L'intégration de la sûreté au sein d'un service Santé-Sécurité : une approche globale et moderne des risques

Walter Brugot

MASTER IS - PREVENTION DES RISQUES & NUISANCES TECHNOLOGIQUES

MEMOIRE DE MASTER PRNT
Alternance en entreprise - 2ème année de Master IS-PRNT
Année 2017/2018

L'intégration de la Sûreté au sein d'un service Santé-Sécurité: une approche globale et moderne des risques

Entreprise :

Ministère des Armées,

14 rue Saint-Dominique 75700 Paris SP 07

Alternant :	Walter BRUGOT
Tuteur Entreprise :	----
Tuteur Universitaire :	Professeur Philippe GALLICE

		Nom :	Date :	Visa
Rédacteur :	Alternant	Brugot	07/08/18	
Approbateur :	Tuteur Entreprise	-----		

Je tiens à remercier le Professeur GALLICE et toute l'équipe pédagogique du Master IS-PRNT

de toute l'aide apportée durant ces deux années

Aix-Marseille Université – Faculté de Pharmacie - 27 bd Jean Moulin – CS 30064 - 13385 Marseille cedex 05 - France
Tél. : +33 (0)4 91 83 55 33 - Fax : +33 (0)4 91 80 94 69 - www.master-prnt.com

Sommaire

I. Introduction 3
II. Santé-Sécurité et Sûreté, deux domaines séparés 5
1. Santé-Sécurité et Sûreté de quoi s'agit-il ? 5
a. La Santé-Sécurité 5
b. La Sûreté 5
c. Dans les faits 6
d. Cas particulier du domaine nucléaire 7
2. Le risque, une notion fondamentale commune mais de nature différente 7
a Le risque comme notion fondamentale 7
b Des risques de natures différentes 9
c L'évaluation de la menace et du danger divergent également 9
3 Une séparation législative et réglementaire mais qui s'ouvre vers de nouvelles perceptives communes 10
a Rappel historique 10
b Les textes réglementaires de la sécurité incendie 11
c Les textes réglementaires de la sûreté (ou sécurité privée) 12
d De nouveaux textes réglementaires ou dérogatoires permettent d'entrevoir de nouvelles perspectives communes 14
4 Des réalités du terrain qui incitent à la dissociation : l'organisation et l'esprit 15
a Le travail quotidien des agents de sécurité incendie 15
b Le formation des chefs de services Santé-Sécurité 16
5 Conclusion 16
III Pourquoi l'intégration de la sûreté est une réponse globale et moderne aux enjeux de l'entreprise 17
1. La Sûreté, un enjeu à intégrer dans une stratégie globale des maitrises des risques pour l'entreprise ? 17
a Du domaine régalien à l'appropriation des entreprises 17
b L'entreprise face à sa responsabilité sûreté 18
c La nécessité d'une approche globale du risques au sein des entreprises 19
2. Les autres enjeux de cette intégration 20
a. Enjeux humains : esprit et emploi 20
b. Enjeux sociaux 20
c. Enjeux économiques et financiers : un ratio efficacité et coût 21
d. L'internationalisation : un facteur de complexité 22
e. La conformité à une nouvelle norme internationale ISO 31000 22
3. Des similtudes indéniables de la conception à l'exploitation 23

a Des similarités dans les grands principes de conception 23
b Des similarités dans les grands principes d'exploitation 24
c Sûreté, santé et-sécurité, les éternels rabats joies 25
4. Le futur rôle du Directeur Sûreté, Santé-Sécurité (DSSS): une fonction tranverse 25
a Aujourd'hui 25
b Demain 26
c Bilan 28
5. Conclusion 28
IV La mise en place d'une fonction transverse Sûreté, Santé-Sécurité au sein de l'entreprise 29
1 La gestion des risques, une approche globale 29
a Une méthodologie s'appuyant sur le management du risques et un engagement de la direction 29
b Première phase : identification des fonctions névralgiques 29
c Deuxième Phase : identification et caractérisation des scénarios de «source de danger-cible » 30
d Troisième phase : le traitement des risques 32
2 Un système de management global des risques : le système de management Sûreté,Santé-Sécurité 33
a Des exigences générales 33
b Première étape :le lancement de la démarche 34
c Deuxième étape : Politique, structure et responsabilité indispensable pour l'intégration de la sûreté 35
d Troisième étape : Objectifs, programme de réduction des risques 35
e Quatrième étape : Communication 35
f Cinquième étape : surveillance du niveau de performance 36
g Sixième étape ; Incident, événement involontaire ou volontaire, non-conformité, action correctives et préventives 36
h Septième étape Contrôle périodique : audit interne et revue de direction 36
3 Un focus sur les nouveaux métiers de la fonction transverse du Sûreté, santé-sécurité 37
a Le nouveau rôle du Directeur Sûreté, Santé-Sécurité 37
b Les différents métiers du collaborateur Sûreté, Santé-Sécurité 37
c Les conditions de succès à la mutation des métiers Sûreté, Santé-Sécurité 38
V Conclusion 41
VI Références bibliographiques et internet 43
VII Glossaire 45

I. Introduction

Au XIXème siècle l'industrialisation s'accompagne de nombreux accidents du travail dus aux conditions de travail très pénibles. L'espérance de vie d'un ouvrier est réduite et la protection sociale est quasi inexistante. Malgré le début de la législation du travail, la santé et la sécurité au travail sont d'abord considérées comme une affaire personnelle et très peu prises en compte par l'employeur. C'est au XXème siècle que la plupart des évolutions majeures feront leurs apparitions. Le renforcement de la réglementation va donc inciter, voire obliger les employeurs à mettre en place toute une organisation autour de la santé et la sécurité au travail (Art L4121-1 du Code du Travail) et en particulier le risque majeur de l'incendie. L'entreprise a donc très tôt pris en compte la gestion les risques sans malveillance (non intentionnels), susceptibles d'avoir des répercussions sur les personnes, les biens et l'environnement.

A contrario, longtemps, le concept de sûreté n'a appartenu qu'à la seule sphère publique. Érigée en droit naturel et imprescriptible par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789, la sûreté est d'abord cet équilibre voulu par les révolutionnaires entre, d'une part, la sécurité des personnes et des biens et, d'autre part, la préservation des libertés individuelles et des libertés publiques. Ce n'est que dans la période contemporaine que la notion s'est progressivement imposée aux organismes « non régaliens » pour désigner une politique, une stratégie de limitation et de gestion des risques en rapport avec des comportements intentionnels malveillants. Les attentats du 11 septembre 2001, parce qu'ils ont à la fois redessiné le paysage et l'expression des menaces et qu'ils ont été à l'origine d'une nouvelle politique de sécurité intérieure largement influencée par les États-Unis, ont, à l'évidence, été un puissant accélérateur d'un processus par lequel la sûreté est entrée dans un domaine partagé entre l'État et les autres acteurs.
Ainsi l'organisation des entreprises s'est adaptée pour prévenir et se protéger de manière distincte des risques liés à chaque domaine sûreté et santé-sécurité en prenant appui sur des corpus législatifs et réglementaires différents.

Mais dorénavant une concurrence exacerbée, une diffusion instantanée de l'information et des Etats moins omniprésents imposent aux entreprises actuelles de mener en permanence une réflexion globale afin de mettre en place des stratégies de maitrise des risques. Elle inclue ceux liés aux comportements intentionnels de malveillance (sûreté) pour répondre aux risques et aux enjeux auxquels elle est confrontée. Une réponse moderne et efficace à cette problématique est l'intégration de la sûreté au sein d'un service santé-sécurité.

Dans ce mémoire, après avoir approfondi et compris les fondements de cette coexistence sûreté et santé-sécurité, nous allons découvrir pourquoi l'intégration de la sûreté est une réponse globale et moderne aux enjeux de l'entreprise. Enfin comment, après un processus de gestion des risques, il est possible de mettre en place de manière systémique et collaborative, cette mutation intellectuelle et organisationnelle en élaborant un système global de management des risques et en créant de nouveaux métiers pluridisciplinaires. Ce mémoire propose une mise en place d'un système de management ***sûreté, santé-sécurité*** ainsi que les nouveaux métiers associés.

II. Santé-Sécurité et Sûreté, deux domaines séparés

Cette première partie va permettre de mieux comprendre la situation actuelle et les évolutions séparées de la santé-sécurité souvent utilisé sous le vocable de « sécurité » et de « sûreté » au sein des entreprises. Après avoir défini ces domaines, l'approche des différents risques et des données réglementaires permettent d'établir plus précisément les notions de sécurité et de sûreté.

1. Santé-Sécurité et Sûreté de quoi s'agit-il ?

Dans le langage courant, la sécurité est donc un concept globalisant, pouvant couvrir de nombreux domaines. De façon simple, on peut considérer que la sécurité est l'état dans lequel le risque accidentel ou intentionnel, quelle que soit sa nature, a été ramené à un niveau acceptable pour l'homme.
Ainsi la sécurité peut donc renvoyer aussi bien à la notion de risques technologiques, d'incendie (sécurité incendie), de risques professionnels (sécurité et santé au travail,) qu'à la notion de malveillance (activités privées de sécurité, gardiennage, contrôle des accès...).

a. La Santé-Sécurité

Le code du travail (Art L421-1) impose à l'employeur de mettre en œuvre tous les moyens nécessaires pour réduire au maximum les risques afin d'assurer l'intégrité physique et morale de ses salariés. L'employeur se doit de respecter des règles spécifiques d'hygiène, de sécurité et d'amélioration des conditions de travail en faveur des salariés.

La santé-sécurité désigne donc l'ensemble des moyens humains, organisationnels et techniques réunis pour prévenir et faire face aux risques (incendie, psychique, biologique, techniques, physiques, chimiques et environnementaux…) pouvant nuire aux personnes, à leur bien-être social, aux biens et à l'environnement sans avoir un but de profit. Cela correspond de façon générique à la démarche ainsi qu'aux méthodes et dispositions associées visant à limiter les risques sans malveillance, susceptibles d'avoir des répercussions sur les personnes, les biens et l'environnement
Il est important de préciser que la santé au travail, incluse dans le domaine santé-sécurité, est davantage liée à des risques chroniques et maladies professionnelles alors que la sécurité se rapproche des risques accidentels. On accorde souvent moins d'importance aux questions qui concernent la santé des travailleurs qu'aux problèmes de sécurité car il est souvent plus difficile à résoudre (traumatismes musculeux squelettiques, troubles psychiques…). Toutefois, lorsqu'on s'occupe de santé, on s'occupe aussi de sécurité car un environnement de travail sain est par définition aussi un environnement sûr.

b. La Sûreté

La sûreté concerne l'ensemble des moyens humains, organisationnels et techniques réunis pour faire face aux actes intentionnels, spontanés ou réfléchis ayant pour but de nuire, ou de porter atteinte dans un but de profit psychique ou/et financier.
Elle correspond à la démarche ainsi qu'aux méthodes et dispositions associées visant à limiter les risques de nature malveillante. Cette volonté de nuire peut donc porter atteinte aux personnes, aux biens matériels ou immatériels (informations, données numériques).

Le tableau 1 ci- dessous permet de fournir quelques exemples d'actes de malveillance de degré de gravités différentes (listes non exhaustive).

	Actes de malveillance
Intégrité physique et morale des personnes	Pressions, harcèlement, agression, incivilité, escroquerie, détournement entrainant des pertes de savoir-faire, actes terroristes…
Atteintes aux biens matériels	Vol, vandalisme, dégradation, pillage, incendie, destruction d'outil de production….
Atteintes aux biens immatériels	Vol d'informations confidentielles, espionnage économique et industriel, atteintes à l'image

Tableau 1 : type d'actes de malveillance

Dans de nombreuses publications le terme sécurité privée est employé au lieu de sûreté. Mais il s'agit bien de sûreté assurée par un organisme non étatique.
En effet, la sécurité privée est définie comme « l'ensemble des activités et des mesures, visant à la protection des personnes, des biens et de l'information, fournies dans le cadre d'un marché compétitif, orienté vers le profit, et où les pourvoyeurs n'assument pas au regard de la loi, des responsabilités de fonctionnaires au service de gouvernement » (Martine Fourcaudot, 1988).

De même il convient de préciser que l'on parle généralement dans le domaine du numérique de « sécurité informatique » mais il s'agit bien de sûreté. Elle vise à se prémunir des atteintes malveillantes à l'intégrité (absence d'altérations indésirables), la disponibilité (fait d'être prêt à l'utilisation pour les sollicitations autorisées) ou la confidentialité (absence de divulgations indésirables) des données et des systèmes impliqués dans leur traitement informatique. La nature malveillante des risques considérés fonde cette différence marquée avec la sécurité, où transparence et large accès à l'information sont le plus souvent recherchés.

c. Dans les faits

La santé-sécurité et la sûreté sont deux domaines séparés dans les faits et dans les textes sur le plan national. Dans un souci de consensus, les différents acteurs du secteur définissent la sûreté comme l'ensemble des activités et mesures prises pour prévenir et lutter contre les risques liés à la malveillance (risques d'origine humaine).
Par opposition, la sécurité couvre quant à elle les mesures visant à circonvenir les risques d'origine accidentelle (risque technologique, biologique, incendie, gaz...) ou chroniques (risque biologique, chimique…).
La sûreté est donc liée à la notion d'accident volontaire alors que la sécurité fait référence à des accidents d'origine involontaire.
En forçant un peu le trait et en caricaturant à peine la situation, nous pourrions l'imager par une transposition dans le domaine privé du clivage policier/pompier de la sécurité publique. Nous verrons d'ailleurs au cours de ce mémoire que la réalité n'est peut-être pas si éloignée.

La terminologie de ces deux domaines a également évolué de manière séparée. Le domaine de la sécurité (terminologie de la prévention des risques) utilisera le terme danger (hazard) pour définir la propriété intrinsèque des produits, des équipements, des procédés…pouvant entraîner un dommage. Alors que pour désigner la même chose dans le domaine de la sûreté (terminologie de la sécurité privée) on

privilégiera le terme menace (threat). Dorénavant nous utiliserons les deux termes indistinctement dans ce mémoire.

d. Cas particulier du domaine nucléaire

Le domaine nucléaire, ayant évolué séparément, a aussi développé des terminologies propres, parfois différenciées selon les secteurs industriels, maniant pourtant des concepts souvent très proches, voire dans certains cas identiques.
Ainsi le glossaire de l'Agence Internationale de l'Energie Atomique (AIEA) définit et explique les termes utilisés dans différentes publications de l'Agence. Ses définitions servent de référence dans le contexte international :

-La sûreté nucléaire (nuclear safety) désigne l'obtention de condition d'exploitation correctes, prévention des accidents ou atténuation de leurs conséquences avec pour résultat la protection des travailleurs, du public et de l'environnement contre des risques radiologiques inclus. (c'est de la sécurité)
- La sécurité nucléaire (nuclear security) désigne les mesures visant à empêcher et à détecter un vol, un sabotage, un accès non autorisé, un transfert illégal ou tout autres actes de malveillances mettant en jeu des matières nucléaires et autres matières radioactives ou installations associées et intervenir en pareil cas (c'est de la sûreté).

