décembre 2015 DRA - 15-150223-10855A

Pilotage de la sécurité
par les indicateurs de performance

Guide à l'attention des ICPE

INERIS
maîtriser le risque
pour un développement durable

Avant-propos

Avec la notion de performance qui envahit l'ensemble des sphères managériales des organisations, y compris sur le sujet de la sécurité, les indicateurs sont devenus une réalité quotidienne où les gestionnaires de la sécurité peuvent se sentir enfermés. Il n'est donc pas étonnant de retrouver les indicateurs au centre de nombreuses discussions, voire controverses, sur leurs apports pour la sécurité, les modalités de leur utilisation ou leurs champs de validité.

Force est de constater que les indicateurs ne sont que des outils, avec les forces et les faiblesses des usages qui leurs sont assignés. A ce titre, ils constituent les symptômes, pas les problèmes.

Par conséquent, dans une littérature déjà foisonnante de démarches d'identification et d'utilisation d'indicateurs de sécurité, nous identifions comme centrale la nécessité pour la communauté des gestionnaires industriels de la sécurité de se réapproprier la notion d'indicateurs en la mettant au service de leurs conceptions de la sécurité et non pas en enfermant cette dernière dans des outils réducteurs. Nous écrivons conceptions avec un « s » car, même si toutes les visions de la sécurité ne peuvent se valoir, il nous semble que plusieurs peuvent prétendre à une légitimité au regard de leurs historiques et contextes d'utilisation respectifs.

Le présent guide s'adresse aux managers industriels en charge de la sécurité de systèmes présentant des risques majeurs. Il s'ancre dans une optique favorable à une distinction claire des outils d'évaluation de performances associées aux risques au poste de travail de ceux associés aux risques majeurs. Ce faisant, la démarche de réappropriation que nous suggérons se base dans un premier temps sur un éclairage élargi du rôle de l'évaluation des performances en gestion des risques majeurs. Puis, plus finement, nous nous intéresserons à contextualiser le rôle des indicateurs parmi une large gamme d'outils d'évaluation de performance ayant différentes forces et faiblesses.

Dans un second temps, la méthode SIPS (Système d'Indicateurs de Performance Sécurité) est proposée avec l'objectif de structurer la manière dont les gestionnaires de la sécurité peuvent construire et sélectionner les indicateurs les plus aptes à servir leurs modèles et représentations de ce qu'est la sécurité. Par ce moyen, nous espérons créer les espaces d'échange et d'interaction au sein de chaque organisation pour, non seulement sélectionner les indicateurs les plus adaptés, mais aussi pour en définir les modalités d'utilisation qui vont dans le sens de la sécurité et non pas qui l'enferment dans des raccourcis préjudiciables. Tout au long de ces deux parties, de nombreuses opportunités sont offertes au lecteur d'approfondir certains aspects ou de questionner les fondements scientifiques du guide à travers des fiches de lecture thématiques présentées en fin de document.

L'utilisation du présent guide au sein des organisations nécessite un investissement à long terme et une mobilisation de l'ensemble des niveaux hiérarchiques. Il ne s'agit pas d'une démarche ponctuelle. C'est plutôt un cadre d'amélioration collectif et continu où l'apprentissage et l'échange sont les maîtres-mots.

Sommaire

Glossaire

Indicateur

Information choisie, associée à un phénomène, destinée à en observer périodiquement les évolutions au regard d'objectifs définis.

Indicateur de résultat

Information permettent d'apprécier le nombre, la qualité ou le type de résultats associés à l'objet (ou processus) mesuré.

Indicateur de fonctionnement

Information(s) relative(s) aux modalités de déroulement des différentes étapes composant l'objet (ou processus) mesuré.

Indicateur d'écosystème

Information décrivant le caractère plus ou moins favorable du contexte technique et organisationnel composant l'écosystème dans lequel l'objet (ou le processus) évolue.

