ATELIER 1
La mesure des risques majeurs au croisement de la résilience des systèmes, écologique et psychologique

Gilles TENEAU1
Docteur en sciences de gestions – CNAM SOGETI

Résumé

Les organisations évoluent dans un contexte de turbulences, de crises. La résilience se résume en l'art de rebondir, elle permet d'anticiper ou de répondre à la crise. Pour notre sujet qui traite de l'approche des risques opérationnels majeurs, nos observations portent sur la résilience individuelle, technique et écologique que nous croisons avec les facteurs de risques Pre-traumatiques, Péri-traumatiques et Post-traumatiques. La résilience constitue une forme bien précise de sécurité reposant sur les savoirs faire, la compétence et l'autonomie des acteurs des systèmes sociotechniques complexes. Nos recherches portent tant sur la résilience, la gestion des crises et l'analyse des risques dans les organisations, les systèmes, les éléments naturels. Nous proposons un scénario d'analyse de risques en 4 étapes (1) définition des classes de scénarios d'interruption, (2) outils et stratégies par classe de scénario, (3) analyse d'écart, (4) planification du projet. En conclusion, notre réflexion s'oriente vers une théorie générale de la résilience, qui prend en compte le cadre d'action de Hyogo, c'est-à-dire construire la résilience des nations et des communautés face aux catastrophes.

Mots-clés : résilience, risque, sécurité, crise, catastrophes, système

Abstract

The measurement of the major risks at the intersection of system resilience, ecological and psychological

Organisations evolve within a framework of turbulence and crisis. Resilience can be summarized as the art of bouncing back, making it possible to anticipate and respond to a crisis. Concerning our approach to dealing with major operational risks, our comments relate to individual, technical and ecological resilience that we cross with Pre-traumatic, Peri-traumatic and Post-traumatic risk factors. Resilience is a specific form of security based on the know-how, competence and autonomy of those involved in complex social-technical systems. Our research focuses on resilience, crises management, and risk analysis within organisations, systems and natural elements. We propose a risk analysis scenario in four steps (1) analysis of the classes of disruption scenarios (2) tools and strategies by classroom scenario (3) gap analysis (4) project planning. In conclusion, our thinking is moving towards a general theory of resilience which takes into account the Hyogo Framework, that is to say, building the resilience of nations and communities in the face of disaster.

Keywords : resilience, risk, safety, crisis, disaster, system

1. Des crises et des chocs

Les organisations sont mises à rude épreuve, (Shrivastava, 1993) elles évoluent dans un contexte de turbulences, de crises et de changements incessants. La stabilité côtoie l'instabilité, la sécurité et l'incertitude se conjuguent. Les évolutions et les ruptures rythment de plus en plus le quotidien des individus et des équipes. Les événements peuvent prendre des allures de crise et générer des chocs ; ils rendent les individus et les équipes hésitants sur la ligne de conduite à tenir. En situation de « choc » les individus et les organisations sont en recherche de repères (Ashforth, 1996). Partant de la survenance d'un choc ou d'un bouleversement au sein de l'organisation, nous allons examiner ce qui se produit, identifier les phases de rupture, observer le cycle de vie de l'organisation, apprécier les résistances face à un choc. La crise peut adopter des formes différentes : le choc, la tension ou la surprise (Kaes, 1979). Plusieurs formes de rebonds sont possibles en situation de crise : l'effondrement et la résilience[1]. Il y a un avant, et un après crise, un entre deux, (Sibony, 1993).

1.1. Risques majeurs

Nos travaux portent sur les risques majeurs qui sont des aléas se produisant dans des zones vulnérables affectant les activités humaines, technologiques, environnementales. Selon le conseil de l'Europe, le risque majeur consiste en une fréquence faible combinée à de nombreuses victimes, d'importants dégâts matériels ou des impacts significatifs sur l'environnement. Cette description inclut le risque naturel et les risques technologiques. La courbe de Farmer (1967), comporte 3 domaines, le premier domaine concerne les risques individuels de la vie quotidienne, le second domaine les risques moyens de temps en temps, le troisième domaine, les risques collectifs rares, ils ont une fréquence faible et une gravité élevée. La difficulté de gestion des risques majeurs est liée à l'imprévisibilité, cela étant du à une faible fréquence de la survenue d'un tel risque.

1.2. Application des risques majeurs à la résilience organisationnelle

Le concept de résilience organisationnelle est né d'un besoin des états et des organisations d'être mieux armé face aux perturbations qui affectent leur fonctionnement. En 2005, la conférence mondiale sur la prévention des catastrophes de l'Organisation des Nations Unies à Hyogo concrétise cette nouvelle tendance internationale. Son objectif concerne la mise en place de dispositifs pouvant accroître la résilience des collectivités et des institutions face aux risques. Par conséquent les décideurs, gestionnaires, patrons sont conduit à repenser leur manière de travailler et à développer une culture de la résilience au sein de leurs organisations. La résilience organisationnelle se compose de la résilience psychologique, de la résilience des systèmes et de la résilience écologique. Pour de plus amples informations concernant la résilience organisationnelle, nous invitons le lecteur à découvrir notre ouvrage[2].

1 Cyrulnik, B (un des premiers à travailler sur le sujet en France) définit la résilience comme « la capacité à réussir à vivre et à se développer de manière acceptable en dépit du stress ou d'une adversité qui comporte normalement le risque grave d'une issue négative ».

[2] Gilles Teneau et Guy Koninckx, La résilience organisationnelle, rebondir face aux turbulences, ed De Boeck, 2010

« *En 1973, Holling a introduit deux nouvelles définitions de la résilience. La première précise que la résistance aux perturbations et la vitesse de retour à un état d'équilibre servent à mesurer la résilience. Il la nomme résilience d'ingénierie. La seconde met l'accent sur des conditions de non-équilibre ou les perturbations risquent de modifier un système vers un autre état. Dans ce cas, la résilience se calcule par l'amplitude de la perturbation pouvant être absorbée avant que le système se restructure en quelque chose de nouveau. Il baptise celle-ci de résilience écologique.* » [3]

Selon le type de résilience et la gravité du choc, le système prend une orientation différente. Dans la résilience psychologique le choc est lié à un traumatisme, ce dernier permet à l'individu de rebondir. Dans la résilience des systèmes, lorsque le choc arrive, il n'y a pas de rebond envisagé, mais une continuité de l'activité. Dans la résilience écologique, que l'on relie aux catastrophes naturelles, lorsque le choc se présente, une autre orientation est proposée, le processus d'origine suit une route différente, il n'y a ni continuité d'activité, ni rebond.