2. Le risque, une notion fondamentale commune mais de nature différente

a Le risque comme notion fondamentale

Un principal point commun entre santé-sécurité et sûreté tient dans le fait que leur évaluation et leur gestion s'appuient largement sur la notion de risque. Le risque se définit dans les deux cas de façon macroscopique pour une équation :

Risque = Probabilité x Gravité du Danger (ou de la Menace)

On peut même élargir les similarités à la gestion des risques *(risk management)* en général, qui inclut trois phases successivement :
-l'analyse de risques *(risk analysis),*
-l'appréciation ou l'évaluation du risque *(risk assessment*) en termes de criticité des conséquences pour l'organisation,
-le traitement du risque (risk treatment) qui en découle.

Dans un premier temps, l'analyse de risques se structure dans les deux domaines autour de phases similaires :

- Identification et caractérisation des menaces/danger,
- Identification et caractérisation des scénarios (ou faiblesses),
- Evaluation des conséquences et des probabilités d'occurrences.

Ainsi la phase d'analyse des risques permet ainsi l'estimation des risques auxquels on peut affecter des valeurs et les quantifier.

Dans un deuxième temps, la phase l'appréciation/évaluation du risque permet de déterminer une hiérarchisation des risques et une appréciation de son importance.

Dans un dernier temps, ce qui permet de conclure le processus de gestion des risques, le traitement des risques détermine les différentes options pour les maitriser. Quatre options sont alors traditionnellement distinguées, à savoir l'évitement (risk avoidance), la réduction (risk reduction), l'acceptation (risk acceptance) ou le transfert (risk transfert), et ce d'un point de vue sûreté comme du point de vue de la sécurité.

L'ensemble de processus « gestion des risques » est toujours accompagné par une surveillance et une communication (interne et externe) des risques.

La figure I permet de schématiser le processus de gestion des risques (risk management) commun à l'ensemble des domaines sûreté, santé et sécurité.

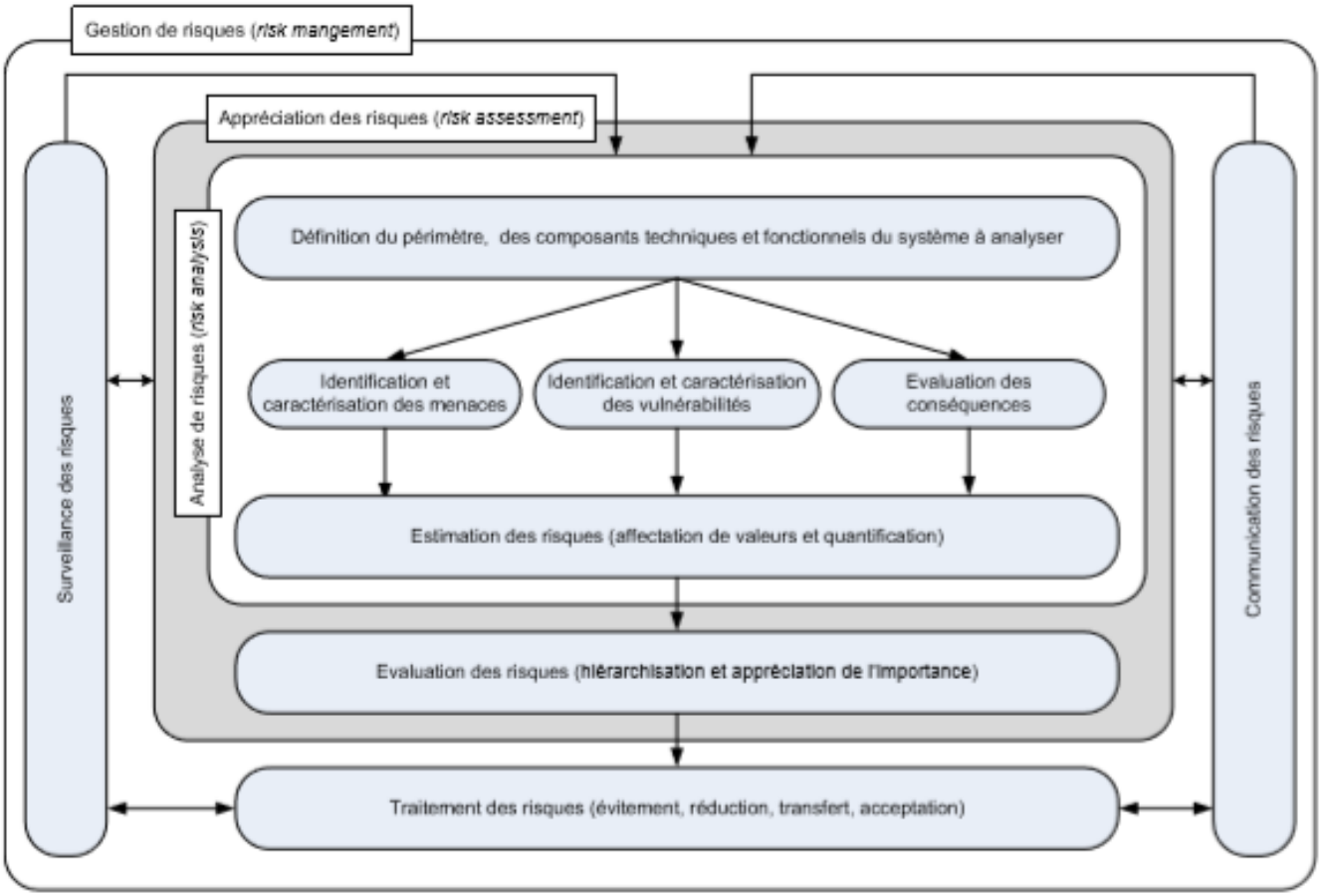


Figure 1 source : hal archives-ouverte.fr

b Des risques de natures différentes

Si en sûreté comme en santé-sécurité, la notion de risque joue un rôle fondamental, la nature du risque considéré diffère cependant.
Le niveau d'un risque en santé-sécurité, une fois qu'il est identifié et traité, reste généralement stable dans le temps. Il a peu de chance d'évoluer, sauf à modifier volontairement les données initiales de l'analyse de risque (nouvelles activités, agrandissement, déplacement ou augmentation importante de stockage de matière dangereuse…).
Dans le domaine de la sûreté, la nature du risque est d'origine humaine. Cela sous-entend qu'à tout moment, l'intelligence de celui qui veut nuire entre en jeu.
Cette intelligence est à considérer au sens de la capacité à analyser la situation donnée et donc d'une capacité à inventer, à imaginer une nouvelle façon de faire, à contourner, à mettre à défaut des dispositifs existants. La logique de « course » entre attaquants et défenseurs contribue ainsi à l'instabilité du niveau de risque.
L'évolution du contexte a aussi son importance. L'environnement social, économique et/ou politique dans laquelle évolue l'organisation peut modifier le risque (terrorisme, vol, vandalisme, sabotage…). Par exemple une société, où règnent des conflits sociaux, est plus sujette à des actes de vandalisme voire de vol qu'une entreprise ou règne un climat de sérénité et de dialogue.

Ainsi ce qui était une menace peut alors disparaitre ou devenir secondaire ou inversement. Ce qui semblait anecdotique peut rapidement devenir préoccupant pour celui qui est en charge de la sûreté.

c L'évaluation de la menace et du danger divergent également

L'évaluation de la menace est radicalement différente selon sa nature malveillante ou accidentelle.
Dans le premier cas, l'origine des menaces à évaluer est par définition hors de tout contrôle de l'analyste, et couvre un champ des possibles d'une extrême largeur. En sûreté, la menace est potentiellement intelligente et adaptive. Elle peut s'adapter vis à vis des vulnérabilités, voire des moyens de protections. Alors qu'en sécurité, danger et vulnérabilités n'ont pas d'interactions dynamiques.
Dans le second cas les caractéristiques des dangers sont plus accessibles, et le nombre de scénarios à considérer peut généralement être réduit à un ensemble restreint mais suffisant pour être considéré comme significatif.

De plus la caractérisation d'une menace type accidentel peut bien souvent s'appuyer sur une approche statistique. En particulier, la modélisation probabiliste des évènements s'appuie fréquemment sur des banques de données historiques considérables. En sûreté, de telles approches statistiques ne peuvent être adoptées pour caractériser la malveillance : trop peu de données sont partagées et mutualisées pour des raisons d'image ou de confidentialité.
Finalement, les difficultés intrinsèques à l'évaluation de la menace en sûreté laissent aussi place à une grande subjectivité dans leur perception. Les glissements vers un comportement irrationnel et paranoïaque y sont plus fréquents que pour des risques de type sécurité.

3 Une séparation législative et réglementaire mais qui s'ouvre vers de nouvelles perceptives communes

Après un rappel historique, nous allons découvrir que cette séparation prend son ancrage dans le corpus législatif et réglementaire français de la sécurité incendie et la sûreté. Dans les deux cas, la législation a été créée pour répondre à des accidents regrettables et dramatiques et à leurs conséquences. Ainsi l'organisation s'est adaptée pour répondre de manière concomitante aux conformités à chaque domaine, créant une culture spécifique à chacun. Cependant à partir de 2012, la réglementation amorce des perceptives communes nouvelles.

a Rappel historique

Il semble intéressant, pour tenter de comprendre la réalité de cette dissociation principalement due à la bicéphalie sécurité incendie au sein des établissements recevant du public (ERP) et des immeubles de grande hauteur (IGH) et sûreté, de remonter à son origine.
Des incidents ayant causé des décès (incendie du cinéma de Rueil-Malmaison le 30 août 1947 par exemple), un premier décret publié le 13 août 1954 commence à légiférer sur la prévention incendie.

Par la suite, devant la multiplication des projets immobiliers concernant des immeubles ou des centres recevant de plus en plus de public, le cadrage réglementaire de ce secteur s'est amplifié.
En 1970 le brasier de la discothèque le 5-7 de la commune de Saint Laurent du Pont en Isère compte un très lourd bilan 146 morts et de nombreux blessés par brûlures et intoxications (photo 1 ci-dessous du journal Le Dauphiné). L'arrêté du 18 octobre 1977 (portant application du règlement de sécurité pour la construction des immeubles de grande hauteur et leur protection contre les risques d'incendie et de panique) définit alors dans ses articles GH60, 62 et 63 la composition des services de sécurité obligatoires ainsi que la nécessité pour ses agents de détenir un certificat d'aptitude.

Photo : le brasier de la discothèque le 5-7 de 1970

Par la suite et en toute logique, l'arrêté du 25 juin 1980 modifié portant application du règlement de sécurité contre les risques d'incendie et de panique dans les établissements recevant du public poursuivit cette œuvre de sécurisation des installations par la mise en place de personnels dédiés et qualifiés.
Ces textes étant antérieurs à la législation sur la sécurité privée, il a alors paru opportun au législateur d'exclure de la loi n°83-629 du 12 juillet 1983 la sécurité incendie, déjà encadrée.
Les deux législations ont continué à évoluer par le biais de modifications successives ou de rajouts de textes. L'arrêté du 2 mai 2005 modifié relatif aux missions, à l'emploi et à la qualification du personnel permanent des services de sécurité incendie des ERP et IGH fixe alors très précisément le cadre de la formation nécessaire afin d'exercer dans ce type d'établissement en prévention incendie.

Or, en 2009, avec la création de la carte professionnelle surgit le problème de son attribution aux agents de sécurité incendie. Le Bureau des polices administratives du ministère de l'intérieur adresse alors aux préfectures en mai 2009 une circulaire rappelant que les « agents de sécurité incendie ne sont pas des agents de sécurité privée. Leurs aptitudes professionnelles respectives sont parfaitement distinctes et n'ont aucune équivalence entre elles. C'est le début d'un bras de fer où lobbyistes des deux camps (pour un rapprochement et pour une différenciation claire) s'affrontent à couteaux tirés.

b Les textes réglementaires de la sécurité incendie

Pour ce qui est de la sécurité incendie, nous pouvons citer, sans être exhaustif, les incendies du cinéma de Rueil-Malmaison le 30 août 1947 (87 morts), de la discothèque du 5/7 le 1er novembre 1970 à Saint-Laurent du Pont (146 morts), du collège Pailleron le 6 février 1973 (20 morts). Ces drames ont contribué à la création d'un cadre réglementaire visant à prévenir les risques d'incendie dans les E.R.P. comme dans les I.G.H. Ce cadre réglementaire, spécifiquement français se montre très efficace. Il se compose de trois documents principaux adossés au code de la construction et de l'habitation :

-***L'arrêté du 25 juin 1980*** modifié portant application du règlement de sécurité contre les risques d'incendie et de panique dans les établissements recevant du public du 1er groupe
-***L'arrêté du 22 juin 1990*** portant approbation de dispositions complétant le règlement de sécurité contre les risques d'incendie et de panique dans les établissements recevant du public (pour les établissements du 2ème groupe)
-***L'arrêté du 30 décembre 2011*** portant règlement de sécurité pour la construction des immeubles de grande hauteur et leur protection contre les risques d'incendie et de panique

Ceux-ci fixent entre autres les mesures constructives à adopter pour la création, la modification ou l'aménagement de ce type de bâtiments.
Mais dans leurs différents chapitres, les règlements de sécurité des E.R.P. et des I.G.H. fixent aussi la composition des services de sécurité ainsi que les qualifications requises pour les agents affectés à la sécurité du public ou des occupants. Ceux-ci doivent être titulaires des diplômes de Service de Sécurité et d'Assistance aux Personnes (S.S.I.A.P.) en fonction de leur niveau d'emploi.

	Diplôme S.S.I.A.P
Agent de sécurité	S.S.I.A.P 1
Chef d'équipe	S.S.I.A.P 2
Chef de service	S.S.I.A.P 3

Types de certificat S.S.I.A.P.

L'article MS 46 du règlement de sécurité dans les E.R.P. fixe par ailleurs que « lorsque le service [de sécurité incendie] est assuré par des agents de sécurité incendie […] le chef d'équipe et un agent de sécurité au moins ne doivent pas être distraits de leurs missions spécifiques. »
Cet argument réglementaire plaide donc en la faveur d'une exclusivité des activités des agents affectés à la sécurité incendie des établissements concernés. Néanmoins le périmètre est alors assez restreint puisque ne sont concernés que deux types d'établissements (ERP et IGH) pour lesquels la commission de sécurité a imposé un tel service et ceux dont la taille justifie la présence d'un service de sécurité incendie dédié. Cette taille critique est fixée dans les différents arrêtés portant application des dispositions particulières au type d'E.R.P.
Mais si le nombre d'établissements est assez restreint au regard du nombre total d'établissements en France, le public concerné lui est particulièrement représentatif et parfois en situation à risque (patients des hôpitaux, pensionnaires des établissements pour personnes âgées ou handicapées, etc.). La définition d'un tel périmètre, en y associant les I.G.H. permet d'affirmer que le nombre d'agents concernés est assez limité (environ 18 000).
Cette argumentation réglementaire visant à séparer agents de sûreté et agents de sécurité se base sur une exclusivité d'activité pour les agents de sécurité incendie.

c Les textes réglementaires de la sûreté (ou sécurité privée)

Du côté de la sûreté, l'exclusivité est aussi mise en avant pour confirmer cette séparation.
Si les textes fondateurs de la sécurité incendie font suite à des incidents particulièrement graves en terme de nombre de victimes, la législation sur la sûreté fait, quant à elle, suite à des incidents non moins dramatiques.
Les assassinats de Pierre Overney le 25 février 1972 par un vigile de l'usine Renault et d'un sans domicile fixe le 23 décembre 1981 au Forum des Halles en sont les illustrations les plus emblématiques. Plus récemment, il faut malheureusement ne pas oublier d'évoquer l'attentat contre le site de Saint-Quentin-Fallavier (Isère) le 26 juin 2015 et aux deux explosions criminelles survenues sur le site pétrochimique de Berre-l'Étang (Bouches-du-Rhône) le 14juillet 2015.).

