Management de la sécurité: le problème de la prise en compte du risque dans les normes de management

Jean-Marc PICARD[1], Jean-François BARBET[2]

[1]CQP2i, Université de Technologie de Compiègne, rue du Dr Schweitzer, Compiègne, F-60200

[2]SECTOR, 12, avenue du Québec, B.P. 636, Villebon-sur-Yvette, F-91965 Courtabœuf Cedex

jean-marc.picard@utc.fr, jean-francois.barbet@sector-group.eu

Résumé – Deux comités techniques issus des principaux organismes de normalisation (ISO TC 223 et CEN TC 391) ont lancé la production de normes de management en matière de sécurité sociétale. Le projet ANR NOTSEG, dont l'objet consistait notamment à fournir une analyse comparée des premières normes en matière de sécurité, est arrivé à son terme. Rassemblant, avec AFNOR, des universitaires, des industriels et des experts internationaux, ce projet a permis de mettre en évidence la difficulté de la prise en compte du management du risque dans le domaine de la sécurité sociétale. Les travaux des comités techniques précités sont le fruit d'une coopération internationale. Celle-ci s'est appuyée sur la compétence d'experts venant d'horizons divers : management de la sécurité des personnes et des biens, sécurité civile, organisations étatiques et dans une moindre mesure management des risques industriels. Il n'a donc pas toujours été facile de trouver un accord sur les concepts. Ces normes traitent avant tout de la sécurité et de la sûreté des organisations. Elles font référence explicitement aux normes relatives au management des risques. Cette dualité entre management des risques et sécurité sociétale est le fruit du recours à des concepts de management différents. L'harmonisation de ces concepts reste à parfaire. L'objet de cette publication est de présenter, après un rapide état des travaux, quelques différences conceptuelles en termes de management dans le domaine de la continuité d'activité et de la résilience. www.notseg.fr

Abstract – *Two technical committees from the major standardization bodies (ISO TC 223 and CEN TC 391) have started to produce management standards regarding societal security. The ANR NOTSEG project, the purpose of which was in particular to provide a comparative analysis of the first standards regarding security, has come to an end. Gathering with AFNOR, academics, manufacturers and international experts together, this project has highlighted the difficulty of taking into account risk management in the field of societal security. The work of the technical committees mentioned above is the result of international cooperation. This one relied on the skills of experts with different backgrounds: people and property safety management, civil security, state organizations and to a lesser extent industrial risk management. It has thus not always been easy to reach an agreement on the concepts. These standards deal primarily with security and safety of organizations. They refer explicitly risk management standards. This duality between risk management and societal safety is the result of the use of different management concepts. The harmonization of these concepts still has to be improved. The purpose of this publication is to present, after a brief description of the work, some conceptual differences in terms of management in the field of business continuity and resilience* www.notseg.fr

1. Les normes de management pour la sécurité globale

1.1 Le contexte

L'objet de notre étude dans le cadre du projet NOTSEG portait principalement sur les normes de l'ISO (International Standard Organisation) et de l'IEC (International Electrotechnical Commission). L'UIT (Union Internationale des Télécommunications) est impliquée dans les travaux de sécurité sociétale principalement par le biais de sa collaboration au sein du JTC1, le Working Group commun ISO/IEC (CEI)/UIT débouchant sur la production notamment des normes de la série 27000 relatives aux systèmes d'informations.

Les autres organismes produisant des spécifications techniques indépendantes en matière de sécurité sociétale sont peu nombreux. Nous avons retenu deux organismes étrangers : l'American Society for Industrial Security (ASIS) et la National Fire Protection Association (NFPA). Ces deux organismes ont produit divers référentiels que nous avons pris en compte. Seule au niveau international, l'ISO dispose d'une structure de normalisation dédiée à la sécurité sociétale, en l'occurrence le Comité Technique TC 223. Ce comité entretient des relations permanentes avec d'autres comités produisant des référentiels en matière de résilience et de continuité d'activité. La plupart des travaux issus de ces comités ou autres organisations ont été pris en compte dans le cadre des travaux du TC 223.

