du risque en général, mais pourra intéresser tout citoyen qui a déjà été ou qui sera fatalement, un jour ou l'autre, un patient.

**Philippe LE POAC**

Nous appelons l'attention de nos lecteurs qui travaillent à l'amélioration de la sécurité sur l'existence du magazine **HindSight** édité par l'organisme européen de contrôle aérien Eurocontrol. Cette revue destinée aux contrôleurs aériens (aiguilleurs du ciel) et pilotes reçoit régulièrement des articles des Pr Hollnagel et Dekker et du Dr Shorrock, pointures internationales en FH s'il en est ! Elle propose, depuis juin dernier, des articles écrits par des professionnels de santé dans différents pays européens, sur la simulation, le travail en équipe plurielle, la formation au travail en équipe dans la santé, l'analyse des évènements indésirables, etc. Des articles provenant d'autres domaines seront prochainement publiés. Vous pouvez recevoir gratuitement ce magazine (en anglais car il n'y a pas de version française) et consulter les articles sur **https://www.skybrary.aero/index.php/HindSight_-_EUROCONTROL**.

**IMdR - 12 avenue Raspail - 94250 Gentilly (RER : Gentilly)**
Tél. : 01 45 36 42 10 • Fax : 01 45 36 42 14 • E-mail : secretariat@imdr.eu • N° ISSN 1639-9706
**CODIT -** Centre d'Orientation, de Documentation et d'Information Technique :
Espace convivial où des animateurs vous renseignent et vous conseillent. Prenez RDV au 01 45 36 42 10
Directeur de la Publication : Philippe Le Poac - Directeur de la Communication : Denis Marty - Délégué Général : Jean-Pierre Petit
Conception et réalisation : Imprimerie ANQUETIL - www.imdr.eu - Webmaster : Ali ALJARF
**L'Institut pour la Maîtrise des Risques (IMdR)**
est une association Loi 1901 à but non lucratif, émanant de l'Institut Sûreté de Fonctionnement (ISdF) - Siret 443 923 719 00027