Ainsi ***La loi n°83-629 du 12 juillet 1983*** réglementant les activités de sécurité privée fut prise pour encadrer cette activité. Si elle constitue un « socle fondateur de référence », elle fut l'objet de nombreux débats. La réglementation sur la sécurité incendie de l'époque donnant satisfaction, il a été décidé de ne pas chercher à de la légiférer davantage. L'objectif est alors uniquement de reprendre le contrôle d'une profession jugée en déliquescence et pas forcément de fédérer les différentes composantes de la sécurité.

De plus dans ***le décret du 23 février 2006 du Code de la Défense*** réglementant les activités qualifiées d'importance vitale, l'État, à travers le secrétariat général de la Défense et de la Sécurité nationale, a identifié 235 opérateurs d'importance vitale (OIV), des entreprises appartenant au secteur privé comme au secteur public, dont la liste est classifiée. Ces OIV opèrent dans douze secteurs d'activités, dont l'énergie, la défense, les transports, l'industrie, la pharmacie, l'espace et la recherche ou encore la gestion de l'eau… Ces derniers exploitent 1 370 points d'importance vitale qu'ils doivent impérativement sécuriser en respectant un ***plan particulier de protection***. Ce dispositif, qui décrit les risques encourus du site et les moyens mis en œuvre pour le protéger, doit être approuvé par le préfet du département.

Pour accentuer la séparation de la sûreté avec les autres domaines, deux décrets plus récents sont publiés : le ***décret n°2009-137 du 9 février 2009*** et le ***décret no 2011-1919 du 22 décembre 2011.***
Lors de la publication du ***décret n°2009-137 du 9 février 2009*** relatif à la carte professionnelle, un certain nombre de questions ont vu le jour. Si jusqu'à là la séparation entre les deux secteurs d'activité faisait

l'objet d'un statu quo, l'obligation de détenir un numéro d'agrément pour accéder à l'emploi a obligé les services de l'état à statuer sur la possibilité ou non d'un agent titulaire du S.S.I.A.P. d'exercer la fonction d'agent de sécurité.
C'est chose faite en mai 2009, lorsque le Bureau des polices administratives adresse une circulaire aux préfectures afin de préciser l'application du décret 2009-137 sur les cartes professionnelles. Sa conclusion est simple et sans ambiguïté :
« Les agents de sécurité incendie ne sont donc pas des agents de sécurité privée. Leurs aptitudes professionnelles respectives sont parfaitement distinctives et n'ont aucune équivalence entre elles. Les agents de sécurité incendie n'ont donc pas à demander la carte professionnelle des agents de sécurité privée. Cependant, un agent de sécurité privée peut être amené à effectuer à titre accessoire des activités de sécurité incendie : dans ce cas, c'est seulement au titre des activités de sécurité privée qu'il devra justifier d'une aptitude professionnelle. »

Cette circulaire, si elle soulève un tollé des entreprises privées de sécurité conforte les tenants de la séparation en légitimant leur position. Cette circulaire s'appuie notamment sur le rapport n°508 de M Christian Estrosi de décembre 2002 qui précise :
«les entreprises [de sécurité privée] ne peuvent exercer d'autres activités, telles que la sécurité incendie ou encore le nettoyage des locaux surveillés ».

Mais cette prise de position ferme crée une levée de bouclier dans le secteur professionnel. En effet, si les textes n'ont pas changé, cette interprétation stricte entraîne une incompatibilité d'exercice pour la majorité des entreprises privées de sécurité. D'un coup, ces entreprises qui proposaient jusqu'à présent des prestations de sûreté comme de sécurité pure se retrouvent en porte-à-faux, dans l'illégalité. Si la Direction des libertés publiques et des affaires juridiques (D.L.P.A.J.) rédige une nouvelle circulaire visant à satisfaire les différentes parties, celle-ci suscite la désapprobation du préfet directeur de la sécurité civile. (***Circulaire n°IOCD1115097 C du 03 juin 2011***)

Le directeur de la sécurité civile de l'époque, le préfet Alain Perret, dans un courrier adressé au directeur de la D.L.P.A.J. ainsi qu'au délégué interministériel de la sécurité privée (D.I.S.P.), fait état de son opposition à l'autorisation qui pourrait être faite aux entreprises de sécurité privée de vendre des prestations de sécurité incendie. Il justifie sa position par la légitimité du rapport n°508 de M Estrosi (cf. supra). Dix jours après sa nomination, son successeur, le préfet Jean-Paul Kihl, interpelle sur le même sujet le ministre de l'intérieur afin d'argumenter son souhait de maintenir la séparation entre les deux secteurs. Il évoque de nouveau le même article du rapport n°508. Mais il avance aussi de nouveaux arguments. Il évoque le fait que la sécurité incendie donne entière satisfaction et qu'elle ne gagnerait pas en efficacité à être menée conjointement avec la sécurité privée, en phase de structuration. À terme, la possibilité pour les entreprises de sécurité privée de vendre à la fois des prestations de sûreté et de sécurité pourrait, selon lui, « diminuer le niveau de sécurité ».

Nouvel élément, ***le décret no 2011-1919 du 22 décembre 2011***, permet la création du Conseil national des activités privées de sécurité (CNAPS). Cet établissement élargit le clivage entre sécurité et sûreté, car dorénavant toute activité de sûreté ou sécurité privée doit être autorisé par cet organisme.

Sa création fait suite à un rapport remis le 7 juin 2010 au ministre de l'Intérieur, relatif à la sécurité privée en France, rédigé conjointement par l'inspection générale de l'administration, l'Inspection générale de la Police nationale et l'Inspection générale de la Gendarmerie nationale. Ces inspections ont recommandé, outre la création au sein du ministère de l'Intérieur d'une délégation interministérielle à la sécurité privée, la mise en place du CNAPS. Ces recommandations ont été appuyées essentiellement par les syndicats de gardiennage et de transports de fonds qui représentent un effectif de plus de 120 000 professionnels en activité.

Le CNAPS est chargé d'une mission de police administrative. Il a pris le relais des préfets qui délivraient avant lui les autorisations administratives, les agréments de l'État aux dirigeants des entreprises concernées ainsi que les cartes professionnelles dématérialisées des salariés.

d De nouveaux textes réglementaires ou dérogatoires permettent d'entrevoir de nouvelles perspectives communes

Cette dernière décennie, un nouveau virage réglementaire est amorcé. Après des discussions nourries entamées depuis 2012, les textes réglementaires ont finalement évolué. Dans un premier temps la parution de ***l'instruction du 12 aout 2015*** autorise l'exercice des activités de sécurité et incendie par des agents doublement qualifiés.

Puis pour le domaine industriel, ***l'instruction gouvernementale du 30 juillet 2015*** est publiée. Il s'agit des derniers développements majeurs concernant la sécurité des sites SEVESO adressés aux préfets de zones de défense et de sécurité, de police, de région et de département. Cette circulaire vise à renforcer la sécurité des sites Seveso contre les actes de malveillance. Elle fait suite de l'attentat contre le site de Saint-Quentin-Fallavier (Isère) le 26 juin 2015 et aux deux explosions criminelles survenues sur le site pétrochimique de Berre-l'Étang (Bouches-du-Rhône) le 14juillet 2015. Un plan d'action prévoit notamment que chaque site **Seveso** devra être inspecté avant la fin de l'année 2015 et qu'une série d'établissements fera l'objet d'audits interministériels approfondis en matière de sûreté. Elle contraint les forces de l'ordre à acquérir une meilleure connaissance des installations et de leurs dispositifs de sûreté. La directive rappelle par ailleurs que le secrétariat général de la Défense et de la Sécurité nationale doit étudier l'opportunité de classer de nouveaux établissements Seveso comme point d'importance vitale au regard de leurs activités.

Photos 2 : deux explosions criminelles survenues sur le site pétrochimique de Berre-l'Étang (Bouches-du-Rhône) le 14 juillet. 2015.

De plus sous la pression de la grande distribution, des procédures dérogatoires sont accordées aux ERP de type M (magasin, centres commerciaux). Un arrêté du 13 juin 2017 dans son article M29 modifie le règlement de la sécurité incendie, permettant aux agents détenant la double compétence d'occuper simultanément les fonctions sûreté/sécurité dans ces ERP de type M : *« paragraphe 2. Dans les établissements où l'effectif reçu est supérieur à 4000 personnes, la surveillance de l'établissement doit être assurée par des agents de sécurité incendie dans les conditions fixées par l'article M46. Par dérogation aux dispositions du paragraphe2 de l'article M46 en dehors du chef d'équipe et de l'agent de sécurité, non distraits de leurs missions spécifiques, les autres agents SSIAP peuvent être employés à d'autres taches concourant à la sécurité globale de l'établissement ».*

Et enfin dans ces ERP, le regroupement sous un seul PC de sécurité et de sûreté est une mesure dérogatoire acceptée par la commission de sécurité*. « Paragraphe 5. Par dérogation aux dispositions du paragraphe 1 de l'article M50, le poste de sécurité incendie peut être mutualisé avec le poste de sûreté de l'établissement. ».*

Ainsi depuis 2012, un nouveau tournant réglementaire s'amorce mais l'esprit et l'organisation démontrent une certaine inertie.

4 Des réalités du terrain qui incitent à la dissociation : l'organisation et l'esprit

Dans la réalité du quotidien, compte tenu de l'organisation et de la conception des acteurs de leur travail, il existe une certaine logique à maintenir cette dissociation entre sûreté et santé-sécurité. Cette logique peut être évoquée sous l'angle double du pragmatisme et de la compétence.

a Le travail quotidien des agents de sécurité incendie

Si dans le paragraphe 1 de son article MS 50 le règlement de sécurité contre les risques d'incendie et de panique dans les E.R.P(sauf pour le type M) prévoit que le poste de sécurité incendie soit exclusivement destiné aux personnels chargés de la sécurité incendie, c'est afin de leur permettre une meilleure efficacité opérationnelle dans la gestion des alarmes ou situations de crises qui pourraient survenir. Il paraît en effet compliqué de gérer simultanément la supervision de nombreux écrans de vidéosurveillance et une situation de crise dans un poste de sécurité incendie (départ de feu dans un établissement recevant du public, secours à personne, etc.).

De la même manière, un agent affecté au contrôle d'accès sur un site, préposé au paramétrage des badges et au contrôle des laissez-passer, sera moins attentif dans la veille de ses moyens de secours et forcément moins efficace et rapide dans la gestion d'une crise éventuelle.

La dualité des postes de sécurité (et des équipes) se justifie alors par un meilleur traitement des différentes actions et des périmètres d'intervention. En outre, si les missions sont sensiblement identiques sur le fond (protection des personnes et des biens), il s'avère que leur application diffère grandement. Pour caricaturer le paradoxe des services mixtes (sécurité et sûreté), nous pouvons évoquer le cas de l'agent qui doit s'assurer, au cours de sa ronde, que la porte est correctement fermée à clef (réponse aux obligations liées à la sûreté) mais en même temps qu'elle puisse s'ouvrir facilement (afin de répondre aux nécessités de la sécurité).

b Le formation des chefs de services Santé-Sécurité

Actuellement la majorité de chef de service du domaine de la santé-sécurité est issue de formation de préventeur Hygiène Sécurité et Environnement (HSE) et est complétement étranger à la notion de sûreté et protection des informations. Ceci est même contre nature quand transparence et large accès à l'information sont le plus souvent recherchés.
De plus jusqu'à présent cette notion de sûreté limitée principalement au gardiennage et contrôle des accès est externalisée et rattachée au service à d'autres services (finance...). Le chef de service HSE est donc mis à l'écart et étranger à l'analyse des menaces et des besoins qui en découlent.

Ces éléments factuels permettent de justifier une séparation sûreté et sécurité.

5 Conclusion

Cette première partie a démontré comment les faits historiques et les réponses réglementaires ou législatives ont forgé ce clivage dans le travail et l'esprit des acteurs de la sûreté, santé-sécurité.
Les évènements et les réglementions de cette dernière décennie ouvrent cependant de nouvelles perceptives.
La prochaine partie va montrer que l'intégration de la sûreté au sein d'un service santé-sécurité va répondre de manière globale aux besoins de l'entreprise moderne et de ses enjeux actuels et futurs.

III Pourquoi l'intégration de la sûreté est une réponse globale et moderne aux enjeux de l'entreprise

Un contexte de plus en plus international, une concurrence exacerbée, la professionnalisation des acteurs de la malveillance, des Etats moins omniprésent imposent aux entreprises de mener en permanence une réflexion globale pour mettre en place tous les moyens de prévention et de protection de ses intérêts et son personnel .Ainsi les nombreux enjeux, auxquels doit faire face l'entreprise imposent de manière logique l'intégration de la sûreté dans son approche globale des risques. Cette intégration offre de nouvelles réponses modernes et transverses à l'entreprise. Elle pourra s'appuyer cependant sur de nombreuses similitudes existantes avec le domaine santé-sécurité.

1. La Sûreté, un enjeu à intégrer dans une stratégie globale des maitrises des risques pour l'entreprise ?

Droit fondamental de la personne, la sûreté, au cours des dernières années, est sortie de la sphère exclusivement « régalienne » pour entrer dans un domaine partagé entre le secteur public et le secteur privé. Définie comme une stratégie de réduction des risques liés à des comportements intentionnels de malveillance, la sûreté doit désormais faire pleinement partie de la stratégie de maîtrise des risques de l'entreprise.

a Du domaine régalien à l'appropriation des entreprises

Longtemps le concept de sûreté n'a appartenu qu'à la seule sphère publique. Érigée en droit naturel et imprescriptible par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789, droit défendu « par une force publique instituée pour l'avantage de tous » selon l'article 12 du même texte fondateur, la sûreté est d'abord cet équilibre voulu par les révolutionnaires entre, d'une part, la sécurité des personnes et des biens et, d'autre part, la préservation des libertés individuelles et des libertés publiques.
Le terme a ensuite longtemps désigné des institutions de puissance publique : « cour de sûreté de l'État », « direction de la sûreté nationale ». Ce n'est que dans la période contemporaine que la notion s'est progressivement imposée aux organismes « non régaliens » pour désigner une politique, une stratégie de limitation et de gestion des risques en rapport avec des comportements intentionnels malveillants.