Le TC 223 et son homologue européen le TC 391 travaillent en étroite collaboration. Du fait de l'incidence

de l'application des accords de Vienne[1], la production normative du TC 391 est limitée.

Compte tenu de thématiques parfois communes, le TC 223 entretient d'étroites relations avec plusieurs comités techniques ISO. Parmi ceux-ci :

- le sous-comité 27 (SC 27) du TC/JTC1 commun à ISO et CEI, notamment au regard de l'ISO 27031 : « Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité » ;

- le TC 8 « Navires et technologie maritime » qui produit la série ISO 28000 concernant les systèmes de management de la sûreté de la chaîne d'approvisionnement ;

- le TC 262 Comité de projet : « Management du risque », nouvellement créé, qui reprend les travaux du Technical Management Board sur la série ISO 31 000.

Le TC 223 entretient également des liaisons avec plusieurs organismes dont :

- une liaison de type « A »[2] avec le PMI (Project Management Institute) ;

- une liaison de type « A » avec la Croix Rouge internationale (Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge). Au début des travaux, la fédération s'est impliquée au sein du TC223 dans les domaines relatifs aux urgences et aux crises ;

- une liaison de type « A » avec ASIS International dont les représentants sont très actifs au sein du TC 223 sur le sujet de la résilience ;

- une liaison de type « A » avec Asian Disaster Reduction Center (association japonaise créée à Kobé regroupant 29 membres en Asie, la France étant l'un des 5 « Advisor Member »).

- enfin une liaison avec le TC 79 de l'IEC (CEI) « Alarm and electronic security systems ».

L'ensemble de ces liaisons permet d'expliquer logiquement la prise en compte des travaux de ces organismes.

Au niveau régional nous nous sommes limités à l'union européenne et plus précisément au niveau du CEN.

Au niveau national nous avons considéré quelques normes reconnues mondialement, particulièrement la norme britannique BS 25999 qui est le fondement d'une partie des travaux tant sur le vocabulaire (ISO 22300) que sur la continuité d'activité (ISO 22301).

1.2 Les types de normes

Une première classification des normes a été entreprise suivant le tableau présenté ci-après :

Famille de document	Contenu
Business continuity /Résilience et risque	Normes traitées par les WG4 et WG1 du TC 223 et normes sur le risque (TC 262 ISO 31000, 31010 et Guide 73)
Management	Normes de management ou guides (ISO 9000, Guides 81, 83 et 72)
Logistique, supply chain	Normes du TC 8 de la série ISO 28000
Technologies de l'information	Normes du SC27/JTC1 de la série ISO 27000
Societal security : autres normes	Autres normes du TC 223
Environnement	Normes du TC 207 issues de la série 14000. Le parallèle entre management environnemental et management de la sécurité nous a paru très intéressant : ces deux domaines doivent conjuguer réglementation et normalisation.
Assessment	Il s'agit ici essentiellement de la collection de normes génériques de l'ISO émanant du CASCO, organe dédié à l'évaluation de la conformité.
Autres normes	

FIG. 1 : une première classification

Cet ensemble représente un peu plus de 110 normes qui, pendant les années consacrées à notre projet, ont connu des évolutions notables. Certaines normes ont ou vont disparaître (ISO 22351, BS 25999), d'autres ont été abandonnées au profit de nouveaux projets (ISO 22323 sur la résilience remplacée par un « New Proposal »), certaines ont abouti (ISO 22301).

La première famille de documents consacrée à la continuité d'activité, la résilience et la maîtrise des risques a fait l'objet d'une étude comparative dans NOTSEG, étude dont nous délivrons quelques conclusions ci-après.