Les risques psychologiques ou risques psychosociaux concernent les individus, ils sont envisagés au sein de la résilience psychologique (Cyrulnik, 1999 ; Vanistendael & Lecomte, 2000). Quelques exemples de ce type de menace : les camps de concentration, la canicule 2003, la maladie de la vache folle, les attentas du World Trade Center, la guerre du Viet Nam, etc …

Les risques sociotechniques concernent les catastrophes technologiques, ils sont envisagés au sein de la résilience des systèmes et de la résilience ingénierie (Weick, 1994 ; Holnagell & all, 2006 ; Amalberti, 2009). Quelques exemples de ce type de menace : Bhopal, 1984 ; Tchernobyl, 1986 ; Challenger, 1986 ; usine AZF Toulouse, 2001 ; Airbus A320 Sao Paulo, 2007, etc …

Les risques socio-environnementaux concernent les catastrophes naturelles, ils sont envisagés au sein de la résilience écologique (Holling, 1973 ; Batty, 2004 ; ICSU, 2002 ; Olson, 2004). Quelques exemples de ce type de menace : Tsunami en Asie, 2004 ; ouragan Katrina, 2005 ; cyclone Nargis en Birmanie, 2008 ; Xynthia en Vendée, 2010 ; séisme Haiti, 2010 ; Japon, séisme et tsunami, 2011, etc …

2. Faire face aux turbulences : apport de la résilience

[3] Therrien, M.-C. (2010) Stratégies de résilience et infrastructures essentielles, Télescope, vol. 16, n° 2, p. 154-171.

Le concept de « résilience » se trouve dans plusieurs disciplines. Nous nous limitons à quelques unes d'entre elles.

En physique, la résilience exprime le rapport de l'énergie cinétique absorbée nécessaire pour provoquer la rupture d'un métal, à la surface de la section brisée. La résilience, qui s'exprime en joules par cm², caractérise la résistance au choc. Capacité à vivre, à se développer, en surmontant les chocs traumatiques, l'adversité. (Le Petit Robert, édition 2002).

En informatique, la résilience concerne la qualité d'un système qui lui permet de fonctionner en dépit d'anomalies liées aux défauts d'un ou plusieurs éléments constitutifs.

En psychologie, il s'agit de la capacité à vivre, à réussir, à se développer en dépit de l'adversité. C'est une combinaison de force intérieure, d'appui de l'extérieur et d'apprentissage à partir de l'expérience acquise.

En écologie, la résilience exprime, d'une part la capacité de récupération ou de régénération d'un organisme ou d'une population, et d'autre part, l'aptitude d'un écosystème à se remettre plus ou moins vite d'une perturbation.

Lors d'une conférence consacrée à la survie des organismes vivants et l'adaptation des systèmes humains au changement et à l'agression, Pierre Bricage affirme : *« Tout organisme vivant est un système organisé indissociable de son milieu de survie. En permanence, tout être vivant doit reconstruire son organisation et recréer son autonomie, il est sans cesse dépendant de son environnement externe de survie dans lequel, il s'auto-régénère continuellement. Dans ce milieu, il puise de la matière, de l'énergie et de l'information, il est intégré au sein d'une chaîne alimentaire. Avant de pouvoir se survivre dans sa descendance, il doit d'abord rester en vie, survivre, en prolongeant son existence au-delà des événements insupportables qui peuvent entraîner sa disparition. »*[4]

La résilience écologique mesure le temps de retour à l'équilibre d'un système après une perturbation. La résilience devient équivalente à la notion de stabilité d'un système autour d'un point d'équilibre. Après une perturbation le système réagit au contraire de manière souvent positive, créatrice, grâce à de multiples changements et réajustements. En ce sens là, la résilience est la propriété d'un système qui conserve néanmoins la même trajectoire après une perturbation. Le système intègre des transformations en évoluant. Dans cette perspective le changement, et la perturbation qui le déclenche, ne sont pas nécessairement des traumatismes.[5] Les limites du paradigme, basé sur l'équilibre pour des systèmes ouverts, apparaissent. L'idée qu'il existe au contraire plusieurs situations possibles implique la possibilité pour un système de se situer loin de l'équilibre sans pour autant s'effondrer.

Dans le langage courant la définition se résume en quelques mots : « La résilience ou l'art de rebondir »

[4] Bricage P., La nature de la violence dans la nature, Faculté des Sciences – Sciences biologiques & Sciences Sanitaires et Sociales, à l'université de Pau, Conférence-débat, organisée par l'AFSCET à propos de la survie des organismes vivants, Groupe de travail systémique et biologie. Adaptation des systèmes humains au changement et à l'agression.

[5] Aschan-Leygonie Christina, Université de Lyon

On remarquera d'emblée l'importance des glissements sémantiques qui se sont opérés lors des passages d'un champ d'application à l'autre, et notamment l'éloignement par rapport à l'acception d'origine :

Premier élargissement : on passe d'une matière inerte et simple à un ensemble complexe ; d'une forme d'homéostasie permettant à la matière de retrouver sa forme originelle à un environnement dynamique où un nombre important de forces doit être maintenu dans un équilibre plus ou moins fragile en dehors duquel la structure se rompt ou éclate.

Second élargissement : là où la mécanique voit dans la résilience une capacité intrinsèque, on parle à présent de mécanismes d'autorégulation, de contre-forces tenues en réserves par le système pour refaire naître l'équilibre brisé. Plus généralement, on voit s'opérer un glissement de l'individu, à l'espèce (système formé par le regroupement d'individus semblables) puis à la société (ensemble d'espèces différentes).