Les attentats du 11 septembre 2001 parce qu'ils ont à la fois redessiné le paysage et l'expression des menaces et qu'ils ont été à l'origine d'une nouvelle politique de sécurité intérieure largement influencée par les États-Unis, ont, à l'évidence, été un puissant accélérateur d'un processus par lequel la sûreté est entrée dans un domaine partagé entre l'État et les autres acteurs. Depuis le choc du 11 septembre 2001, le crime au sens générique du terme a, en quelque sorte, changé de statut : il a quitté, pour partie, la sphère de la déviance d'individus ou de groupes pour accéder à celui de phénomène collectif, rejoignant en cela « les grands risques » naturels ou industriels. Marquée dans le même temps par la consécration du principe de précaution, notre société a vu s'estomper la frontière entre le crime et l'accident, la sûreté et la sécurité. Ceci s'est avéré dans de nombreux cas, soit parce que l'on ne puisse pas identifier avec certitude les causes d'une catastrophe (type AZF), soit parce que les conséquences du fait criminel ou du fait accidentel soient les mêmes (risque de contamination d'un produit de grande consommation par exemple).

Ci-dessous un schéma extrait d'une enquête de la revue Sciences et Avenir au sujet de l'accident d'AZF synthétisant les phénomènes non explicables dans le cadre d'un scénario accidentel.

Source « Sciences et Avenir »

b L'entreprise face à sa responsabilité sûreté

Peu d'entreprises échappent à la malveillance, ne serait-ce que dans les formes la plus couramment constatées dans les études spécialisées que constituent le vol commis à l'intérieur du périmètre de l'entreprise et la fraude interne. La liste des atteintes possibles à la sûreté de l'entreprise s'est enrichie au gré de la sophistication et de la mondialisation des échanges ainsi que de la multiplication des risques géopolitiques. Les menaces au sens de « manifestations intentionnelles d'un danger » sont traditionnellement réparties en trois catégories de cibles :
-Intégrité physique et morale des personnes
-Atteinte aux biens matériels,
-Atteinte aux biens immatériels.

À cette diversification et pression accrue des menaces s'est jointe une évolution des normes juridiques qui fait de la sûreté une responsabilité à part entière de l'entreprise.
Deux illustrations en attestent :
– des normes internationales comme le code ISPS (International Ship and Port Facility) dans le domaine maritime depuis 2004 visent à sécuriser la chaîne logistique internationale. En France une directive nationale de sécurité impose des plans de sûreté aux entreprises dont l'activité se situe dans des secteurs d'importance vitale ;
– la jurisprudence inclut désormais dans l'obligation de sécurité que l'employeur doit à ses salariés au titre de l'article L 412-1 du Code du travail la prévention des risques d'origine intentionnelle comme en attestent deux décisions de justice emblématiques. L'obligation de sécurité de résultat a été retenue à l'encontre de la DCN par le tribunal des affaires de sécurité sociale de la Manche en juillet 2004. L'entreprise, qui n'a pas su empêcher l'attentat de Karachi contre un car transportant ses collaborateurs, a commis une faute inexcusable par absence de connaissance du danger : « le contexte politique local aurait dû inciter l'employeur à des mesures de sécurité beaucoup plus drastiques […] ». Dans une affaire moins dramatique, la Cour de cassation établit en 2000 que la SNCF a une obligation de sécurité de résultat qui inclut la prévention d'un acte d'agression commis par un voyageur sur un autre voyageur.

Dorénavant, l'état et l'entreprise ont vocation à être en synergie forte face aux enjeux de sûreté. L'État protège les entreprises par des règles, les conseille via ses services spécialisés. De son côté, les entreprises, ainsi confortées, peuvent s'engager dans des stratégies de sûreté durable et limiter leurs risques.

c La nécessité d'une approche globale du risques au sein des entreprises

Comme nous l'avons vu précédemment, dans bien des cas la responsabilité de l'entreprise voire de sa survie, peut être engagée dans le domaine de la sûreté et il est de même dans le domaine de la santé sécurité (code du travail). Une logique de transfert de risque, dans le cadre d'un contrat d'assurance, ne suffit pas à se prémunir de l'ensemble des conséquences :
-des conséquences internes : dues aux pertes humaines, à la perte de l'outil de production ou à celles d'informations capitales à la poursuite des activités, à la dégradation de son image
-des conséquences externes : dues à la perte de crédibilité auprès de ses clients, à la dégradation de son image, à l'interdiction administrative d'exploiter un site de production à la poursuite judiciaire, etc.

Pour tous ses enjeux majeurs, elle doit s'armer afin de de prévenir efficacement tous ses risques. Elle doit donc pouvoir mettre en place un système de management global. Ce process permet de structurer son organisation afin notamment :
-d'identifier tous les dangers et menaces potentielles pour les biens matériels et immatériel dont la protection du savoir-faire, le personnel, et ses partenaires (clients, fournisseurs…) ;
-d'argumenter le niveau de maitrise suffisant mis en œuvre face à ces dangers/menaces et de viser une amélioration et une adaptation constante du niveau sécurité ;
-de définir l'implication dans le système de management global du personnel à tous les niveaux de l'organisation ;
-de garantir, aux diverses parties prenantes, le fonctionnement efficace d'une organisation structurée permettant une maitrise des risques.

2. Les autres enjeux de cette intégration

a. Enjeux humains : esprit et emploi

Qu'ils soient préventeurs, agents de sécurité incendie, vigiles ou directeurs sûreté, santé-sécurité ces hommes et ces femmes travaillent avec à terme le même objectif : « assurer la Sécurité des personnes et des biens ». S'il existe donc de nombreuses raisons pour une séparation physique entre la sûreté et la santé-sécurité, elles ne sont pas toujours évidentes pour le commun des mortels, un citoyen à la recherche d'une sécurité toujours plus importante. Il existe aussi bon nombre de raisons plaidant en la faveur d'un rapprochement de ces deux composantes de la fonction Sécurité.
La première des raisons qui justifie un rapprochement tient à leur sphère d'appartenance. Les deux secteurs, conjointement regroupés sous le vocable « Sécurité » appartiennent au domaine de la sécurité privée. Employés par des sociétés de droit privé, ou par des entités publiques mais sous contrat de droit privé, les salariés qu'ils soient chargés de protéger les personnes et les biens, contre les accidents du travail, contre l'incendie ou la malveillance dépendent de la sphère privée. Ces hommes et ces femmes ont l'esprit de service et ont tous en tête les termes de ***prévention et protection***.

De plus, si l'esprit de service favorise un tel rapprochement, les premiers intéressés (salariés) sont eux-aussi majoritairement favorable à ce rapprochement. Certes, un certain nombre a mené une campagne de communication en faveur d'une scission sans concession au début de ce siècle, mais si cette campagne a été entendue, elle ne fut le fruit, comme souvent, que d'une minorité. En outre, peu suivi, ce mouvement de protestation tend à s'éteindre à petit feu. Les gens du domaine ont pour la plupart compris que leur intérêt était plutôt dans la possession de la double qualification afin de pouvoir retrouver plus rapidement du travail dans un métier où la sécurité de l'emploi n'est jamais acquise. Cette double qualification leur donne une polyvalence et une vision globale du métier qui leur permet tout à la fois de remplir correctement leur mission et d'être en capacité de rebondir sur d'autres fonctions en cas de perte de marché par leur employeur.

Franchir le pas d'une formation commune n'est pas insurmontable d'ailleurs. Les formations S.S.I.A.P. 1 et C.Q.P. A.P.S ont des objectifs identiques dans certaine unité de valeur. Que ce soit la formation à la lutte contre le feu, au déroulement d'une ronde, à la rédaction d'un compte-rendu et d'autres encore, les savoirs et savoir-faire enseignés diffèrent peu. Dans les faits, nous sommes donc en présence de deux formations d'un volume limité disposant d'un tronc commun permettant de gommer encore la perception des différences au cours de la formation.
Un rapprochement de ses formations permettrait ainsi de diminuer les coûts de formation mais aussi de répondre aux enjeux sociaux ci-dessous.

b. Enjeux sociaux

Le fait de valoriser ses employés en passant une vision partielle à plus globale de la « Sécurité » est un véritable atout pour l'entreprise. Elle permet de développer un véritable esprit d'entreprise et une adhésion de la démarche en motivant et fidélisant les salariés. Grâce à cela, la qualité des produits et des prestations fournis est en hausse, le climat social dans l'entreprise est amélioré, l'environnement est préservé, et l'image de marque de l'entreprise est plus favorable.
De plus en sensibilisant voire en les formant aux aspects techniques et psychologiques de ce métier pluridisciplinaire, tous les acteurs de l'entreprise seront ainsi impliqués et compétents dans la prévention globale du risque. Mais tout ceci serait inefficace, si on imposait des mesures de prévention sans tenir compte des réalités de chaque situation de travail et surtout sans tenir compte des personnes.

Il faut toujours garder à l'esprit que la démarche de prévention dans l'entreprise repose sur le respect de trois valeurs essentielles :
-***les personnes*** : le chef d'entreprise, l'encadrement, les salariés, tous sont impliqués, tout changement se fait dans le respect des personnes.
-***la transparence*** : Le chef d'entreprise et l'encadrement affichent clairement les objectifs, s'engagent personnellement et fournissent les moyens nécessaires, prennent en compte la réalité des situations de travail et communiquent avec les travailleurs concernés.
-***le dialogue social*** : Il est indispensable d'impliquer les salariés et les instances qui les représentent : CHSCT, le futur CSE.

Une entreprise motivante et soucieuse de ses salariés accroît son dynamisme.

c. Enjeux économiques et financiers : un ratio efficacité et coût

La réalité économique et financière plaide également pour un rapprochement.
Les clients, directeurs sécurité ou managers sont les premiers à appeler de leurs vœux une telle unification, synonyme d'efficacité et de simplification dans la vie quotidienne avec des interlocuteurs uniques.
La gestion de services sûreté, santé et sécurité, équipés parfois de matériels similaires (prévention, communication, caméras et moniteurs, mains courantes et autres moyens de secours) avec des registres de consignes différenciés, des salariés non polyvalents est un problème permanent doublé d'une source de coûts supplémentaires non négligeable. En outre, quel donneur d'ordre (ou acheteur) a envie de payer deux fois un service qu'il estime, peu ou prou identique et qu'il est difficile au quotidien de différencier ?

De plus les entreprises ont trop souvent tendance à considérer les mesures de sûreté et sécurité comme des coûts obligatoires. Une vision globale leur permettrait au contraire de les envisager comme un investissement nécessaire et indispensable pour protéger leurs salariés, leurs biens et d'assurer leur image de marque face à des accidents et des menaces réelles.
Cette réalité est d'autant plus criante lorsque survient un événement malveillant : cyber-attaque ou encore attentat terroriste. Outre la mise en danger des salariés ou des clients, ces phénomènes laissent des traces durables, pour ne pas dire indélébiles auprès de l'opinion publique.

Comment en arrive-t-on là ? La plupart du temps, en ne considérant pas les mesures de sûreté à leur juste importance au sein des entreprises.

La preuve la plus flagrante de ce manque de considération est que la majorité des consultations et appels d'offres affichent le prix comme critère principal de sélection des prestations de sûreté / sécurité. Au même titre qu'une simple assurance multirisques, les entreprises ont tendance à y souscrire par obligation, en cherchant les moins "*disantes"* sans vraiment se soucier de ce qu'elles englobent réellement.

En effet, parmi les devoirs stratégiques d'une Direction se trouve l'obligation de protéger le personnel. La responsabilité des entreprises est aujourd'hui un enjeu majeur. Par ailleurs, l'entreprise doit veiller à son image et à sa notoriété qui font partie de son capital immatériel. La réputation a en effet des impacts directs sur la confiance accordée par les clients et en conséquence sur le volume d'affaires. Qu'une institution ne soit pas capable d'apporter la preuve qu'elle a mis en œuvre tous les moyens nécessaires pour prévenir la réalisation d'un risque ou d'un incident, n'est pas acceptable par l'opinion. Même lorsque la solution est apportée rapidement au problème, le public retient le défaut d'anticipation.

Ainsi, outre la protection indispensable du personnel, mettre en œuvre une véritable culture sûreté, santé et sécurité, c'est aussi préserver la stabilité commerciale et financière de l'entreprise.

Il est donc temps pour les dirigeants de changer d'état d'esprit et de remettre ce domaine transverse au cœur de la stratégie des entreprises et des institutions. Cela revient à choisir ses futurs salariés et ses partenaires sécurité et sûreté dans une logique de performance et non pas de coût. Tout l'enjeu est de trouver l'équilibre entre rentabilité et sécurité globale pour entrer dans une logique d'investissement.

Considérés à leur juste place, ces services et ces partenaires pourront auditer finement tous les risques et les menaces qui pèsent sur l'entreprise de manière globale : qu'ils soient internes (santé, sociaux, techniques, organisationnels, financiers, etc.) ou externes (politiques, environnementaux, commerciaux, liés à la production, à la sous-traitance, aux partenariats, au marché…). Les mesures qui ressortiront de cet audit impliqueront pour l'entreprise d'y affecter toutes les ressources techniques, financières, et humaines nécessaires optimales et efficaces avec un cout acceptable.

d. L'internationalisation : un facteur de complexité

Nombre d'entreprises parmi celles qui exportent et/ou qui sont implantées à l'étranger ont un modèle de fonctionnement qui dépasse les limites du territoire national et qui devient supranational. Les entreprises véritablement globalisées ne peuvent plus compter sur le seul État pour leur sûreté, pour se projeter à l'extérieur. Ainsi dans le cadre de la mondialisation, de nombreuses entreprises évoluent dans un cadre environnement international (juridique, économique, réglementaire…). Chez nos voisins européens, comme sur les autres continents, il semble très difficile de trouver une catégorie de salariés dédiés uniquement à la sûreté, à la santé et sécurité incendie. Il n'est d'ailleurs pas possible d'identifier d'autres qualifications (carte professionnelle, S.S.I.A.P) qui pourraient être équivalentes, dans l'esprit ou dans la forme, à celle en vigueur en France en matière de prévention de ces risques. A titre d'exemple la Suède reconnait une unique formation sécurité incendie et sûreté

Aux Etats-Unis, pays réputé pour la judiciarisation de sa société, potentiellement envisageable après de graves incidents, il n'a pas été jugé pertinent de mettre en place ce type de moyens dissociés (sûreté et sécurité). Il existe bien une formation spécifique dans le monde de la sécurité des hôpitaux (the Basic Certified Healthcare Security Officer), mais celle-ci ne se focalise pas sur la prévention incendie, cette formation aborde l'aspect plus large de la sécurité dans ce milieu hospitalier parfois sensible (proximité de produits dangereux, violence physiques, fragilité des patients).
D'autre part au Canada par exemple, s'il existe une loi sur la sécurité incendie, celle-ci, forte de cent quatre-vingt-six articles ne mentionne jamais la présence d'agents de sécurité dédiés à la prévention des risques incendie. En revanche, il est spécifié, dans le « Livre blanc sur la sécurité privée partenaire de la sécurité intérieure », rédigé par le ministère de la sécurité publique du Québec en 2003, que « la fonction de surveillance et de gardiennage inclut la sécurité incendie et les premiers soins ». Il n'y a pas dissociation de la santé-sécurité de la sûreté au quotidien. Il semble donc que ce soit une spécificité française.