Cette famille de normes peut elle-même être subdivisée de la manière suivante :

- les normes système relatives aux organisations :

[1] Les accords de Vienne entre l'ISO et le CEN et les accords de Dresde (ex-Lugano) entre la IEC/CEI et le CENELEC traitent de la production commune de référentiels, leur but étant de limiter la production de normes concurrentes ou divergentes.

[2] Les liaisons de type A concernent les organisations apportant une contribution effective aux travaux du comité technique ou sous-comité pour les questions traitées. Les liaisons de type B concernent les organisations ayant émis le souhait d'être tenues informées des travaux du comité technique ou sous-comité. Les liaisons de catégorie C concernent le JTC 1.

- parmi celles-ci, des lignes directrices ou bonnes pratiques sous forme de guide (ISO 22313 sur la continuité d'activité) ;

- d'autres proposent des exigences (*requirements*) dont la mise en œuvre devra être démontrée dans le cadre d'une certification. Ces normes sont moins volumineuses que les précédentes mais elles sont en principe plus précises ;

- les normes traitant de l'interopérabilité :

- celles concernant les organisations : il s'agit par exemple de l'ISO 22315 (évacuation de masse), ISO 22320 (exigences des opérations des secours) ;

- les autres concernant les systèmes techniques : ISO 22311 (vidéosurveillance - Interopérabilité de l'export), projet ISO 22351 (interopérabilité et partage de données sur les situations d'urgence).

1.3 Les normes

1.3.1 La série 22300

En ce qui concerne les domaines de la continuité d'activité et de la résilience, la série 22300 sur la sécurité sociétale comporte actuellement trois normes principales et un projet. L'ISO 22300 fixe plus ou moins le vocabulaire, l'ISO 22301 dispose des exigences en vue d'une certification pour les systèmes de management de la continuité d'activité, l'ISO 22313 dispose de lignes directrices en matière de systèmes de management de la continuité d'activité, enfin le projet ISO 22323, récemment remis en cause, traite de la résilience. Suivant des dispositions régionales (en U.E. notamment), cette série devrait reléguer à un second plan les normes nationales (AS/NZS 5050), voire les faire disparaître à terme (BS 25999).

1.3.2 La série 27000

Issue du plus important comité technique commun (JTC1) à l'ISO et à la CEI, la série 27 000 comprend plusieurs normes relatives au management de la sécurité des systèmes d'information au sens le plus large du terme. Outre l'ISO 27000 portant sur le vocabulaire, la série comporte des normes d'exigences (27001), des normes guides (27002, 27003) et des normes de spécifications techniques (27004 : Management de la sécurité de l'information — Mesurage). Certaines de ces normes traitent explicitement des risques (27005) de l'audit et de l'évaluation en vue de la certification des systèmes de management de la sécurité (27006 ; 27007) enfin de la continuité d'activité (27031).

1.3.3 La série 28000

La série 28000 concerne la *Supply chain*. Elle se positionne comme un ensemble cohérent traitant de la sécurité et de la sûreté qu'elle définit comme *: « la résistance à un ou des actes intentionnels non autorisés destinés à endommager la chaîne d'approvisionnement ou à nuire à son fonctionnement »*. Cette définition ou tout au moins le concept sous-tendu semble être accepté dans la communauté du TC 223. Le fameux débat sécurité/sûreté, ou Safety/Security serait-il en passe d'être clos ?! La série ISO 28000 propose de nombreuses normes sur la résilience (28002), les exigences en matière de sûreté (28001), l'évaluation (28003) ou encore des bonnes pratiques (28004).

1.3.4 La série 31000

Outre de nombreuses normes nationales que avons recensées, nous terminerons ce panorama normatif en évoquant une série de quelques grandes normes concernant le management du risque. Il s'agit de documents très mûrs ayant fait l'objet d'un fort consensus et de nombreux débats internationaux. Ce succès est à mettre à l'actif de la direction technique de l'ISO (TMB) qui dans un premier temps a pris directement en main les travaux en lieu et en place d'un comité technique. Procurant un vocabulaire étendu (Guide 73), cette série comprend la norme générique de référence sur le management du risque (ISO 31000). Cette norme, citée en référence dans la majeure partie des normes produites par le TC 223, est complétée par un recueil méthodologique et technique (ISO 31010). Celui-ci offre aux managers une véritable boîte à outils dont beaucoup sont issus du domaine de la Fûreté de Fonctionnement et du management du risque. L'ISO 31004 et d'autres projets de déclinaisons de l'ISO 31000 sont en cours de développement.