2.1. Résilience des systèmes

Pour notre sujet qui a trait aux risques opérationnels nous traiterons de la résilience des systèmes. La particularité de la résilience des systèmes est qu'elle se préoccupe de la gestion des risques opérationnels dans une relation homme/machine. Tandis que la résilience organisationnelle se préoccupe de la gestion des risques psychosociaux, techniques et environnementaux. Nous préconisons d'intégrer à la résilience des systèmes les concepts de résilience psychologique et de résilience écologique.

La « *résilience des systèmes est la capacité intrinsèque d'un système* (sociotechnique) *à adapter son mode de fonctionnement avant, pendant ou après des changements et des perturbations de manière à ce qu'il maintienne les performances requises dans les conditions prévues aussi bien qu'imprévues* » (traduction d'après Hollnagel, 2006).

En parallèle des approches systémiques, Hollnagel, Woods et Leveson (2006) ont mis l'accent sur les conditions d'un meilleur couplage homme - machine, qui ferait considérer le risque lié aux systèmes plus par leur dynamique d'interaction que par les risques de défaillances des composantes isolées de ce système, machine d'un côté et homme de l'autre (Amalberti, 2009). Nous sommes dans une relation Homme/Machine, où la confiance est prioritairement attribuée à la machine. Les premiers efforts en matière de sécurité ont porté sur le développement de méthodes et outils visant à fiabiliser les composants techniques des systèmes. Leur mise en œuvre s'est traduite par une diminution très nette des accidents attribués aux défaillances techniques. Des accidents majeurs comme Three Miles Island (1979) ont fait prendre conscience des limites de ces méthodes de quantification des erreurs et de la nécessité de développer de nouveaux cadres de description visant à mieux appréhender la composante humaine dans sa dimension cognitive. Rapidement, l'objectif d'évitement total de l'erreur a été abandonné (irréaliste d'un simple point de vue théorique) et la sécurité s'est naturellement déplacée vers une perspective plus systémique (Reason, 1997 ; Rasmussen, 1991, 1999). La série d'accidents majeurs survenus entre 1985 et 1990 (Bhopal, 1984 ; Tchernobyl, 1986,…) au sein d'un éventail de technologies pourtant bien défendues, ont révélé que les causes de ces accidents pouvaient se situer au niveau des sphères managériales et organisationnelles des systèmes complexes et non pas uniquement au niveau où le travail est réalisé par les opérateurs. La multiplication récente d'accidents et de catastrophes a conduit les chercheurs à réfléchir à une autre approche de la sécurité des systèmes complexes articulée autour de la capacité d'une organisation à conserver ou à recouvrer rapidement un

état stable, lui permettant de poursuivre ses activités durant et après un accident majeur ou bien en présence de pressions continues et importantes (Wreathall, 2006).

Les catastrophes survenues à Bangkok, Sumatra, les îles Samoa en 2009, soulignent la nécessité de renforcer la préparation aux catastrophes, disent des experts, même si les progrès en gestion des risques sont indéniables, il n'en reste pas moins de nombreuses lacunes. D'après Terje Skavdal, chef du Bureau des Nations Unies pour la coordination des affaires humanitaires (OCHA) à Bangkok, les acteurs impliqués reconnaissent de plus en plus le rôle crucial de la préparation aux catastrophes. « *Les lacunes sont nombreuses. Certaines sont liées aux alertes précoces, il faudrait, par exemple, que les alertes précoces puissent être traduites dans des langues compréhensibles pour la population, et qu'elles soient transmises jusque dans les régions les plus reculées* », a indiqué l'expert en gestion des risques, Mr Skavdal [6]. En 2010, près d'un millier de personnes ont péri dans des catastrophes aériennes une statistique en augmentation par rapport à 2009. Ces données sont compilées par le cabinet spécialisé dans l'aéronautique Ascend. Au regard de ces catastrophes environnementales ou techniques il est important de réagir et de se demander pour quelle raison, les menaces, les risques, les dangers sont toujours aussi présents. Les grandes catastrophes industrielles, où la sécurité a souvent été négligée, conduisent à une remise en cause de la gestion ISR[7] (Investissement Socialement Responsable), dont les analystes n'ont pas toujours anticipés les risques. Les différentes catastrophes survenues récemment au Japon alimentent un débat sur la sécurité nucléaire et sur cette énergie. Sans évacuer la nécessité de ces discussions, une analyse de la relation entre activité humaine et ses effets sur la nature doivent également s'inviter aux réflexions. Surtout quand les solutions proposées sont principalement technologiques (Prade & all, 2005).

2.2. Sécurité observée

Il a été montré que la résilience des systèmes constituait une forme bien précise de sécurité reposant sur les savoirs faire, la compétence et l'autonomie des acteurs des systèmes sociotechniques complexes. Ainsi, la résilience constitue une forme de sécurité dite gérée (Sg) qui, associée à la sécurité dite prescriptive (Sp), (procédures, réglementations, normes, règles, etc.) complète l'équation de la sécurité observée au sein des systèmes (i.e. la sécurité que l'on peut mesurer par des données objectives comme le nombre d'accidents du travail, de maladies professionnelles, etc.) (Morel, 2007 ; Morel, Amalberti, Chauvin, 2009).

SécuritéObservée *= (Sp + Sg).*

D'un point de vue historique, la sécurisation des systèmes sociotechniques complexes a toujours été réalisée en favorisant la sécurité prescriptive. Cela a eu pour effet de réduire considérablement la composante adaptative de ces mêmes systèmes les rendant ainsi extrêmement rigides et par conséquent très peu adaptables à la survenue de perturbations importantes.