L'efficacité de ce dispositif en France n'est plus à démontrer. Mais elle peut conduire à se poser une question différemment sur la séparation sûreté et santé-sécurité. L'absence de service de sécurité dédié à la prévention incendie à la française excluant la sûreté dans les autres pays est-il un facteur accidentogène ? Les buildings américains (ou qataris ou singapourien) sont-ils plus dangereux que nos I.G.H. ? La réponse n'est pas certaine.

e. La conformité à une nouvelle norme internationale ISO 31000

La conformité aux normes internationales représente un gage de confiance pour les consommateurs pour des produits et services sûrs, fiables et de bonne qualité. Les autorités de réglementation et les autorités publiques comptent sur les normes ISO pour étayer leurs réglementations, sachant qu'elles disposent

ainsi d'une base solide puisque les normes ont été établies avec le concours d'experts internationaux sur de très nombreux domaines.

La norme ISO 34001, publiée le 21/03/2018, s'adresse à tous les organismes devant prendre en compte un risque de **sûreté**. Elle insiste sur le fait qu'il est important de bien faire la part des choses entre **sûreté**, **sécurité** et **qualité**.
La norme ISO 34001 permet d'adresser, à travers un **système de management de la sûreté**, la protection de ses actifs contre des actes malveillants et frauduleux, alors que cette norme s'intitule, **« Sécurité et Résilience** », ce qui est étonnant !

A peine publiée, la norme ISO 34001 est déjà supplantée par la norme ISO 31000, intitulée, « Management des risques-Lignes directrices » qui a une vision plus globale, pour un management efficace du risque. Elle est publiée depuis le 9 juin 2018 et devrait aider les entreprises en fournissant un nouvel outil de management.
Elle n'est pas destinée à être utilisé à des fins de certification. Elle permettra aux entreprises d'identifier et de gérer les risques.
Contrairement aux systèmes de management normalisés existant dans les domaines de la qualité (ISO 9001), de l'environnement (ISO 14001), de la santé et la sécurité au travail (OHSAS 18001), ou de la responsabilité sociétale (SA 8000), qui permettent de maitriser les risques propres à un domaine particulier, la norme ISO 31000 permet un management global des risques. Elle a été élaborée pour aider les entreprises à intégrer les incertitudes de tout ordre dans leur système de management global.
La norme ISO 31000 introduit, comme le souligne l'Afnor, une méthodologie au service de l'identification et de la gestion de tout événement pouvant influer de façon positive ou négative sur l'atteinte d'un objectif.
La norme ISO 31000 fournit des principes, un cadre et des lignes directrices pour gérer toute forme de risque dans quelque domaine et quelque contexte que ce soit. Elle est structurée en trois parties qui sont :
-Les principes
-Le cadre organisationnel : intégration du management des risques dans la stratégie de l'organisation.
-Le processus de management : intégration du management des risques au niveau opérationnel à stratégique. Elle a également pour ambition d'harmoniser les processus de management du risque avec les normes existantes, telles que l'ISO 9001, l'ISO 14001 ou l'OHSAS 18001.

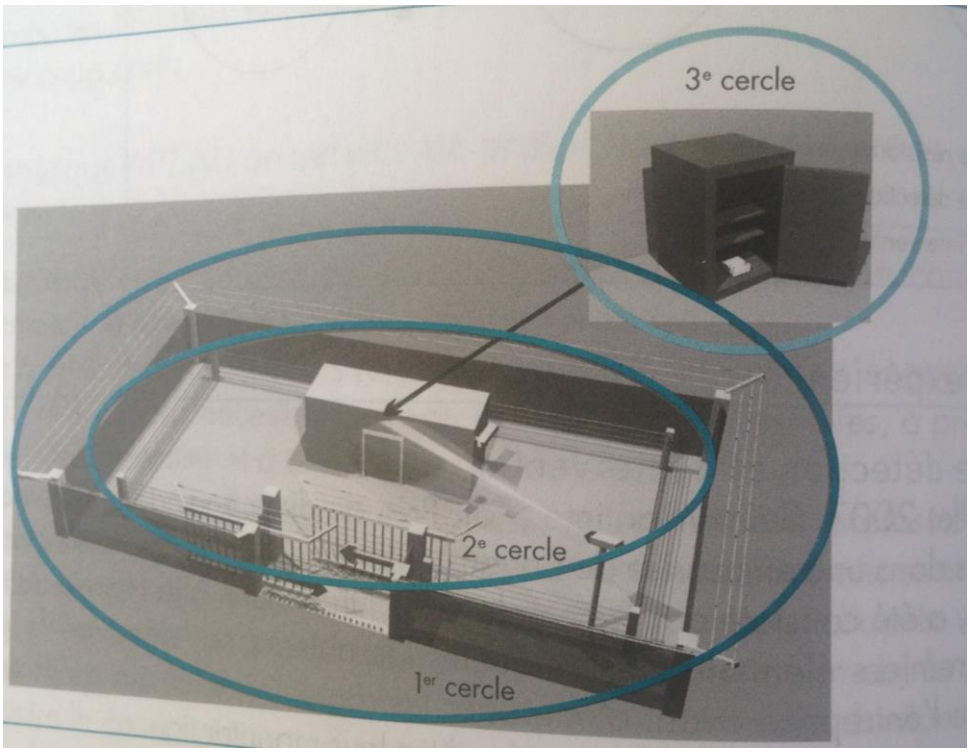
Le respect de cette norme, gage de vision moderne et d'efficacité de l'entreprise, nécessite d'intégrer la sûreté au sein de son domaine santé-sécurité.

3. Des similtudes indéniables de la conception à l'exploitation

a Des similarités dans les grands principes de conception

En conception, la sûreté comme la santé-sécurité, il est souhaitable de définir en priorité des dispositions de types préventifs. Les travaux de recherche et bon sens se rejoignent pour dénoncer la complexité comme leur ennemis communs. Plus les mesures sont considérées en amont de la conception, plus la mise en œuvre efficace et économiquement optimale. Les problématiques peuvent en effet avoir des impacts conséquents en termes l'implantation et le dimensionnement des ouvrages et d'organisation managériale.
Par exemple dans le cadre d'une installation de vidéo-surveillance, il est préférable de l'établir dès sa conception sinon le coût peut rapidement être prohibitif en fonction de la typologie des locaux. L'installation sera plus complexe (travaux à prévoir) et donc plus onéreuse puisque nécessitant de la main d'œuvre.

De plus les notions de risque et d'approches graduées évoquées jouent un rôle central en conception, dans les domaines. Elle s'appuie sur l'étude des dispositifs de protection sous forme concentrique de l'environnement extérieur jusqu'à l'objet sensible. Cette représentation permet d'adapter la protection au fur et à mesure que l'on s'approche de l'objet à protéger (voir schéma ci-dessous) :
-la protection périphérique (1ier cercle),
-la protection périmétrique (2ième cercle),
-la protection ponctuelle (3ième cercle).



Source CNPP : dispositifs concentriques de protection

b Des similarités dans les grands principes d'exploitation

En exploitation on trouve également un bon nombre de similitudes.
En outre la sûreté et la santé sécurité exigent toutes un suivi et une connaissance approfondie des procédures, des matériels et des personnels, ainsi il est indispensable de tenir des inventaires, le suivi des modifications, celui des éventuelles mesures palliatives temporaires…La notion de maintenance préventive joue un rôle également capital.
De plus le retour d'expérience doit être régulièrement et minutieusement traité. Il est alimenté par la mise à jour des référentiels et stimulé par le suivi rapproché des évolutions réglementaires, scientifiques et techniques. Ces conformités sont réexaminées par des audits et des revues internes.

Enfin la gestion des crises en sûreté comme en santé-sécurité est aussi semblable à plusieurs égards. Elle implique l'élaboration préventive de plan d'urgence et la réalisation d'exercices périodique. Ces derniers permettent de vérifier d'adéquation des plans et des moyens de crises, d'évaluer l'entrainement des intervenants et les délais associés aux étapes du plan, de tester les chaines décisionnelles, ou encore

d'améliorer les interfaces et la coordination entre les différentes entités impliquées. Ceci-dit, le détail de procédures et notamment les entités impliquées peuvent bien sûr changer selon la nature des risques.

c Sûreté, santé et-sécurité, les éternels rabats joies

Les domaines partagent un lourd fardeau : ils impliquent tous de se prémunir contre des évènements redoutés de nature « négative » (attaques, accidents), à l'opposé de résultats recherchés, de nature « positive » (service rendu, productions de biens). Ils sont souvent perçus comme des freins à la productivité ou plus généralement comme une entrave aux exigences fonctionnelles et aux objectifs des organisations. Dans ces conditions leur évaluation est particulièrement délicate. D'une part, elle nécessite de l'objectivité qu'il est difficile d'attendre des parties prenantes. D'autre part, elle requiert une connaissance fine de domaine sensible, peu compatible avec des intervenants extérieurs. De plus, alors qu'une gestion de risques efficace nécessite une bonne circulation des informations annonciatrices d'incidents (« signaux faibles »), elle est entravée par la tentation des responsables à les étouffer ou les gérer localement. La valorisation des efforts en sûreté comme en santé-sécurité est peut-être encore problématique. En simplifiant, les retours sur investissements concrets sont généralement difficiles à justifier des arbitrages budgétaires contraints.
Comme parade, le développement de cultures spécifiques à la gestion des risques sûreté et santé-sécurité, couplées à des obligations réglementaires adaptées, permet de responsabiliser le management et d'amoindrir les difficultés mentionnées.
On entend par cultures spécifiques (culture sûreté et santé-sécurité), l'ensemble de caractéristiques et des attitudes qui, dans l'organisme et chez les personnes, font que les questions de sûreté/santé/sécurité bénéficient, en tant que priorité absolue, de l'attention qu'elles méritent en raison de leur importance. Dans cette acceptation, toutes partagent d'importantes ressemblances : l'engagement explicite de la direction, une politique volontariste de formation, et l'assimilation par chacun des enjeux et de sa place à jouer en termes de sûreté, de santé et de sécurité. Ce sont d'indispensables composantes. Pour cela, la croyance dans la crédibilité des menaces est fondamentale. Les cultures doivent nourrir une attitude de vigilance générale et un questionnement proactif permanent. Le partage et l'échange d'information y sont également centraux (mais dans des modalités différentes). Ainsi le Directeur sûreté, santé-sécurité doit être le chef d'orchestre de ses cultures spécifiques pour en ressortir une savante mélodie.

4. Le futur rôle du Directeur Sûreté, Santé-Sécurité (DSSS): une fonction tranverse

a Aujourd'hui

Aujourd'hui, le Directeur SSS, est un expert en charge de la sûreté, sécurité des personnes et des biens, aux respects des normes, et à la fiabilité des installations. Il veille à réduire l'impact de l'activité industrielle sur l'environnement, les nuisances et aide l'entreprise à préserver son niveau de production et de performance.
Dans le cadre de ses fonctions, il conseille et assiste la direction de l'entreprise pour la définition de sa politique de sécurité (sûreté-malveillance, sécurité incendie, hygiène et sécurité au travail, conditions de travail, et protection de l'environnement) en assure la mise en place, l'animation et le suivi. Il établit des programmes de prévention afin de réduire le nombre d'incidents, d'accidents, de maladies professionnelles et leur coût. Il anime et dirige des équipes de techniciens ou de cadres.

Actuellement la majorité des managers ne couvre que partiellement le domaine comme l'indique la pluralité des dénominations :
-Directeur Prévention,
-Directeur Sûreté
-Directeur Sécurité
-Directeur HSE,
-Coordonnateur sûreté et sécurité
-Directeur de la sécurité du site…

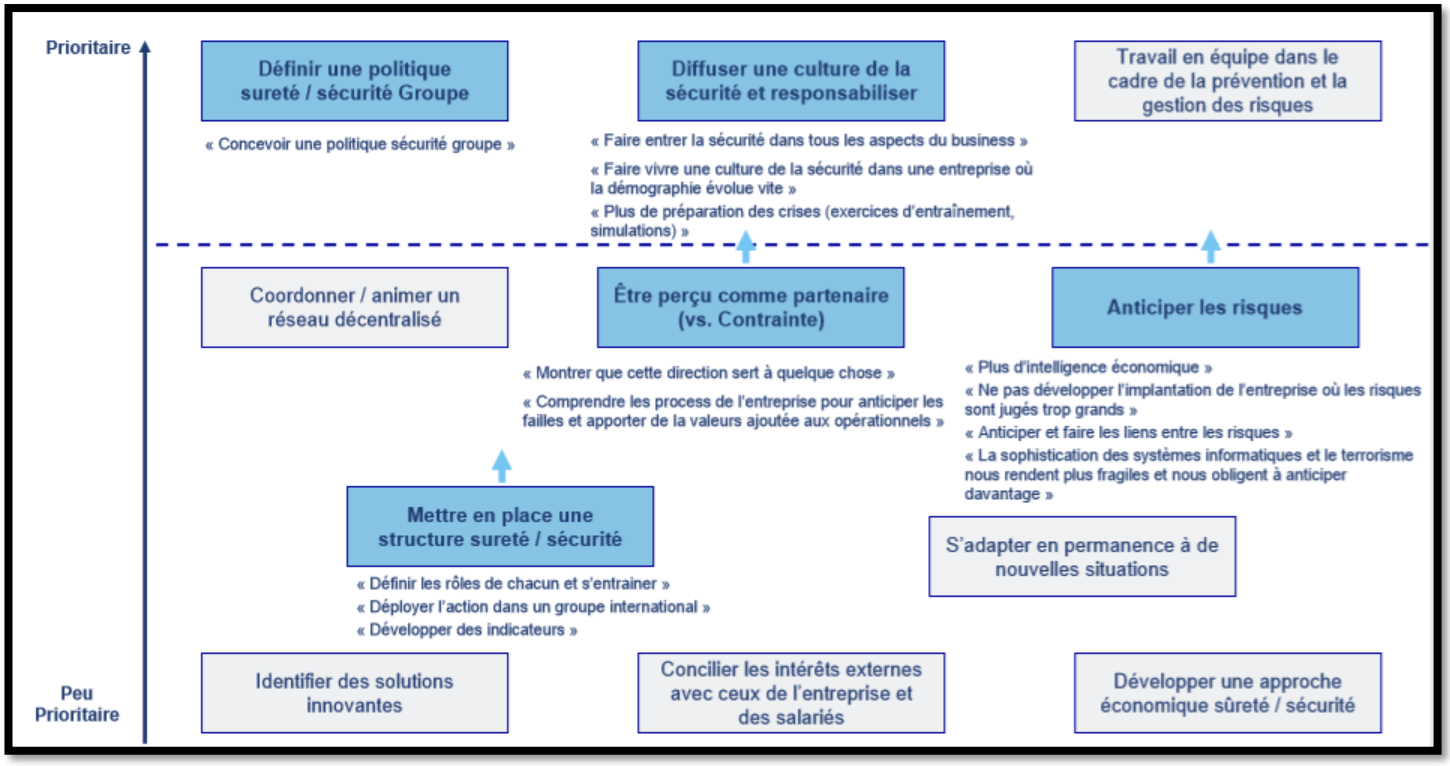
Ainsi les compétences et les profils recherchés des managers du domaine sont liés à la nature des risques majeurs spécifiques à l'entreprise et à ses conséquences sur les biens, les salariés et sur la continuité de l'activité de l'entreprise.
Il est donc impératif que le manager ait une excellente connaissance de l'entreprise et de son cœur de métier pour qu'il ne devienne pas un frein mais un acteur. Il doit pouvoir réagir vite à des nouvelles situations grâce à des solutions innovantes et à son réseau qu'il a su développer et gérer en toute humilité.

b Demain

Dans l'avenir, ce poste devra être celui d'un véritable manager des risques et des crises dans l'entreprise, rattaché à un membre du comité exécutif et qui jouera un rôle de conseiller opérationnel et stratégique auprès de la direction. Ainsi ce domaine transverse aura toute la légitimité hiérarchique et ne sera pas perçu comme un frein mais acteur du management des risques
Pour effectivement déployer une approche globale, la direction sûreté, santé-sécurité devra travailler en *business partner* avec le reste de l'entreprise et organiser/développer les activités du domaine de l'entreprise en maitrisant les enjeux de l'entreprise. A cela s'ajoute un « leadership » incontestable consolidé par ses compétences d'expert.