2. Structure et principes des normes systèmes

Le projet NOTSEG fournit une importante analyse comparée de la structure de ces normes. Nous en livrons ci-après quelques résultats.

2.1 L'harmonisation du vocabulaire

L'étude des normes ne pouvait s'abstraire d'une étude des concepts, à commencer par une étude du vocabulaire. Un important volet du projet NOTSEG y a été consacré. A partir d'une sélection de normes, l'équipe MoDyCo a construit un glossaire bilingue contrastif qui regroupe les termes présents sous la rubrique "Terms and definitions". L'algorithme utilisé a permis d'extraire, à partir des normes étudiées, les termes et leurs définitions. Il a également permis de relier toutes les définitions jugées lexicalement identiques ou proches. En outre, différents outils ont ainsi pu être développés offrant de nombreuses fonctionnalités permettant, par des techniques diverses, la représentation des ontologies et mettant en évidence des relations entre vocabulaires de normes. Une plate-forme logiciel donnant accès à un glossaire contrastif ontologique, dénommée KONTRAST, a ainsi été développée. Indépendamment de ce travail, afin d'en faciliter sa lecture, CQP2i a développé un lexique de l'ensemble des termes définis dans les normes, y incluant les références croisées.

2.1.1 L'introduction de nouveaux concepts

Ce travail sur le vocabulaire a permis de mettre en évidence plusieurs points.

Le remarquable volume des références croisées (*cross reference*). Ainsi, près de 27 % des termes recensés dans les glossaires des normes sélectionnées, soit 274/1024 termes, renvoient ou reprennent une définition issue d'une autre norme. De plus, la moitié des termes d'origine externe proviennent explicitement du Guide 73, c'est-à-dire du domaine du « Risk Management ». Cela démontre que le TC 223 a parfaitement intégré, en théorie tout au moins, les concepts du Guide 73 se focalisant essentiellement sur le terme « Risk ».

Dde nouveaux termes apparaissent ou sont redéfinis. Les normes ISO 9000 et ISO 9001 ont toujours été les normes de référence en matière de système de management , procurant un vocabulaire abondant. Les normes du risque et du management de la sécurité fournissent de nouveaux termes ou les redéfinissent. Nous en donnons ici quelques exemples.

Risk : ce terme, faisant l'objet de 637 définitions dans la collection ISO et présent dans plus de 1000 normes, fait l'objet généralement de deux principales définitions relativement génériques :

- la première, reprise dans les Guides 51 et 63, et bien d'autres encore, dispose que le risque est une *«combinaison de la probabilité d'occurrence d'un dommage et de la gravité de ce dommage»*. On retrouve ainsi le concept de criticité (probabilité/gravité associée le cas échéant au concept de non-détection). Cette conception du risque est issue de la Sûreté de Fonctionnement ;
- la seconde définition, plus récente et formulée par le Guide 73 est aujourd'hui presque unanimement reprise. Elle est agrémentée de longues notes. Elle dispose d'emblée que « *le risque est un effet de l'incertitude sur l'atteinte des objectifs* ».

Menace : d'après deux définitions de la série ISO 27000 il s'agit d'une *« cause potentielle d'un incident indésirable, qui peut nuire à un système ou une organisation »* ou encore d'une *« cause potentielle d'un incident indésirable pouvant entraîner des dommages au sein d'un système ou d'un organisme »*.