« *La sûreté de fonctionnement répond aux exigences de fiabilité du système particulièrement contraignantes dans les systèmes critiques (transports, espace, nucléaire…) souvent soumis à certification et aux exigences de disponibilité, mettant en jeu des propriétés de fiabilité et de maintenabilité intrinsèques au système, mais aussi d'efficacité de son système de maintien en*

[6] Terje Skavdal, chef du Bureau des Nations Unies pour la coordination des affaires humanitaires (OCHA) à Bangkok

[7] Se référer au code de transparence AFG-FIR pour les fonds ISR ouverts au public - janvier 2010

condition opérationnelle. La sécurité de fonctionnement n'est pas suffisante, du fait des comportements plus ou moins prévisibles de l'environnement. Il faut que le système soit sécurisé (au sens de son immunité) vis à vis des menaces accidentelles ou intentionnelles de l'environnement et qu'il soit capable d'assurer ses missions à un niveau acceptable de fonctionnalité, performance et sûreté en maîtrisant ou s'adaptant aux situations ou événements prévus ou imprévus. C'est ce qui a conduit au concept plus large de résilience des systèmes. La résilience des systèmes nécessite une approche système très large fortement intégrée à l'ensemble des activités d'ingénierie système, puis, après mise en service, à l'ensemble des activités d'exploitation et de maintien en condition opérationnelle. Elle rejoint ainsi le domaine de la maîtrise des risques systèmes. »[8]

Bien évidemment, nous devons nous interroger sur la réelle capacité des systèmes déjà ultra sûrs (et sécurisés par la prescription) à assumer un tel changement. Le retour en arrière est-il encore possible, sachant que tout a été mis en œuvre pour limiter, voire faire disparaître la résilience au sein de ces systèmes ?

3. Mise en œuvre d'une gestion des risques opérationnels

Le centre asiatique de réduction des catastrophes et le bureau pour la coordination des affaires humanitaire à l'ONU ont développé une approche stratégique de réduction des catastrophes. Cette approche est nommée Total Disaster Risk Management (TDRM). Les préconisations ci-dessous sont issues de cette approche, développée à son origine en Australie et Nouvelle-Zélande suite à de nouvelles normes de sécurité civile, depuis plusieurs pays l'ont adopté. Depuis 2009, l'ISO à publié une norme de gestion des risques, ISO 31000. Cette norme est une véritable démarche d'anticipation ; pour que cela soit efficace, il faut respecter les exigences de la norme. La norme ISO 31000 présente les différents risques possibles : risque au travail, risque sur l'environnement, risque sur la sécurité (Teneau, Ahanda, 2009). La gestion des risques opérationnels se gère comme un véritable projet. Le périmètre est large ; il touche l'entreprise, les différentes directions et les activités, institutions, associations en dehors de l'entreprise. Une fois le périmètre identifié, il est plus facile de se fixer les objectifs à atteindre.

Quels sont les risques que l'entreprise devra prendre en compte et cela à partir de la source du risque, jusqu'à son résultat (dégâts, pertes…). Des questions sont posées : Pourquoi cela peut-il arriver ? Quels sont les endroits à risques ? À quelles périodes ?… Il faut aussi que tout le monde comprenne le risque. Classer les risques, leur donner un poids, une importance, une priorité, est une nécessité. Ensuite il faudra prendre du recul par rapport au risque, et commencer à comprendre le risque, son cycle de vie, les interactions avec les autres risques qui sont directement ou indirectement rattachés au risque principal, le niveau de récurrence ; il faut faire le diagnostic du risque. On arrive alors à la qualification du risque par lui-même ; à cet effet, il faut avoir une base de connaissance des risques qui permet d'avoir des repères en termes d'évaluation. Cette évaluation permettra de prendre les bonnes décisions pour limiter les risques dans l'immédiat et pour le futur.

L'étape suivante est la correction du risque, un plan d'actions est décidé, l'entreprise est d'accord, une validation a été faite, et après avoir corrigé le risque, on va suivre un programme de surveillance afin d'être vigilant pour que le risque ne se reproduise plus. Un

[8] AFIS Association Française d'Ingénierie Système, http://www.afis.fr/nm-is/Pages/S%C3%BBret%C3%A9%20de%20fonctionnement/S%C3%BBret%C3%A9%20de%20fonctionnement.aspx

peu comme pour la norme ISO 9001:2000, on se doit de revoir, réactualiser le programme de surveillance qui fait partie intégrante du processus de management des risques.

La dernière étape est la communication et la consultation ; il ne faut pas les oublier, car elles permettent de renforcer l'esprit de groupe, d'échanger, de partager les actions, informations qui découlent du processus de management des risques.

« *En dépit de la résilience du système bancaire national, Bank Al-Maghrib met l'accent sur la nécessité de poursuivre les efforts entrepris en matière de gestion des risques face à la montée de certaines vulnérabilités. La Banque centrale, qui vient de publier son rapport sur « le contrôle, l'activité et les résultats des établissements de crédit » pour l'exercice 2010, souligne l'importance d'une gouvernance saine assignant aux établissements de crédit une stratégie et des objectifs bien définis.* »[9]

3.1. Proposition d'un scénario d'analyse de risques

Nous somme membre du HCFDC (Haut Comité Français pour la Défense Civile) et nous travaillons à la rédaction d'un rapport annuel 2011, concernant les risques et menaces exceptionnels. Ce rapport sera présenté au premier trimestre 2012 à la presse et aux acteurs concernés par la gestion des risques. Son objet porte sur divers points. Quel est l'état des menaces et des risques majeurs ainsi que les principaux retours d'expériences des crises récentes (tempête Xynthia, inondations du Var, catastrophe de Fukushima, …). Quelles sont les organisations en charge de la gestion des catastrophes et comment les acteurs peuvent se préparer. Enfin, comment allons-nous agir face aux risques majeurs à venir. Par ailleurs, nous réfléchissons à l'élaboration d'un scénario d'analyse de risques, nous vous présentons ci-dessous une ébauche de cette réflexion. Ce scénario est à l'étude et n'a pas encore été appliqué en entreprise.

3.1.1. Plan du scénario

- Étape 1 : Définition des classes de scénarios d'interruption et établissement d'une matrice Impact / Gravité.
- Étape 2 : Détermination des stratégies par classe de scénario : composants cumulatifs de la continuité et évitement de l'interruption. Etablissement d'une matrice relatif aux risques humains, techniques, environnementaux et selon les risques PRE, PERI et POST traumatiques.
- Étape 3 : Analyse d'écart : Entre les capacités actuelles de l'entreprise et les recommandations pour éviter une perte d'exploitation / mesures d'atténuation par classes de scénarios.
- Étape 4 : Planification du projet : Délais et estimations des coûts pour aller plus loin.