Ainsi pour répondre à toutes ces attentes, il est impératif que le DSSS outre son besoin d'anticipation, soit capable à la fois d'être un homme d'action (acteur/coordinateur) tout en prenant du recul sur les évènements.
Pour cela il faut être capable :
-d'organiser des campagnes de communication interne (sensibilisation),
-de comprendre les évolutions organisationnelles et technologiques pour les anticiper et les accompagner d'un point de vue sécurité/sûreté,
-comprendre la mécanique de contrôle de gestion pour répondre aux arguments sur les coûts, pour maîtriser ses indicateurs et faire passer ses projets,
- être capable de donner de l'élan à ses équipes, analyser la prise de décision sous pression et les racines des comportements anormaux…

Le schéma ci-dessous priorise les tâches et les qualités que doit détenir actuellement un DSSS. Les axes d'évolution du DSSS de demain sont symbolisés par les flèches bleues. Certaines permettent de faire franchir l'axe en pointillé matérialisant ce qui prioritaire et ce qu'il l'est moins.



Source Hay Group SA

c Bilan

Le tableau ci-dessous décline ainsi une synthèse des évolutions pour devenir le DSSS de demain :

Aujourd'hui	Demain
J'installe une politique sûreté-sécurité Je diffuse une culture de la Sécurité au sein de mon entreprise	J'installe une politique sûreté-santé-sécurité Je diffuse une culture sécurité au sein de mon entreprise
Je réagis	Je structure J'anticipe, je prévois Je réagis vite
Je résous des problèmes de manière empirique	J'installe des méthodes des procédures, mesure de contrôle et retour d'expériences
Je suis un expert, un spécialiste : je suis consulté sur le management des risques et sur le pilotage des crises	Je comprends les processus de l'entreprise. Je suis un « business partner »

5. Conclusion

Nous avons vu dans ce chapitre, l'intérêt d'une vision globale et moderne d'intégration de la sûreté au sein de la santé -sécurité pour l'entreprise ou son environnement (étatique, contexte sécuritaire, international, opinion publique, marché de l'emploi…) en perpétuelle évolution.
Le prochain permettra d'en définir les modalités.

IV La mise en place d'une fonction transverse Sûreté, Santé-Sécurité au sein de l'entreprise.

L'objectif d'intégrer la fonction sûreté au sein d'un service Santé-Sécurité n'est pas une fin en soi. Elle doit apporter une solution à l'entreprise afin de répondre aux nouveaux enjeux et à l'ensemble des risques évolutifs auxquels elle est confrontée. Pour cela elle devra passer par un processus systémique de la gestion des risques. La réalisation de celle-ci deviendra ainsi le socle de la mise en œuvre et du maintien d'un système de management Sûreté, Santé-Sécurité face à des dangers et menaces internes et externes. Pour que cette mise en place soit réussie, il est indispensable de bien définir le rôle de ses nouveaux acteurs pluridisciplinaires : directeur Sûreté, Santé-Sécurité, agent polyvalent de la sécurité… Le point essentiel d'une intégration pérenne et efficace est que l'ensemble du personnel y adhère et soit impliqué dans cette mise en place.

Nous allons définir dans les parties suivantes les phases allant du processus de gestion des risques à la mise en place des nouveaux métiers via une démarche de système de management.

1 La gestion des risques, une approche globale

a Une méthodologie s'appuyant sur le management du risques et un engagement de la direction

La gestion des risques est le processus général d'estimation de l'étendue des risques et de prise de décision concernant l'acceptation de ces derniers. Par analogie la gestion des risques se rapproche de l'évaluation des risques dans une étude de danger. Elle implique donc l'identification des dangers/menaces et des conséquences possibles des accidents involontaires ou volontaires sur le fonctionnement de l'organisme.

La méthode proposée s'appuie sur les principes et les concepts génériques du management des risques. Elle repose donc sur une approche itérative et a pour objectifs :

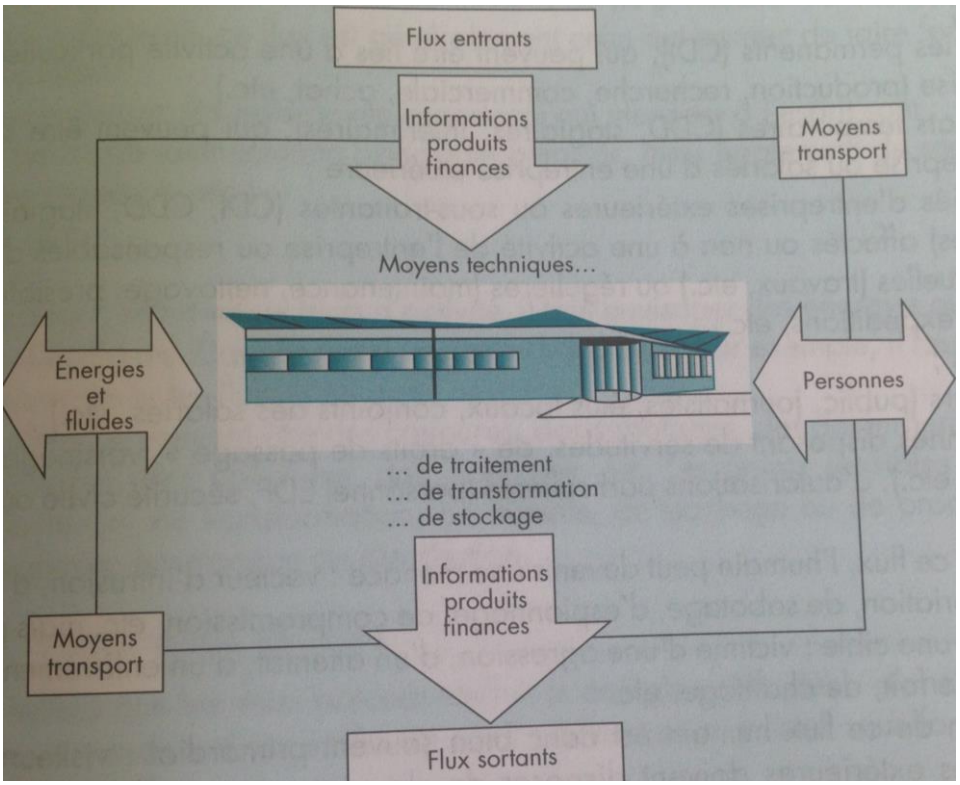
- d'identifier les fonctions névralgiques (biens matériels, immatériels, personnel…)
- d'identifier et de caractériser les scenarios de risques identifiés,
- de traiter les risques,

Dans ce cadre, il est indispensable que la direction s'engage tout d'abord en faisant mener cette réalisation dans le cadre d'une gestion de projet (objectif, désignation d'une équipe et du comité de pilotage, calendrier, moyens, délais...).
Son engagement ne s'arrête pas là. La direction doit fixer également le seuil d'acceptabilité des risques et valider les composantes des plans de prévention, plan de surveillance et de continuité d'activités. Elle attribue les ressources nécessaires et s'assure des révisions engendrées par les potentielles évolutions des menaces/danger.

b Première phase : identification des fonctions névralgiques

Cette phase est essentielle pour la bonne conduite de l'analyse et repose sur un examen global de l'entreprise permettant de recueillir l'ensemble des informations nécessaires à la mise en évidence de ses fonctions névralgiques (bien matériel, immatériel, personnel). Ces informations portent principalement sur:
-les flux de production (matériels), d'informations (immatériels) et de services,

-les flux humains,
-les énergies,
-l'organisation humaine des différentes fonctions (financière, sécurité, sûreté…),
-les marchés sur lesquels l'organisme est positionné,
-l'étude de l'environnement de l'entreprise (géopolitique, localisation, moyens d'accès, délais de ralliement des moyens de secours/police…).



Source CNPP : Les flux de l'entreprise

c Deuxième Phase : identification et caractérisation des scénarios de «source de danger-cible »

Le préalable à toute démarche de gestion des risques consiste à identifier, de manière la plus exhaustive possible, tous les scénarios danger-cible pour l'entreprise pouvant conduire à sa remise en cause ou au non-respect de ses objectifs. Pour entreprendre ce recensement plusieurs techniques peuvent alors être utilisées, puis combinées : l'analyse de la documentation existante, l'interview d'experts, la réalisation de réunions de brainstorming, l'utilisation d'approches méthodologiques (comme l'AMDEC, les arbres de causes…), la consultation de bases de données de risques rencontrés lors d'études antérieures ou encore l'utilisation de check-lists ou de questionnaires préétablis couvrant les différents domaines du projet.

La survenue des risques peut être alors définie par un scénario élaboré en déterminant :
- la source de danger/menace (ou éléments initiateurs) interne ou externe,
- le mode d'action de la source sur la cible
- la cible impactée
- la conséquence de l'atteinte de la source de danger sur la cible.

L'exploitation des informations recueillies dans la première phase, conjuguée à des recensements utilisant plusieurs techniques ci-dessus, permet d'établir les scénarios « source de danger-cible ».

Il convient ensuite d'analyser, de manière plus ou moins détaillée, les causes et les incidences potentielles des scénarios, et de les caractériser. Il s'agit également d'examiner les interactions possibles et les combinaisons éventuelles, afin de déceler les risques qui peuvent en découler et compléter ainsi la liste de risques déjà identifiés. L'objectif de cette quantification est alors double. Il est nécessaire, de bien distinguer parmi les risques préalablement identifiés, ceux qui n'en sont pas ou qui sont non fondés, et qu'il convient par conséquent de rejeter de l'analyse, et ceux qui sont réels et susceptibles d'affecter le bon fonctionnement de l'entreprise. Ces derniers demandent alors une attention constante et doivent faire l'objet d'un traitement et d'un suivi particuliers.

La caractérisation des risques est une phase quantitative. Pour cela il faut affecter d'une valeur chiffrée à chacune des deux composantes :
-à la source de danger : il s'agit de caractériser sa fréquence,
-à la cible: il s'agit de caractériser de sa gravité d'atteinte.

Il n'existe pas de cotation absolue pour la fréquence et la gravité. La classe de fréquence doit être appréciée avec des critères les plus objectifs possibles qui sont propres à l'entreprise. Elle s'appuie sur les données statistiques dont elle dispose par exemple : le taux d'accident de travail sur un type de machine dans son secteur d'activité, le taux de délinquance de la région, taux d'arrêt de travail,…
La gravité d'atteinte de la cible quant à elle, peut s'effectuer suivant deux classes de mesure quantitatives (coût direct ou indirect de la valeur en euros de la perte du matériel, de l'arrêt de l'exploitation…et qualitatives (atteinte à l'image de l'entreprise, dégradation de climat social…).
La finalité de cette quantification est de pouvoir ainsi se focaliser sur les risques prépondérants, de préparer les parades les plus efficaces possibles et de définir les actions à mener en priorité pour les maîtriser.

Une fois les risques évalués, il convient ensuite de les hiérarchiser, c'est-à-dire fournir un ordre de grandeur permettant de distinguer les risques acceptables des risques non acceptables pour l'entreprise. Le but de cette hiérarchisation est d'apprécier l'impact de chacun des risques détectés et de déterminer globalement le niveau d'exposition aux risques. Une matrice de criticité est une représentation schématique qui permet de visualiser facilement les scénarii des risques identifiés et de les hiérarchisés en acceptables, inacceptables et maitrisés.

Ci-dessous un exemple de matrice de criticité de caractérisation du scénario en croisant la fréquence de la source de danger (classé de 1à 4) et la gravité des atteintes (de 1 à 4). Ainsi on obtient l'apparition de 3 zones :
-La verte (de 4 à 9) correspondant aux scénarii de risques acceptables c'est-à-dire sous le seuil de vulnérabilité fixé à 10 déterminer par l'entreprise. (risques non significatifs)
-L'orange (de 12 à 18) correspondant à la zone de risques à mettre sous vigilance renforcée avec des indicateurs et de prendre les mesures de prévention. (risques maitrisés)
-La rouge (supérieur à 20) correspondant aux scénarii inacceptables qui imposent de mettre en place doit effectuer de mesure de prévention et de protection. (risques confirmés)

Source internet: matrice de criticité

d Troisième phase : le traitement des risques

Le management des risques consiste également à les traiter, c'est-à-dire définir et mettre en œuvre les dispositions appropriées pour les ramener à un niveau acceptable et les rendre ainsi plus supportables. Cela nécessite donc de définir des réponses types et de mettre en œuvre, risque par risque, un certain nombre d'actions visant soit à supprimer ses causes, soit à transférer ou partager sa responsabilité ou le coût du dommage à un tiers, soit à réduire sa criticité (en diminuant sa probabilité d'apparition ou en limitant la gravité de ses conséquences), soit à accepter le risque tout en le surveillant.

Dans ce cadre l'entreprise peut mettre un plan de surveillance. Un plan de surveillance est à la fois un document et une stratégie regroupant l'ensemble des contrôles à réaliser (autocontrôles, contrôle hiérarchique, contrôles délégués…). Les différents contrôles sont réalisés sur différents thèmes (gestion des documents classifiés, suivi du matériel incendie, épreuve des matériaux de levage..). De même sont intégrés au sein du plan de surveillance, les mains courantes et de l'historique des différentes détections utilisées. Ce plan est élaboré à partir des risques et défauts potentiels identifiés. Il vise à garantir une « conformité » à certains critères via la mesure d'indicateurs et/ou d'indices. C'est un outil de prévention visant à éviter ou limiter les crises et il est souvent l'un des éléments d'une dynamique de gestion des risques et reste un élément important d'une démarche qualité.

Ainsi un plan de surveillance définit :

- la responsabilité de la personne en charge la sûreté, santé-sécurité,
- le plan de gestion de la qualité;

- la liste des équipements, systèmes et infrastructures faisant l'objet de la surveillance;
- l'organisation de l'équipe de surveillance (des accès, biens matériel, habilitation,..)
- les procédures applicables à la surveillance (vérifications, essais, changements, qualité, etc.);
- le plan d'inspection et d'essai;
- les critères d'acceptation;
- la liste des documents à recevoir,
- le format et le contenu des rapports de surveillance à produire,
- les politiques et les procédures de projets du maître de l'ouvrage qui ont un impact sur la surveillance (ex. : gestion des changements).