Ces deux termes nous amènent logiquement à associer, d'une part, risque et traitement des non-conformités et, d'autre part, menace et actions préventives (selon le modèle ISO 9000), voire le concept d'actions de protection, concept non fixé à l'ISO. Le risque s'exprimerait donc au regard des effets de l'incertitude, alors que la menace procéderait des causes potentielles. Ce distinguo nous semble une avancée majeure dans les normes ISO. Les nouvelles normes fixent ainsi progressivement la dualité risque/menace dont la différenciation n'était pas toujours claire. On parlait souvent de menace pour des risques d'origine volontaire nonobstant la menace naturelle (menace d'orage par exemple). Cette dualité risque/menace est maintenant clairement posée par l'ISO, notamment dans l'ISO 28000, § 3.3, au niveau de la définition du management de la sûreté :

« ensemble des activités et pratiques coordonnées systématiques par lesquelles un organisme gère ses risques et les menaces et impacts potentiels qui leur sont associés »

Ces éléments de vocabulaire fondent donc des pratiques et concepts de management. D'autres termes ont retenu notre attention dans notre étude. Nous évoquerons le *Monitoring* défini par le Guide 73 comme: *«continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected»*. Nous terminerons par un dernier terme développé dans la première des normes de la série 22300, l'ISO PAS 22399, le concept de "*mitigation*", repris dans de nombreuses séries depuis et défini comme : *« limitation of any negative consequence of a particular incident »*.

FIG. 2 : la roue de Deming

Dans le cas du concept PDCA (*Plan, Do, Check, Act* ou roue de Deming), il semble que le « *Check* » ou le Contrôle, propre à un concept formulé par Walter A. Shewhart dans les années 40, fasse place à une notion de contrôle continu, y ajoutant une forme d'asservissement fondant ainsi le monitoring.

2.2 Les structures pré-existantes

Comme nous l'avons souligné dans notre étude, les normes de management sont très inspirées des concepts ISO 9000/9001. D'une part par la similarité du champ des exigences ou recommandations : documentation, audit, action préventives, actions correctives, leadership, politique, responsabilités, autorités etc. ; d'autre part par la prééminence du concept PDCA et de la planification dans la structure des modèles de systèmes proposés. Pour autant, la référence au PDCA nécessitera de plus en plus de schémas explicatifs, tant les normes semblent s'en éloigner, et ce notamment du fait de la référence presque constante à l'ISO 31000 ou à ses concepts.

2.3 L'apport de l'ISO 31000

L'ISO 31000 n'est pas à proprement parler une norme système mais une norme process. Elle propose une démarche pour le processus du management du risque, se fondant sur un enchaînement précis des activités.

Ce modèle de processus va inspirer voire structurer la production des nouvelles normes.

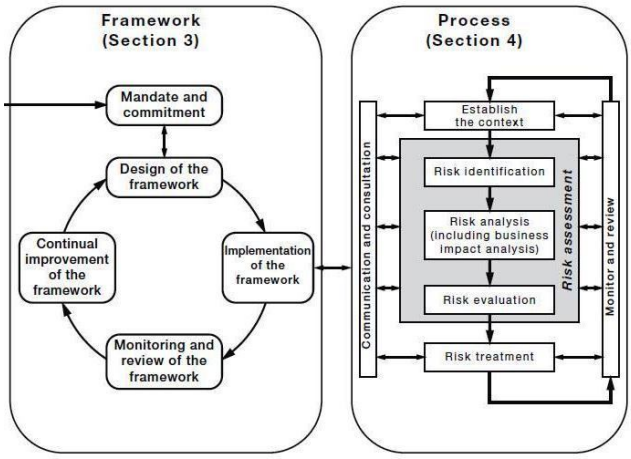

FIG. 3 : ISO 31000 structures

Les normes de la série 22300 vont y faire référence mais la plupart des normes de management vont s'appuyer sur ce modèle sous tendu de management du risque. Par exemple, la plupart des normes systèmes ont un chapitre sur la prise en compte du contexte généralement appelé « Understanding the context ».