3.1.2. Étape 1

Définitions des classes de scénarios d'interruption

Nous avons identifié 5 types de classe selon l'impact et la gravité. Seuls les 3 derniers types de classe correspondent aux risques majeurs. Pour ce classement nous nous sommes inspirés

[9] http://www.fr.albayane.org/economie/9580-en-depit-de-la-resilience-du-systeme-bancaire-national--bank-al-maghrib-souligne-limportance-de-poursuivre-les-efforts-en-matiere-de-gestion-des-risques.html

des Systèmes de Sécurité Incendie (SSI) qui sont classés en cinq catégories par ordre de sévérité décroissante: Catégories A, B, C, D et E.

Impact et gravité

L'impact : comme le nom l'indique, c'est l'impact du risque sur l'activité de l'organisation. L'impact est déterminé en prenant en compte les points suivants (le nombre d'infrastructures touchés, la dégradation de l'image de l'entreprise, le nombre de personnes tuées ou blessées).
La gravité : correspond à la durée de blocage de l'infrastructure, le coût financier.

1. Mineur (sans conséquence, ni machine, ni humaine)
   - Impact faible – Gravité faible
   - Panne informatique
   - Coupure réseau

2. Moyenne (avec une légère conséquence machine, sans conséquence humaine)
   - Impact faible – Gravité moyenne
   - Défaut mécanique
   - Arrêt d'un serveur d'application critique
   - Accident automobile, sans décès

3. Importante (avec une conséquence pour la machine, sans conséquence humaine)
   - Impact faible – Gravité élevée
   - Impact moyen – Gravité moyenne
   - Impact élevé – Gravité faible
   - Nuage de cendres du volcan islandais Eyjaf¨joll
   - Incident du Crédit Lyonnais

4. Conséquente (conséquence importante machine, avec une conséquence légère humaine)
   - Impact moyen – Gravité élevée
   - Impact élevée – Gravité moyenne
   - Tempête Xinthia
   - Usine AZF de Toulouse
   - Virus H1N1

5. Catastrophique (conséquence importante machine, avec une forte conséquence humaine)
   - Impact élevé – Gravité élevée
   - Tremblement de terre (Haïti)
   - Séisme et tsunami au Japon
   - Forte chaleur été 2007 en France

		IMPACT		
		ELEVE	**MOYEN**	**FAIBLE**
GRAVITE	**ELEVE**	**5**	**4**	**3**
	MOYEN	**4**	**3**	**2**
	FAIBLE	**3**	**2**	**1**

Caractéristiques des scénarios externes

- Jour/heure (heures de travail ou non)
    - Le serveur de la banque en ligne s'est arrêté le vendredi 10 mars 2011
- Étendue géographique (lieu, endroit, site, service, …)
    - Le lieu de l'arrêt se trouve à Paris 1er, rue de Rivoli
    - Le service impacté, est la gestion des clients
- Localisation de l'impact sur le système (accident de train, état du train)
    - Arrêt complet du serveur
- Localisation des dommages dans l'entreprise (accident de train, état de l'environnement, rails, caténaires, gare, …)
    - Dysfonctionnement grave lié au système d'information
    - Erreur critique 512 annoncée
- Blessés parmi les employés du personnel (scénarios 4 ou 5)
    - N/A
- Conséquences sur le lieu de travail (accident de train, grève, blocage de la circulation)
    - Basculement sur le serveur de secours
    - Fonctionnement en mode dégradé

Associer les classes de scénario et les caractéristiques. Par exemple, un scénario de type 3 (incendie du Crédit Lyonnais) et ses différentes caractéristiques.

3.1.3. Étape 2

Détermination des stratégies par classe de scénario : composants cumulatifs de la continuité et évitement de l'interruption. Selon la classe déterminée, établir un croisement entre les risques humains, techniques ou environnementaux et le risque traumatique (PRE, PERI, POST). Le risque PRE-traumatique est un risque qui a déjà été vécu par les individus. Le risque PERI-traumatique est le moment précis lorsque la menace arrive, il est perçu comme une surprise, entre l'avant et l'après plus rien ne sera identique. Le risque POST-traumatique est l'après, il laisse souvent une marque importante dans l'esprit des individus impactés.

Risques PRE-traumatiques : Au sein de nombreuses populations, des antériorités psychiatriques et/ou psychologiques personnels et familiaux (dépression, dépendance, abus de substance, anxiété, etc.) ou des traumatismes passés (abus sexuel, violence, etc.) constituent des facteurs de risque (O'Toole & all, 1998).

Risques PERI-traumatiques : Plusieurs individus vivent de fortes réactions émotionnelles négatives (colère, honte, peur, tristesse, culpabilité) ou de fortes réactions physiques d'anxiété (tremblements, étourdissements, palpitations, transpiration, frissons) pendant et immédiatement après la crise (Andrews & all, 2000).

Risques POST-traumatiques : Des réactions dépressives au sein des victimes d'accidents, des stresseurs additionnels qui surviennent à la suite de la crise (difficultés financières, perte d'emploi, maladies ou décès d'un proche) et l'état de stress aigu sont des indicateurs du développement futur de troubles (Harvey, Bryant, 1998).