2 Un système de management global des risques : le système de management Sûreté,Santé-Sécurité

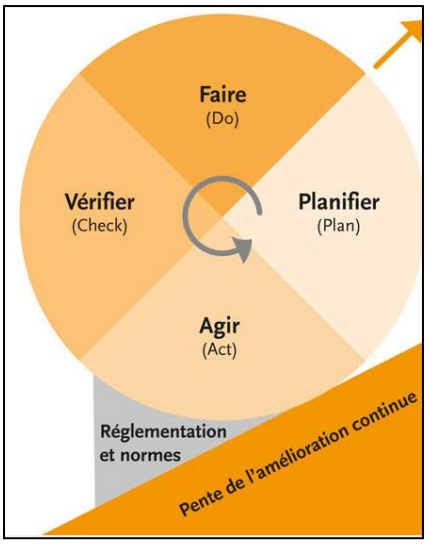
Une fois ce processus de gestion de risques réalisé, il est possible de d'entreprendre la mise en place d'un système de management global, sûreté, santé-sécurité afin de rendre efficace et pérenne cette démarche grâce à une implication forte de la direction. Cette partie propose un système de management sûreté, santé-sécurité élaboré par la synthèse de différentes lectures.

a Des exigences générales

Un système de management de la sûreté, sécurité-santé au travail a pour objectif de prendre en compte l'amélioration des conditions de travail, de manière globale et partagée par tous les acteurs de l'entreprise. Il s'agit d'une méthodologie de gestion de la performance de la basée sur des politiques de prévention, des procédures, des plans d'action, impliquant chaque niveau de responsabilité. Le schéma de développement d'un système de management de la sûreté, santé-sécurité s'élabore à partir d'un projet d'entreprise et s'inscrit dans une dynamique de changement qui requiert de la pédagogie, une démarche participative et collaborative.

Ainsi ce Système de Management de la Sûreté, Santé-Sécurité doit être l'outil de l'entreprise pour améliorer et structurer sa réponse aux obligations réglementaires, pour faire de la prévention des risques un facteur de performance de l'entreprise. Il en résulte une meilleure maitrise des risques professionnels, une meilleure prévention des actes de malveillance, des accidents du travail, des maladies professionnelles et des conformités réglementaires.

La démarche repose sur une méthodologie « Planifier, Mettre en œuvre, Contrôler, Agir (Plan, Do, Check, Act PDCA) selon le principe de l'amélioration continue.



Source internet ; la roue de Deming

Cette méthode proposée, en sept étapes, vise à mettre en place de manière progressive un processus de management de la sûreté, santé-sécurité. Chaque étape présente des objectifs et résultats à atteindre.

b Première étape : le lancement de la démarche

Le lancement d'une démarche sûreté, santé et sécurité est une décision responsable de l'entreprise vis à vis de l'ensemble du personnel qui doit être proportionnée aux risques de l'organisme. Plusieurs éléments qualitatifs ou quantitatifs incitatifs sont disponibles afin d'aider le chef d'entreprise à prendre cette décision : financiers (taux de cotisation…), organisationnels (nombre d'acte de malveillance, nombre d'accidents du travail et maladies professionnelles…), juridiques (contentieux civil et/ou pénal), commerciaux (image de marque…) et sociaux.

L'annonce officielle de la démarche globale, sûreté, santé et sécurité au travail et la sensibilisation du personnel peuvent se faire dans le cadre d'une réunion générale au cours de laquelle la direction (la personne ou le groupe de personnes qui possède la responsabilité du fonctionnement de l'organisme) informe le personnel.

Le choix de l'animateur potentiel directeur sûreté, santé-sécurité au travail doit être en rapport avec l'effectif de l'organisme et il est conseillé de s'appuyer sur une personne ayant des capacités d'animation et de communication avérées. Le profil sera développé dans le chapitre 3 de cette partie.

Une attention particulière doit être portée à la participation effective des salariés (y compris personnel temporaire) à cette démarche. Le domaine d'application doit inclure les activités pour lesquelles tous les salariés de l'organisme, y compris le dirigeant, peuvent être exposés. Il doit inclure également les activités exercées par les entreprises extérieures. A dessein de communication un classeur peut être créé afin d'y archiver toutes les informations et documentations relatives à la démarche sûreté, santé et sécurité.

Cependant la responsabilité pénale repose sur l'employeur ou le chef d'établissement. L'animateur sûreté, santé et sécurité au travail ne peut donc avoir qu'un rôle de conseil et d'appui du dirigeant dans la démarche.

c Deuxième étape : Politique, structure et responsabilité indispensable pour l'intégration de la sûreté

L'objectif est de définir une politique de sûreté, santé-sécurité et de communiquer les rôles, responsabilités et délégations des autorités impliquées dans la mise en œuvre et le suivi du système de management sûreté, santé-sécurité. Cette structure doit garantir la disponibilité des ressources nécessaires (humaines et financières).
Il est conseillé d'intégrer l'élément sûreté dans les fonctions existantes de la santé-sécurité. L'intégration de certaines règles au règlement intérieur de l'entreprise doit faciliter la portée à la connaissance du personnel, salarié ou non, la contractualisation ainsi que l'évaluation effective visant au respect de ces règles. Pouvant être intégrées au règlement intérieur celle-ci portent notamment sur les dispositions d'accès à l'entreprise, le port du badge, la préservation des informations sensibles…

Il est souhaitable que la mise en œuvre de l'intégration de la sûreté soit à la charge du directeur ou responsable sûreté. Si pour raisons de positionnement hiérarchique, de disponibilité, ou de compétence, cette intégration ne peut lui être confiée, une autre personne doit être désignée. Cela peut être par exemple son N+1: le directeur en charge de l'ensemble des domaines : sûreté, santé et sécurité. Dans ce cas, un fonctionnement « en binôme » doit être mis en place entre les deux personnes pour permettre l'intégration des composantes techniques et organisationnelle.

d Troisième étape : Objectifs, programme de réduction des risques

A partir de la politique sûreté, santé-sécurité, des exigences légales et du processus de gestion des risques qui permet de dégager les risques majeurs, l'entreprise doit donc définir les objectifs (axes d'améliorations) et élaborer un programme permettant d'atteindre ces derniers.
Pour cela il faut définir un calendrier de réalisation et un tableau de bord regroupant les actions, les indicateurs et les échéances permettant de juger de la mise en œuvre et l'efficacité des mesures prises.
Le tableau de bord doit hiérarchiser les actions prioritaires et les voies de progrès en matière de:

- moyens de prévention à affecter et les délais de réalisations,
- moyens de protection à affecter et délais de réalisations,
- sensibilisation et d'adhésion du personnel,
- formation et compétence (par exemple polyvalences des agents sûreté-sécurité),
- modalités de fonctionnement en cas de situation dégradée,
- maîtrise opérationnelle (établir, mettre en œuvre et tenir à jour des procédures documentées pour maîtriser les situations où l'absence de telles procédures pourrait entraîner des écarts par rapport à la politique environnementale et aux objectifs et cibles,
- gestions des situations d'urgences.

e Quatrième étape : Communication

L'objectif de cette étape est de favoriser la mise en place d'actions de communication interne en matière de sûreté malveillance et de ses interactions avec le domaine de la santé-sécurité (incendie volontaire, intoxication alimentaire, protection du patrimoine intellectuel…) afin de permettre une sensibilisation du personnel au regard des enjeux de l'entreprise.
L'organisme a de nombreuses occasions de communiquer vers l'externe (salons professionnel, sites internet de l'entreprise, visites de l'entreprise, plaquettes d'informations...). Dans le cadre de l'intégration de la sûreté et de ses procédures, il est important que des dispositions soient prises afin de maîtriser la diffusion des informations sensibles. En effet l'information est une valeur à protéger. Elle peut être disponible sur différents supports d'enregistrement (papier, électronique…). La gestion des documents et des données relatifs aux biens et informations sensibles de l'entreprise revêt un caractère important dans

une approche « protection du patrimoine intellectuel ». La maitrise des informations sensibles et de sa communication étant un point clef, il est important de sensibiliser les personnes détentrices de l'information et les chargés de communications afin qu'ils puissent travailler ensemble sur ce que l'on peut dire ou pas. Ceci nécessite de mettre en place des formations pour les « communicants » et l'élaboration d'une procédure de validation des modalités de communication (appelées communément « éléments de langage » Et si l'entreprise possède déjà une politique de communication externe elle doit intégrer la sûreté, santé-sécurité dans celle-ci.

f Cinquième étape : surveillance du niveau de performance

Cette étape vise à mettre en œuvre des actions de surveillance permettant la pérennité, la fiabilité des fonctions sûreté, santé-sécurité qu'elles soient organisationnelles et/ou techniques. Ceci s'appuie le processus de gestion des risques réalisé en amont et notamment sur le plan de surveillance.

De plus la menace étant évolutive, le portefeuille des risques potentiels doit être réajusté en fonction des nouvelles informations recueillies. Certains risques pouvant disparaître, d'autres apparaître ou d'autres encore, considérés initialement comme faibles, pouvant devenir rapidement inacceptables pour l'entreprise dès lors qu'ils n'ont pu être maîtrisés, le niveau d'exposition aux risques est amené à changer. C'est pourquoi il est important de procéder périodiquement au suivi et au contrôle des risques encourus. Ainsi il est important de mettre à jour la liste initiale des risques identifiés, d'affiner les données caractéristiques des risques déjà connus, de réévaluer leur criticité, de contrôler l'application des actions de maîtrise, d'apprécier l'efficacité des actions engagées, et de surveiller le déclenchement des événements redoutés et leurs conséquences. Ceci n'est possible qu'avec la mise en place d'indicateurs simples découlant de l'analyse des risques (nombre d'actes de malveillance…) et des indicateurs plus élaborés tels que des indicateurs d'efficacités (exercices grandeur nature, simulation, test de situation de crise…).

g Sixième étape ; Incident, événement involontaire ou volontaire, non-conformité, action correctives et préventives

Comme dans tout système de management, il est recommandé de mettre en œuvre une organisation permettant à tout membre de l'entreprise de détecter et de faire remonter tout incident, presqu'incident (presqu'acte de malveillance, presqu'accident) et non-conformité relative au système de management. L'amélioration continue repose en partie sur ses évènements sans être assimilé à de la délation.

L'analyse en deux phases est une réponse souvent efficace :
- une analyse à chaud : examen des faits, sans formalisme spécifique, donnant lieu à des actions immédiates,
- une analyse à froid avec un formalisme précis et donnant lieu à des actions correctives et préventives, celle-ci est pilotée par un comité.

h Septième étape Contrôle périodique : audit interne et revue de direction

Le cadre de la réalisation d'audit interne et de revue de direction du système de management de la sûreté, santé-sécurité ainsi que les procédures applicables sont identiques aux autres systèmes de management (qualité, environnement…).
En effet les audits internes portent tout d'abord sur la conformité puis ensuite une fois que celle-ci est avérée, sur l'évaluation de l'efficacité du système de management.
Concernant la revue de direction, elle permet à la direction de définir de nouveaux objectifs.

3 Un focus sur les nouveaux métiers de la fonction transverse du Sûreté, santé-sécurité

Les métiers des domaines sûreté, santé et sécurité sont en pleine mutation pour ne devenir d'une fonction transverse de l'entreprise travaillant en « business partner » avec tous les autres acteurs de l'entreprise. Leur mise en place doit faire l'objet d'une démarche participative.

a Le nouveau rôle du Directeur Sûreté, Santé-Sécurité

Rattaché au comité exécutif et véritable manager des risques et des crises dans l'entreprise, le Directeur sûreté, santé-sécurité joue un rôle de conseiller opérationnel et stratégique auprès de la direction. Cette fonction transverse, armée d'une vision globale travaille en étroite collaboration avec le reste de l'entreprise.

Ainsi en accord avec la politique globale, il devra définir une politique sûreté, santé-sécurité et énoncer clairement ses objectifs généraux. Grâce à sa capacité d'anticipation et sa vision stratégique des crises, et à la mise en place et à la coordination des procédures sûreté, santé-sécurité, il doit être capable très rapidement de faire face à des risques nouveaux et émergents causés par une menace intelligente et adaptive.
Excellent communicant, il est garant de la diffusion et du respect de la culture sûreté, santé- sécurité dans l'organisation grâce à des campagnes de communication interne (sensibilisation).
Il doit établir et tenir à jour un programme et des procédures pour la réalisation périodique d'audits sur les process opérationnels, détecter des failles et manques à gagner pour être perçu comme un partenaire.
Il anime un réseau décentralisé et des process sur place pour faire vivre la culture sûreté, santé-sécurité.
Son Leadership lui permet de former les opérationnels pour se dégager du quotidien et en cas de gestion de crise il peut s'appuyer en cas de besoins sur un réseau développé de sachants / référents sécurités.
Doté d'un discernement aiguisé et de recul, la prise de décision se fait dans une optique d'optimisation risques/coûts, il est consulté systématiquement et prioritairement lors de la prise de décisions business ayant des enjeux sécurité. Il pilote l'identification et le management des risques.

Afin d'évaluer la qualité des services rendus, il met en place des facteurs de performance. Il s'appuie sur des indicateurs de diffusion de la culture (ex: autoévaluation des opérationnels sur leur capacité à prévenir/gérer les crises) et des résultats mesurés à long terme.

b Les différents métiers du collaborateur Sûreté, Santé-Sécurité

La nouvelle mission des collaborateurs de la sûreté, santé-sécurité doit être globale, préventive et simultanée, mais cela ne veut pas dire que tous soient des experts dans les trois domaines.
Auparavant les partisans de la polyvalence et ceux de la spécialisation semblaient bien opposés. Cet affrontement n'est plus d'actualité, il faut des généralistes et des spécialistes, une vision globale et des expertises pointues. En effet il faut dans la majorité des cas former des personnes polyvalentes pour réaliser le panel des missions dédiées (développées ultérieurement) mais aussi des experts qui soient capables de conseiller de manière fine et pertinente aux questions des différents domaines (sûreté, santé et sécurité…). Ces experts ne doivent pas forcement être au sein de l'entreprise. Ils peuvent faire partie des sièges de groupes, dans des organismes de formation ou dans des sociétés d'audit et de consultants.

Le but n'est pas non plus la polyvalence à outrance, il est nécessaire de se poser la question du besoin de l'entreprise (environnement, risques spécifiques, réglementation…) pour ne pas dégrader le niveau de compétence. Par exemple si l'entreprise de l'industrie chimique conserve un contrat d'externalisation pour le contrôle des accès, il n'est pas nécessaire de former tout le personnel à cette fonction au détriment de

leur cœur de métier, le risque chimique. Il suffit de former le directeur et son adjoint afin qu'ils puissent définir de nouveaux besoins et contrôles les services rendus.