2.4 Le guide 83 et les futures normes ISO

Ainsi, parallèlement aux travaux du TC 223 et en lien avec le TMB ISO, les normalisateurs se sont employés à imaginer la « norme des normes » ou tout au moins un modèle ou une structure de haut niveau sur laquelle se fonderait toute norme. C'est ainsi que Guide 83, né en 2010, sera supprimé pour être intégré immédiatement aux directives ISO. De la sorte, ce modèle en dix chapitres, dont l'avant-dernier est consacré au monitoring, reprendra plusieurs éléments issus de l'ISO 31000. Soulignons que les récentes réunions sur la révision majeure de l'ISO 9001 évoquent la reprise de ce modèle et l'inclusion du management des risques ou un lien avec le Guide 73.

2.5 Planification et prévention du risque : les limites

Indépendamment de la roue de Deming, toutes les normes de management produites sous une forte influence anglo-saxonne ont laissé la part belle à la planification correspondant au Plan du PDCA. Or la planification est indissociable de la prévision, raison pour laquelle la majorité des normes sur le management du risque s'appuie sur l'anticipation des risques et menaces et sur la prévision par la planification anticipée des activités.

Mais l'expérience douloureuse des crises a démontré que les crises ne suivaient jamais les plans ! Ainsi, si la planification permet aux organisations de s'affranchir des urgences, elle ne permet pas d'anticiper des crises caractérisées par une situation le plus souvent imprévue.

3. Forces et faiblesses du corpus normatif de la Maîtrise des Risques et de la Sûreté de Fonctionnement pour la maîtrise de la Sécurité Globale

Le corpus normatif analysé a porté sur les normes liées à la Maîtrise des Risques, les normes dites de Sûreté de Fonctionnement, celles liées la Sécurité Globale, dont celles incluant a minima explicitement les notions de continuité d'activité et de « résilience ».

L'une des principales raisons qui expliquent les discordances entre les différentes normes est très certainement le manque de compréhension partagée de ces différents concepts de Maîtrise des Risques, de Sûreté de Fonctionnement, de Sécurité Globale, de continuité d'activité et de Résilience.

Le vocable de « Maîtrise des Risques » correspond sur le fond, à la prise de conscience que, d'une part, toute activité présente des risques non nuls et que, d'autre part, il est donc important d'en assurer explicitement la maîtrise.

Mais cette prise de conscience s'est développée de façons différentes selon que les acteurs concernés étaient :

- des industriels –au sens large-, dont la préoccupation portait principalement sur des objets « technologiques » (systèmes d'armes, aéronefs, centrales nucléaires, sites industriels à risques, etc.)
- des managers dont la préoccupation principale était d'ordre financier.

La réflexion sur les risques industriels, souvent désignés » par le vocable de « risque technologique », voire de « risque technologique majeur », a vu se développer en parallèle la notion de Sûreté de Fonctionnement qui permettait de décliner le risque technologique- événement redouté craint- en préoccupations techniques et mesurables sur les technologies concernées : systèmes et composants mécaniques, fluides, électriques, électroniques et plus généralement systèmes incluant toutes ces technologies.

La Sûreté de Fonctionnement s'est ainsi préoccupée initialement de ce qui constituaient ses 4 principaux « attributs » : la fiabilité, la maintenabilité, la disponibilité, la sécurité évalués de façon probabiliste au niveau prévisionnel, et statistique au niveau opérationnel.

En parallèle, les acteurs respectivement concernés ont développé des réflexions autour de leurs préoccupations, au sein d'« associations savantes ».

Comme d'une part, pour ce qui est de la France :

- la 3SF (Sté pour l'avancement de la Sécurité des Systèmes en France) – initiée par l'Aérospatiale avant qu'elle ne devienne EADS -, devenue plus tard l'Institut de Cyndiniques
- l'ISdF (Institut de Sûreté de Fonctionnement) devenu en 2002 l'IMdR (Institut de Maîtrise des Risques) ayant intégré l'Institut de Cyndiniques,

regroupant en très grande majorité des acteurs impliqués dans la maîtrise des risques des systèmes technologiques,

mais aussi d'autre part, des associations comme l'AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise).