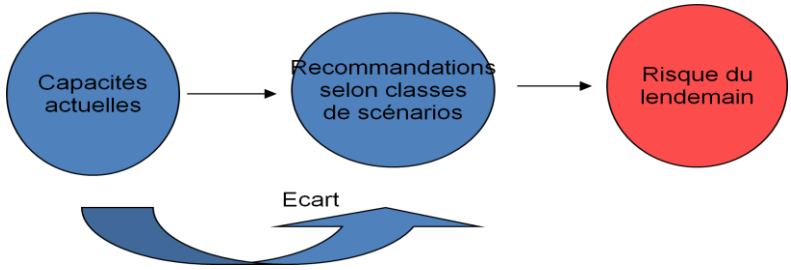
		Risque traumatique		
		PRE-traumatique	**PERI-traumatique**	**POST-traumatique**
Type de risque	**Humain**	Anticipation	Communication	Formation
	Technique	Veille Identification des risques	Gestion de crise	Plan d'urgence Plan de continuité

		Evaluation des risques		Retour d'expérience
	Environnement	Système d'alerte	Alerte	Plan d'exposition aux risques Plan de prévention des risques

« *Le courant de l'ingénierie de la résilience vise à formaliser les fonctions nécessaires pour assurer des performances de résilience organisationnelle. Ces fonctions sont au nombre de quatre. La première est relative à l'apprentissage par l'acquisition de connaissance sur les événements du passé qu'il s'agisse de presque accidents, d'incidents, d'accidents ou bien de succès. La seconde est relative à la faculté à réagir à la survenue d'un événement en apprenant les attitudes correctes à tenir lors de la survenue d'un événement. La troisième est relative aux mécanismes d'attention en formalisant les facteurs à observer afin de détecter au plutôt les prémisses de la survenue d'un événement potentiellement porteurs de dommages. La quatrième est relative aux fonctions d'anticipation destinées à chercher à identifier les événements pouvant survenir en fonction des mutations de l'environnement dans lequel évolue le système.* »[10]

3.1.4. Étape 3

Analyse d'écart : Entre les capacités actuelles de l'entreprise et les recommandations pour éviter une perte d'exploitation / mesures d'atténuation par classes de scénarios. Cette analyse d'écart donnera les risques du lendemain. Le calcul des écarts permet de se situer. Il établit l'intervalle entre des objectifs et la réalité. Ce calcul d'écart n'est pas une fin en soi, ce qui est important, c'est leur analyse pour évaluer les possibilités d'actions correctrices et piloter l'activité de l'organisation.



Exemple : si accident de train
Capacité actuelle : aucune procédure existante
Scénario 3 - matériel HS (procédures techniques)
Scénario 4 - matériel HS ; humain blessé (procédures techniques et humaines)
Scénario 5 - matériel HS ; décès d'humain (procédures techniques et gouvernementales)

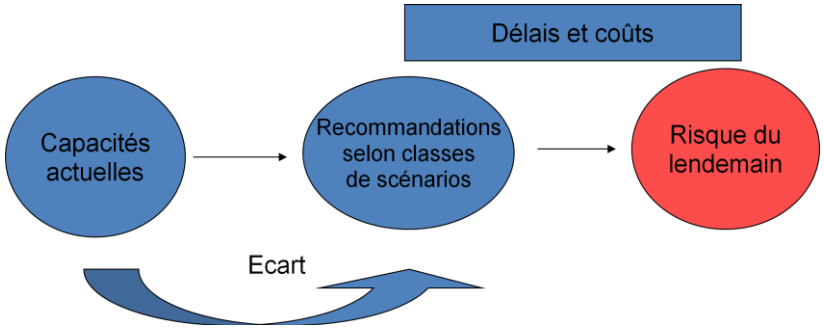
Essayer de mettre en commun une vision tripartite des risques techniques, humains, environnementaux en considérant les formes de résilience des systèmes, psychologiques et écologiques. Exemple : avec l'accident de la navette Challenger, la rupture des joints toriques (technique) est due à une température extrêmement froide (environnement), l'accident est lié à un ensemble de prise de décision mal géré de type pression de production (psychologique). Après l'accident de la navette spatiale Columbia en 2003, l'attention fut une nouvelle fois mis sur l'attitude de la NASA dans la gestion des problèmes de sécurité. Le Columbia Accident Investigation Board (CAIB) a conclu que la NASA n'avait pas réussi à tirer toutes les leçons

[10] Rigaud, E. Formalisation d'une démarche d'ingénierie de la résilience. 16ème congrès de maîtrise des risques et de sureté de fonctionnement. Avignon du 6 au 10 octobre 2008, Communication 4C-5. Mines ParisTech, CRC – Centre de Recherche sur les Risques et les Crises

de Challenger. En particulier, l'agence n'avait pas mis en place un véritable bureau indépendant pour la supervision de la sécurité ; la CAIB a estimé que dans ce domaine, « la réponse de la NASA à la Commission Rogers ne satisfaisait pas les attentes de la Commission ». La CAIB (Columbia Accident Investigation Board) a estimé que « *il n'a pas été remédié aux causes de l'échec institutionnel responsable de Challenger* », affirmant que le même « *processus de prise de décisions erronées* » qui a abouti à l'accident de Challenger a été responsable de la destruction de Columbia dix-sept ans plus tard.[11]

3.1.5. Étape 4

Planification du projet : Délais et estimations des coûts pour aller plus loin.
Il faut partir des capacités actuelles de l'entreprise, pour cela un audit de sécurité, des systèmes, des processus SI ou de gestion des risques peut être envisagé. Au regard des risques envisagés faire les recommandations selon les classes de scénarios. Les recommandations seront tirées des dangers futurs. Puis définir le coût de la mise en place des recommandations.



4. Critique de la proposition

La méthode d'analyse de risque que nous proposons n'a pas été testée (nous souhaitons dans un premier temps la mettre en parallèle avec les principaux risques majeurs de ces dernières années). Cela va nous permettre de sortir un ensemble d'éléments et de réaliser les matrices correspondantes aux 5 classes. Nous chercherons les correspondances techniques, psychologiques et environnementales pour chacun des risques. Nous pensons en retirés des règles importantes qui pourraient intégrer une gestion des risques résilientes.