La majorité des collaborateurs sera en charge de missions polyvalentes telles que (liste non exhaustive) :
-contrôle d'accès (entrée/sortie) : surveillance, inspection des cargaisons, palpations de sécurité,
-vidéo surveillance sur site ou déportée : opérateur de vidéosurveillance ou télé vidéosurveillance
-levée de doute sécurité/sûreté,
-ronde/prévention : incendie, évacuation, santé au travail, dissuasion, respect des règlements intérieurs…
-assistance à la personne ; lutte contre les incivilités, gestion colis suspect, secours à la personne…
-protection des biens : lutte contre le vol, vandalisme incendie…
-protection des biens immatériels : patrimoine intellectuel, sécurité informatique
-contrainte physique : interpellation, rétention…
-maintenance de tous les moyens de secours
-formations : gestes et postures (TMS), gestion du stress et harcèlement agression (RPS), incendie…

A cela peut s'ajouter l'utilisation de nouvelles technologies telles que l'utilisation de drones qui permettent
-Le contrôle des zones sensibles et de leurs abords immédiats
- La surveillance des flux (véhicules, piétons…)
- L'appui aux services d'intervention et de secours
- Observations, levées de doutes, enquêtes…
- Compléter les dispositifs de sécurité déployés (vidéosurveillance, agents de sécurité,…)
- Prévention/dissuasion

c Les conditions de succès à la mutation des métiers Sûreté, Santé-Sécurité

Comme dans une démarche de mise en place d'un système de management, la mutation des métiers sûreté, santé-sécurité s'appuie également sur une approche systémique, c'est-à-dire de sa fonction dans son environnement (environnement international, entreprise très décentralisée, variété des risques, secteur exposé…) et des enjeux de l'entreprise (sociétaux, économiques et financiers...).

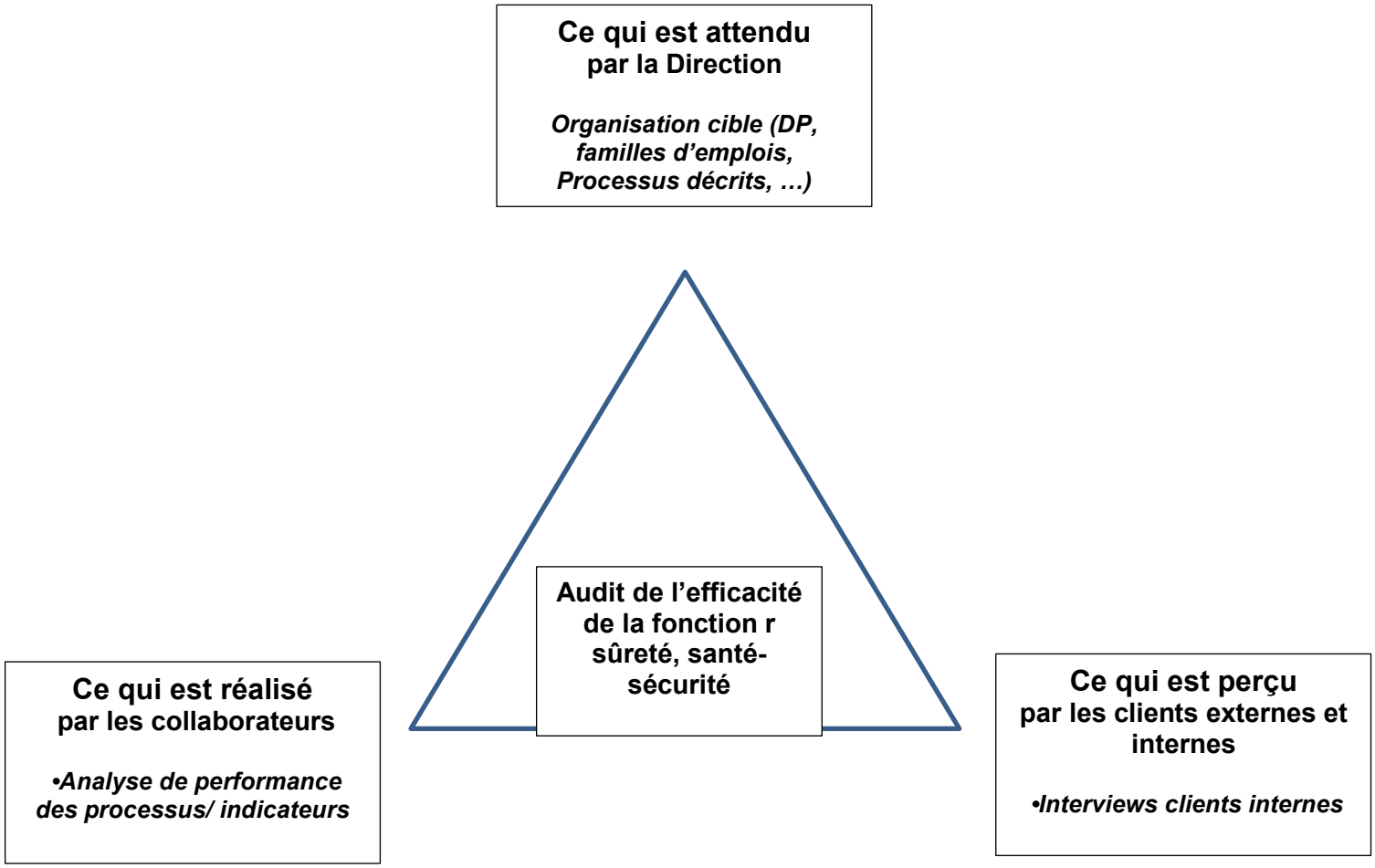
Le directeur sûreté, santé-sécurité doit ainsi réaliser les 3 actions clefs suivantes pour assurer l'installation et la reconnaissance des métiers :
-l'élargissement de l'étude à des benchmarks internes et externes,
-l'approfondissement et appropriation des résultats de l'enquête (groupes projet),
-l'analyse de l'efficacité rôle au sein d'une organisation (autodiagnostic)

Dans un premier temps, l'élargissement de l'étude à des benchmarks internes et externes permet la recherche de meilleures pratiques au sein du groupe ou au sein d'autres entreprises dans le domaine :
-l'organisations / rôles
- les Modes de fonctionnement
-processus,
-compétences, …
Le benchmark peut ainsi servir à la direction sûreté, santé-sécurité afin de dresser un panorama de l'existant avant de lancer d'installation de la fonction.

Dans un deuxième temps, il s'agit de l'étape d'approfondissement et d'appropriation des résultats de l'enquête par le groupe de projet minutieusement choisi.
Pour la mise en place d'une démarche, il est conseillé de constituer une équipe qui pourra piloter le projet et donner les axes d'amélioration. La constitution de ce comité reste à la charge de l'employeur. Une

proposition des acteurs peut être la suivante : délégué du personnel, ressources humaines, préventeur, agent de sécurité incendie, agent de sûreté, directeur sûreté, coordonnateur HSE (si poste existant dans la structure). Le rôle de chaque acteur dans ce comité devra être défini au préalable afin d'obtenir un pilotage efficace. Il pourrait être intéressant de faire porter la démarche par l'ensemble des acteurs concernés et non pas exclusivement ceux qui « gèrent » le Sécurité dans l'entreprise.
Le chef de projet serait donc le futur manager du domaine qui aurait la responsabilité de planifier les réunions et d'inviter des intervenants extérieurs suivant les besoins du projet (médecin du travail, psychologue du travail, responsable informatique…). Cependant, il est nécessaire de choisir ces personnes avec grand soin puisqu'il faut qu'elles aient de la légitimité face aux autres employés (ancienneté, connaissance globale de l'entreprise, des activités, des salariés et des enjeux).

Il en découle une troisième étape, l'analyse de l'efficacité du rôle au sein d'une organisation (autodiagnostic).
Pour cela l'audit évalue l'efficacité de la fonction au travers des attendus de la direction, de ce qui est perçu par les clients internes et externes (interview, questionnaires…), ce qui est réalisé par les collaborateurs (analyse de performances des processus à travers les indicateurs…). Il est intéressant de comprendre que les trois points interagissent entre eux de telle manière que l'on peut schématiser l'efficacité sous forme d'un triangle à l'instar du triangle du feu.



V Conclusion

Droit fondamental de la personne, la sûreté, au cours des dernières années, est sortie de la sphère exclusivement « régalienne » pour entrer dans un domaine partagé entre le secteur public et le secteur privé. Définie comme une stratégie de réduction des risques liés à des comportements intentionnels de malveillance, la sûreté doit désormais faire pleinement partie de la stratégie de maîtrise des risques de l'entreprise.
Or jusqu'à présent en France la législation a été créée pour répondre à des accidents regrettables et dramatiques, et à leurs conséquences. L'organisation des entreprises et la culture spécifique des acteurs de chaque domaine sûreté et santé-sécurité ont donc pris leur ancrage dans des corpus législatifs et réglementaires différents.
Dorénavant suite à une concurrence exacerbée et des Etats moins omniprésents, les entreprises doivent mener en permanence une réflexion globale afin de mettre en place tous les moyens de prévention et de protection de leurs intérêts et ceux de leur personnel. L'intégration de la sûreté au sein d'un service santé-sécurité est une réponse globale aux besoins de l'entreprise moderne et de ses enjeux majeurs face à un risque évolutif portant atteintes aux salariés et aux biens (matériels et immatériels).
L'apparition de réglementations récentes (IG du 30 juillet 2015 au profit des sites SEVESO, Arrêté du 13 juin 2017 au profit ERP de type M…) et la prise de conscience des acteurs des entreprises agissent comme des catalyseurs, accélérant ainsi la fonction *sûreté, santé-sécurité*, dans sa mutation en tant qu'un nouveau « business partner » incontournable au sein de celles-ci.
Ainsi cette transition doit passer tout d'abord par un processus de gestion des risques allant de l'identification au traitement des risques. Puis l'entreprise doit mettre en place un système de management global des risques sûreté, santé-sécurité afin de pérenniser une organisation efficace. Tout n'est possible que par l'adhésion et une meilleure compréhension de leur nouveau métier, c'est à dire des hommes et des femmes au service des autres. Encore une fois l'Homme est au cœur du changement.

« Tout est changement non pour ne plus être mais pour devenir ce qui n'est pas encore. »
(Epictète, philosophe grec, 50-125)

VI Références bibliographiques et internet

-Arrêté du 18 octobre 1977 : portant application du règlement de la sécurité pour la construction des IGH et leur protection (en particulier les articles GH 60, 62 et 63)

-**Arrêté du 25 juin 1980** modifié portant application du règlement intérieur contre les risques incendies et de panique dans les ERP (en particulier les articles MS 46 et M50)

-Arrêté du 2 mai 2005 modifié relatif aux missions, à l'emploi et à la qualification du personnel permanent des services incendie des ERP et IGH

-**Arrêté du 30 décembre 2011** portant règlement de sécurité pour la construction des IGH et leur protection contre les risques d'incendie et panique

-Arrêté du 13 juin 2017 modifie règlement intérieur contre les risques incendies et de panique dans les ERP (en particulier l'article M29)

-**Article internet du site sûreté-sécurité.asp** suite au forum 6ème édition sur la sûreté et la sécurité des entreprises qui sait tenue à Paris de 22 juin 2016

Assemblée des chambres de commerces françaises et de l'industrie (ACFCI) Guide pour la mise en place par étapes d'un système de management de la santé et de la sécurité au travail, octobre 2007

-**Bélanger Yves**, directeur du Groupe de recherche sur l'industrie militaire et la sécurité, publication de ERIMS, *« Le marché de la protection, de la sécurité et de la défense : perspective d'ici 2015 », décembre 2014*

-CFREOPS, *programme de formation du CQP APS - Certificat de Qualification Professionnelle d'Agent de Prévention et de Sécurité,* mai 2018

-Circulaire n°IOCD 1115097 du 03 juin 2011

- **CNPP : Traité pratique de la sûreté malveillance** 4ème édition du de janvier 2015

- **CNPP Référenciel 1302** : *Système de management de la sûreté, lutte contre la malveillance et la prévention des menaces*, édition de septembre 2009

- **CNPP Référencief 6011** *: « Analyse de vulnérabilité, approche globale et méthode pour l'incendie et la malveillance »,*

-**Code du Travail** Article L4121-1

-COESS (Confederation of european security service) **INHES** (institut national des hautes études de sécuirtés) LIVRE BLANC *« La participation de la sécurité privée à la sécurité générale en Europe »* décembre 2008

CONTY Albert COULIER Stéphane PILLET Caroline du Hays group, présentation *« Bilan et perspective de la fonction de Directeur Sûreté–Sécurité dans l'entreprise »*,31 mai 2007

-Décret du 23février 2006. du Code de la Défense réglementant les activités qualifiées d'importance vitale

-Décret n°2009-137 du 09 février 2009 relatif à la carte professionnelle

-Décret n°2011-1919 du 22 décembre 2011 permettant la création du CNAPS

Organisation International du Travail (OIT), Fascicule de formation de collection des modules ; *« introduction à la santé et à la sécurité au travail »*,de janvier 2018

-FLOBE conseil et formation *programme de formation du FORMATION : SSIAP 1 (+ SST + H0B0)*, mai 2018

-Fourcaudot Martine*, « Etude descriptive des agences de sécurité au Québec »,* décembre 1988

-Galea Bernard et Couvin Edouard : Revue *« De la mise en place des indicateurs sûreté dans les entreprises »,* février 2009

-Instruction du 12 août 2015 du Ministère de l'Intérieur autorisant l'exercice des activités de sécurité et incendie par des agents doublement qualifiés

-Instruction gouvernementale du 30 juillet 2015 concernant le développement de la sécurité dans les sites SEVESO

Juglaret Frédéric Publication *« Indicateurs et tableaux de bord pour la prévention des risques en santé-sécurité au travail »*, du 30 avril 2013

-Loi n°83-629 du 12 juillet 1983 réglementant les activités de sécurité privée

-Ministère de la sécurité publique au Québec, Livre blanc de *« la sécurité privée partenaire de la sécurité intérieure »* , décembre 2003

-**Norme ISO 31000,** *« Management des risques-Lignes directrices »* du 09 juin 2018

-**Norme ISO 34001,** *« Sécurité et Résilience »* du 21 mars 2018

- **Piètre-Cambacèdès Ludovic** Publication dans HAL archives-ouvert.fr, *« Des relations entre sûreté et sécurité »*, 28 février 2011

-**Qualitique** Revue N° 260 avril 2015 dossier *« Le management de la sûreté et de la sécurité »*

VII Glossaire

AMDEC : Analyse des Modes de Défaillance, de leur Effets et de leur Criticité

AIEA : Agence Internationale de l'Energie Atomique

CHSCT : Comité d'Hygiène, de Sécurité et des Conditions de Travail

CNAPS : Conseil National des Activités Privées de Sécurité

CQP APS : Certificat de Qualification Professionnelle d'Agent de Prévention et de Sécurité,

CSE : Comité Social et Economique

D.I.S.P : Délégué Interministériel de la Sécurité Privée

D.L.P.A.J : Direction des Libertés Publiques et des Affaires Juridiques

DSSS : Directeur Sûreté, Santé-Sécurité

ERP : Etablissement Recevant du Public

HSE : Hygiène Sécurité Environnement

IGH : Immeuble de Grande Hauteur

ISPS : International Ship and Port Facility

PDCA : Plan, Do, Check, Act

RPS : Risques Psychosociaux

S.S.I.A.P : Service de Sécurité et d'Assistance aux Personnes

TMS : Troubles MusculoSquelettiques