Cette différenciation des jeux d'acteurs, et donc de leurs préoccupations respectives, a tout naturellement donné lieu à des différences de conditions de mise en œuvre et de « traduction » dans les référentiels normatifs correspondants.

Ainsi, les activités de Maîtrise des Risques - au sens industriel – ont historiquement traité la partie endogène du problème en s'attachant au raisonnement suivant ; maîtriser les risques c'est soit :

- maîtriser la probabilité d'occurrence d'un accident du fait principalement des défaillances des « composantes » du système (*[3]), en jouant en priorité sur la conception, dont les règles d'exploitation et de maintenance (on parle de précautions « exportées » vers l'exploitation et la maintenance),
- maîtriser la gravité des conséquences en protégeant les entités vulnérables en cas d'accident.

Les référentiels correspondants de Sûreté de Fonctionnement ont été produits dans cet objectif. Ces référentiels ont donc principalement concerné la conception vis-à-vis de la sécurité, mais réciproquement, ils n'intègrent que très peu :

- la dimension économique,
- la dimension organisationnelle,
- la prise en compte des « agressions externes », autres que celles de dimensionnement –par ex. tenue au séisme- et en particulier pratiquement jamais la malveillance,
- la notion de résilience et de continuité d'activité.

Réciproquement, comme on l'a vu plus haut, se sont développés avec un retard certain par rapport aux référentiels de « conception », des référentiels :

- dont la dimension managériale était prédominante, mais dont la mise en œuvre technique concrète sur des grands projets était difficile,
- dont la dimension continuité d'activité, résilience, était prédominante mais dont la mise en œuvre n'avait pratiquement aucun lien avec les activités de « conception ».

Le corpus normatif actuel fournit donc des référentiels qui « couvrent l'ensemble des problématiques de Maîtrise des risques techniques et organisationnels, de Sûreté de Fonctionnement, de continuité d'activité et de résilience, mais d'une part, la complémentarité pratique et la cohérence, ne serait-ce qu'au niveau du vocabulaire, sont loin d'être atteintes, et d'autre part, il n'existe pas de référentiels « chapeau », de haut niveau dans les organisations et les projets, qui prenne en compte pratiquement toutes les composantes et en permette la déclinaison aux niveaux inférieurs.

4. Le problème de l'évaluation

Le projet NOTSEG a consacré une partie entière à l'évaluation de la conformité. Une des principales conclusions concerne la préservation de la confidentialité. La production d'informations sensibles, dont la divulgation ne serait pas maîtrisée, pourrait créer des vulnérabilités. Or, tout le principe du management de Deming et du management système consacré par les normes de la série 17000 produites par le CASCO se fonde sur le concept de démonstration par la preuve, sur les principes d'impartialité et surtout de transparence. Les normes relatives au risque en matière de sûreté ou de résilience s'accommodent difficilement des principes de transparence et de l'intégration des parties intéressées. Enfin, certaines exigences de ces normes peuvent empiéter sur le domaine réglementaire, domaine où les activités de contrôle relèvent des Etats.

Enfin, les normes d'exigences basées sur le concept PDCA avaient au bout de vingt ans fini par être parfaitement assimilées par la communauté de l'évaluation. A tel enseigne que ce concept fondait certaines qualifications d'auditeurs « système ». Le manque de précision de l'ISO 31000, très intéressante mais très conceptuelle, à l'inverse le trop grand recours aux procédures dans l'ISO 22301, prenant à contre-courant l'évolution des normes, l'absence de modèles partagés et de normes techniques sur l'évaluation des risques naturels et sociaux, ne rendent pas les missions d'accréditation et de certification faciles. De plus, il n'est pas sûr que le recours aux procédures dans les normes, favorable aux activités d'évaluation, soit une garantie de diminution du risque organisationnel suivant le concept de « *mitigation* ».