Il est difficile de relier le risque humain, technique et environnemental. Dans certain cas les risques techniques sont causés par les conditions climatiques. Exemple : le séisme et le tsunami au japon qui ont impacté les centrales nucléaires. Dans cette catastrophe, nous ne percevons pas bien l'aspect humain, sauf en termes de victimes. Pourtant une catastrophe impacte sérieusement l'état psychologique des individus. La guerre du Viet Nam est porteuse du syndrome de stress post traumatique (SSPT) chez de nombreux vétérans. Nous soulevons également une déviation de la gestion du risque conséquente au contexte socio-géo-politique. La catastrophe liée au séisme d'Haïti à causé 250000 décès tandis que le séisme et le tsunami au Japon à causé 20000 décès. Pourquoi une différence aussi importante entre le nombre de décès et les dégâts organisationnels, peut-on dire que le Japon est un pays résilient, préparé à ce genre de situation, tandis que Haïti a subit la catastrophe sans aucune préparation. Les zones mondiales sensibles aux catastrophes sont connues et pourtant, pour une grande partie de ces zones, aucune protection ni préparation existe, nous sommes dans la dialectique du

[11] Columbia Accident Investigation Board, Report of Columbia Accident Investigation Board, Volume I, chapter 8, p. 195, 2003

profit et du bien être. Cela implique qu'une bonne gestion des risques devra tenir compte d'une éthique gouvernementale et nationale. D'après des sources officielles, la région Asie-Pacifique est la zone la plus exposée aux risques de catastrophes. Un habitant de cette région est cinq fois plus susceptible d'être affecté par une catastrophe naturelle que quelqu'un vivant en Afrique, et 25 fois plus qu'une personne installée en Europe ou en Amérique du Nord, d'après la Commission économique et sociale des Nations Unies pour l'Asie et le Pacifique (CESAP).

Un défaut de perception peut apparaitre entre la réalité du risque et le ressentiment. Pour cette raison il est important que le risque soit expertisé par une personne en dehors du système impacté. Importance de la tierce expertise lors d'une catastrophe. Il s'agit d'une procédure initiée par l'administration dont les objectifs sont spécifiés par celle-ci. Elle consiste à expertiser en totalité ou en partie, à la demande de l'administration, l'étude des dangers.

5. En guise de conclusion : vers une résilience gouvernementale

Le cadre d'Action de Hyogo 2005-2015: construire la résilience des nations et des communautés face aux catastrophes

Accepté par 168 gouvernements lors de la deuxième Conférence Mondiale sur la Réduction des Catastrophes, Kobe, Hyogo, Japon, 18-22 Janvier 2005. Il indique que la réduction des risques de catastrophes est essentielle pour le développement durable. Qu'il faut renforcer les institutions (en particulier les communautés) qui construisent la résilience et élaborer à partir de la réduction des risques, la gestion de l'urgence et de la reconstruction. *« On s'attend à ce que le changement climatique accroisse la fréquence et la force de certaines catastrophes naturelles. Nos villes et nos côtes devenant plus vulnérables, ces menaces peuvent engendrer des catastrophes d'une magnitude encore jamais vue jusqu'ici. Nous sommes donc dans l'obligation sociale, morale et économique d'augmenter notre résilience, à échéance de 2015 comme le préconise le Cadre d'Action de Hyogo, ce qui aidera également à réaliser les Objectifs du Millénaire pour le Développement. »*[12]

Dans sa publication « Hotspot Studies » en 2005, la Banque mondiale identifie les risques de catastrophe comme une contrainte majeure en matière de développement. La « Facilité mondiale de réduction des catastrophes et de relèvement (GFDRR) », mise en place en 2006 par la Banque mondiale et de la SIPC, est l'un des instruments visant à instaurer la prévention des catastrophes comme un élément transversal du développement durable. La priorité dans ce dispositif est de soutenir l'évaluation et la cartographie des risques au niveau national, afin d'identifier les activités de réduction des risques susceptibles de produire un maximum de bénéfices en termes de réduction des pertes (humaines et économiques).

Global Risk Report 2011, parait chaque année depuis 2006, ce rapport est publié par le Global Risk Network, qui est le groupe de travail du World Economic Forum. Ce groupe a établi les 36 risques mondiaux les plus importants classés en 5 catégories (économique, géopolitique, environnementale, sociétale, technologique). Dans ce papier nous proposons l'étude de trois de ces catégories, environnementale avec la résilience écologique, technique avec la résilience ingénierie, sociétale avec la résilience psychologique. Dans nos travaux ultérieurs, nous proposons d'analyser les 5 catégories en intégrant la résilience communautaire (résilience et éthique sociétale) pour la catégorie socio-géopolitique et la résilience économique

[12] Ban-Ki-Moon, Secrétaire Général de l'ONU, 2007

(dialectique des profits et du bien être) pour la catégorie économique. A partir de ces résultats, les 5 catégories de risques seront envisagées par les différentes classes de résilience, tenant compte de l'impact et de la gravité du risque. Chacune de ces classes sera considérée selon les risques PRE, PERI et POST traumatiques. Pour nous aider à analyser les risques, peut-être une autre façon de voir comme le propose Hollnagel (2010). « *Il faut une nouvelle définition du concept de sécurité, de façon à maximiser l'apprentissage organisationnel dans les situations normales d'activité, c'est-à-dire en l'absence d'accidents et autres événements fâcheux.* » Notre façon de voir sera une théorie généralisée du concept de résilience appliquée à toutes les formes de risques, il s'agit d'une interaction, d'une imbrication des différents systèmes (sociaux, techniques, environnementaux, financiers, nationaux).

Bibliographie

AFNOR. (2010), *Norme NF ISO 31000 Management du risque, Principes et lignes directrices*, Afnor.

Amalberti, R. (2001), « La maitrise des situations dynamiques ». *Psychologie Française*, vol 46, pp 105-117.

Amalberti R. (2009), « Violations et migrations ordinaires dans les interactions avec les systèmes automatisés », *Journal Européen des Systèmes Automatisés*, Vol 43/6, pp.647-660

Andrews, B., C.R. Brewin, S. Rose et M. Kirk. (2000), "Predicting PTSD symptoms in victims of violent : crime the role of shame, anger, and childhood abus", *Journal of Abnormal Psychology*, vol. 109, no 1, pp. 69-73.

Ashforth B.E. & Mael. F. (1996), Organizationnal identity and strategy as a context for the individual. In : J.A.C. Baum et J.E. Dutton (éd.), *Advances in strategic management*, Greenwich, CT, JAI.

Batty, M., Barros, J. and Alves Junior, S. (2004). *Cities: Continuity, Transformation, and Emergence*. CASA Working Paper Series, Number 72. Centre for Advanced Spatial Analysis (CASA), University College, London.

Billings C.E. (1999), "The NASA Aviation Safety Reporting System: Lessons Learned from Voluntary Incident Reporting." In : Proceedings of Enhancing Patient Safety and Reducing Errors in Health Care. *National Patient Safety Foundation*, Chicago IL (held at Annenberg Center for Health Sciences, Rancho Mirage CA Nov. 8-10, 1998).

Cook R. (2007), *Challenger Revealed: An Insider's Account of How the Reagan Administration Caused the Greatest Tragedy of the Space Age*, Enslow Publishers.

Cyrulnik, B. (1999), *Un merveilleux malheur*. Paris : Odile Jacob.

Farmer, F.R. (1967), "Siting Criteria, a New Approach", *Atom*, vol 128, pp 152-170 and presented at the IAEA

Harvey, A.G. et R.A. Bryant. (1998), "The relationship between acute stress disorder and posttraumatic stress disorder: a prospective evaluation of motor vehicle accident survivors", *Journal of Consulting and Clinical Psychology*, vol 66, no 3, pp. 507-512.

Hoc J-M. et Amalberti, R. (2007), « Cognitive control dynamics for reaching a satisficing performance in complex dynamic situations ». *Journal of Cognitive Engineering and Decision Making*. n°1.

Holling, C.S. (1973), "Resilience and stability of ecological systems". in: *Annual Review of Ecology and Systematics*. vol 4, pp. 1-23.

Hollnagel, E. Woods, D., & Leveson, N. (2006). *Resilience Engineering: concepts and precepts*. Aldershot, UK: Ashgate publishing.

Hollnagel, E. "Que peut-on apprendre lorsqu'il n'y a pas d'accident". *RSE*, n° 3, mars-avril 2010,

International Council for Science (ICSU) (2002). "Resilience and Sustainable Development: Building Adaptive Capacity in a World of Transformations". *Series on Science for Sustainable Development* N° 3. ICSU, France.
Kaës R. (1979), *Crise, rupture et dépassement*, Paris, Dunod.
Klein G. (1998), *Sources of Power: How People Make Decisions*. MIT Press, Cambridge.
LaPorte, T.R. (1982), "On the design and management of nearly error free organizational control systems". In David L. Sills, C.P. Wolf, & Vivien Shelanski (Eds.) *Accident at Three Mile Island: The human dimension*. Boulder, CO: Westview Press, 185-200.
Lieurance S. (2001), *The Space Shuttle Challenger Disaster in American History*, Thunder's Mouth Press.
Mayer P. (2003), *Challenger, les ratages de la décision*, Presses Universitaires de France.
McConnell M. (1987), *Challenger: A Major Malfunction*, Garden City, New York: Doubleday.
Morel, G. (2007). *La sécurité et la résilience dans les activités peu sûres : exemple de la pêche maritime*. Thèse de doctorat, Université de Bretagne Sud, Lorient.
Morel, G., Amalberti, R., Chauvin, C. (2009), « How good Micro/Macro Ergonomics May Improve Resilience, But Not Necessarily Safety ». *Safety Science*, N° 47, pp 285-294.
Olsson, P., Folke, C., and Berkes, F. (2004). "Adaptive Comanagement for Building Resilience in Social-Ecological Systems". *Environmental Management* N° 34, pp 75-90.
O'Toole, B.I., R.P. Marshall, R.J. Schureck et M. Dobson. (1998), "Risk factors for posttraumatic stress disorder in Australian Vietnam veterans", *Australian and New Zealand Journal of Psychiatry*, vol 32, pp 21-31.
Prades J. et all. (2005), « Vers une stratégie de transport durable fondée sur le développement de l'innovation technologique », *Esprit Critique*, volume 7, hiver
Rasmussen J. (1999), "The concept of human error: Is it useful for the design of safe systems in health care?" In Vincent C, deMoll B. (Eds.) *Risk and Safety in Medicine*. London: Elsevier.
Rasmussen J, Brehmer B, and Lepat J, Eds. (1991), *Distributed Decision Making: Cognitive Models for Cooperative Work*. Chichester, England: Wiley.
Reason J. (1997), *Managing the Risks of Organizational Accidents*. Brookfield, VT: Ashgate.
Roberts, K.H. (1990), "Some characteristics of high reliability organizations". *Organization Science*. 1, 160-177.
Shrivastava P. (1993), "Crisis theory and practice", *Industrial and environmental crisis quarterly*, n° 7.
Sibony D. (1991), *Entre-deux, l'origine en partage*, Paris, Seuil, 1991.
Teneau G, Ahanda J-G. (2009), *Guide commenté des normes et référentiels*, ed d'Organisation.
Teneau G & Koninckx G. (2010), *La résilience organisationnelle, rebondir face aux turbulences*, Ed De Boeck.
Teneau G. (2011*), La résistance au changement, perspective sociocognitive*, seconde édition, Paris, l'Harmattan.
Vanistendael, S. Lecomte, J. (2000), *Le bonheur est toujours possible-Construire la résilience*. Paris : Bayard.
Vaughan D. (1997), *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at Nasa* , University of Chicago Press (réédition).
Weick, K.E. & Roberts, K.H. (1993), "Collective mind and organizational reliability: The case of flight operations on an aircraft carrier deck". *Administrative Science Quarterly*. N° 38, pp 57-381.

Woods DD, Johannesen L, Cook RI, and Sarter NB. (1994), *Behind Human Error: Cognitive Systems, Computers and Hindsight*. Crew Systems Ergonomic Information and Analysis Center, Wright Patterson Air Force Base, Dayton OH.
Wreathall, J. (2006), "Properties of Resilient Organizations: An Initial View". In E. Hollnagel, D. D. Woods and N. Leveson (Eds.), *Resilience Engineering: Concepts and Precepts* (pp. 275-285) . Aldershot, UK: Ashgate.