5. Conclusion

Beaucoup se posent encore la question de la pertinence des systèmes de management de la sécurité basés sur le concept de planification. Ceux -ci semblent pouvoir limiter les occurrences de crises mais, paradoxalement, ils peuvent, en donnant une confiance excessive, être source de danger. « A chaque catastrophe on avait pourtant tout

[3] Par ex., la composante « facteur humain » n'a été introduite que tardivement et n'est toujours pas systématiquement présente

prévu ! ». Les normes sur la sécurité sociétale et le risque intègreront-elles d'autres concepts comme l'agilité ? Il est très difficile de le prédire. Les concepts de continuité d'activité ont été intégrés, l'absorption relative de la BS 25999, parties 1 et 2, par les normes ISO est en partie réalisée. Pour autant, le concept de résilience ne semble pas fixé et les récents symposiums ISO ont illustré la difficulté à positionner la résilience par rapport à la continuité d'activité. En attendant, il semble acquis que le concept de PDCA a vécu dans la forme que nous lui connaissions.

Enfin, les risques sociétaux, comme le risque terroriste, n'obéissent à aucun modèle disponible en matière de management de la prévision du risque, contrairement au management du risque technologique qui commence à faire sectoriellement l'objet de consensus.

Références

[1] Picard J.-M., *Sécurité sociétale : une classification des normes, Lot 5.1* , projet ANR NOTSEG, UTC, livrable sur demande auprès des auteurs, Compiègne 2012.

[2] Picard J.-M., *Etude comparative des référentiels liens conceptuels Lot 5.2* , projet ANR NOTSEG, UTC, livrable sur demande auprès des auteurs, Compiègne 2012.

[3] Picard J.-M., *Sécurité sociétale : lexique normatif Lot 5.3* , projet ANR NOTSEG, UTC Compiègne, 2012, livrable sur demande auprès des auteurs, Compiègne 2012.

[4] Picard J.-M., *Sécurité sociétale : l'évaluation de la conformité Lot 7*, projet ANR NOTSEG, livrable sur demande auprès des auteurs, Compiègne 2012.

[5] Barbet J.-F., Mothes F., Paulmier C., *Forces et faiblesses du corpus normatif de la Maîtrise des Risques et de la Sûreté de Fonctionnement pour la maîtrise de la « Sécurité Globale* », lot 8, projet ANR NOTSEG, livrable sur demande auprès des auteurs, SECTOR, 2012.

[6] Picard J.-M., La Documentation française,*« Sécurité globale : de Prague à Bangkok, les nouveaux enjeux de la normalisation technique »*, Cahiers de la sécurité intérieure, INHES, La documentation française, Paris, 2012.

[7] Lafréchoux, M., Juanals, B., Minel J.L. *KONTRAST : création d'un glossaire contrastif à partir d'un corpus de normes internationales, 11e journées internationales d'analyse statistique des données textuelles (JADT)*, Liège, juin 2012.

[8] Picard J.-M., 2010. « Societal Security : *First standards for business continuity and ISO 31000, concepts, similarities and differences* »; communication avec actes, congrès LMU La Rochelle octobre 2010.

[9] Juanals B., Picard J.-M., 2010. « Normalisation et sécurité globale : ontologies, vocabulaire et cartographie des acteurs », communication à la réunion plénière du TC 391 CEN, Prague, 04/11/2010.

[10] Picard J.-M., *Gestion de crise : vocabulaire et concepts*, Les Cahiers de la Sécurité Intérieure n° 10, La documentation française, Paris, octobre 2009

[11] Picard J.-M., *Les travaux de normalisation dans les domaines de la gestion de crise et de la continuité des activités*, Les Cahiers de la Sécurité Intérieure n° 10, La documentation française, Paris, octobre ,2009