Modèle de sécurité

Le modèle de sécurité identifie l'ensemble des moyens techniques, humains et organisationnels à travers lesquels l'organisation entend exercer un contrôle sur son système à risque pour en piloter la sécurité. Ce modèle reflète la vision que l'organisation a de la sécurité et des moyens de l'assurer.

Performance

Concept multidimensionnel servant à apprécier les forces et faiblesses d'une organisation. Son utilisation sert de base à un cycle continu d'analyse et diagnostic impliquant et confrontant de multiples représentations au sein de l'organisation (Voir fiche 3 pour plus d'éléments).

Sécurité

Différentes conceptions du mot sécurité coexistent. Elle se définit dans certains contextes comme l'absence de risque ou son maintien à un niveau acceptable. Dans d'autres contextes, c'est une propriété émergente résultant des capacités d'adaptation des organisations à la variabilité de leurs conditions opératoires. (Pour plus de détails, voir fiche 4 pour plus d'éléments).

SIPS

Système d'Indicateurs de Performance Sécurité.

Introduction

(1) Le terme contrôle s'entend dans ce document comme le suivi et l'adaptation dynamique des dispositifs de maîtrise des risques identifiés.

Il ne se limite donc pas à une simple vérification de conformité au regard d'une norme donnée.

Les systèmes à risques majeurs sont complexes (voir ***fiche 1***). Pour y faire face et maintenir les risques à un niveau acceptable, des cadres de contrôle systématiques sont mis en place. Nous parlons ici de gestion de la sécurité.

La gestion de la sécurité se définit comme la mise en place, le maintien et l'évaluation des leviers de contrôle[1] adoptés pour maintenir les risques à un niveau acceptable. Ces leviers peuvent être :

- **techniques** (soupapes, vannes, indicateurs niveau haut et très haut, bassins de rétention,...),
- **humains** (formation, études ergonomiques...)
- **organisationnels** (gestion des modifications, définition des responsabilités...).

Les leviers de contrôle considérés en gestion de la sécurité

La littérature regorge de descriptions des systèmes de contrôles en gestion de la sécurité. Les plus connus demeurent les **M**esures de **M**aîtrise des **R**isques (**MMR**) ou barrières de sécurité : évents ou systèmes instrumentés de sécurité sont des exemples de dispositifs techniques au service de l'exercice de contrôle des risques. Des dispositifs humains ou organisationnels sont aussi à considérer :

- **Les directives Seveso II et III** citent un certain nombre de leviers de contrôle organisationnels dans leurs annexes 3 : Gestion des modifications, planification des situations d'urgence, surveillance des performances, formation du personnel, définition des responsabilités...
- **L'OSHA** (Occupational Safety and Health Administration) a identifié dans son référentiel OSHA 3132 (2000) les dispositifs techniques et organisationnels grâce auxquels un contrôle peut être exercé sur la sécurité. Sans être exhaustif : Intégrité mécanique (maintenance), permis de travail, retour d'expérience, audits de conformité...
- **Le HSE** (2006) suggère une liste de Risk Control Systems (RCS) que tout gestionnaire de systèmes à risques majeurs devrait continuellement implémenter et évaluer au regard de standards prédéfinis. Il s'agit de :
  - gestion des modifications,
  - inspection et maintenance,
  - gestion des compétences, procédures opérationnelles,
  - gestion des situations d'urgence,
  - gestion des permis de travail.
- Enfin, à un niveau plus académique, nous pouvons citer l'analyse comparative réalisée par **Grote** (2012) qui identifie les leviers de contrôle suivants comme étant les plus communs en gestion de la sécurité :
  - définition d'une politique sécurité,
  - définition des responsabilités et affectation des ressources associées,
  - définition des standards et procédures opérationnels,
  - prise en compte des facteurs humains lors de la conception du système,
  - gestion des compétences,
  - retour d'expériences,
  - audits, amélioration continue
  - gestion des modifications.

Introduction

Quels que soient les moyens de contrôles considérés, ceux-ci s'exercent dans le cadre d'une boucle de régulation composée des éléments suivants :

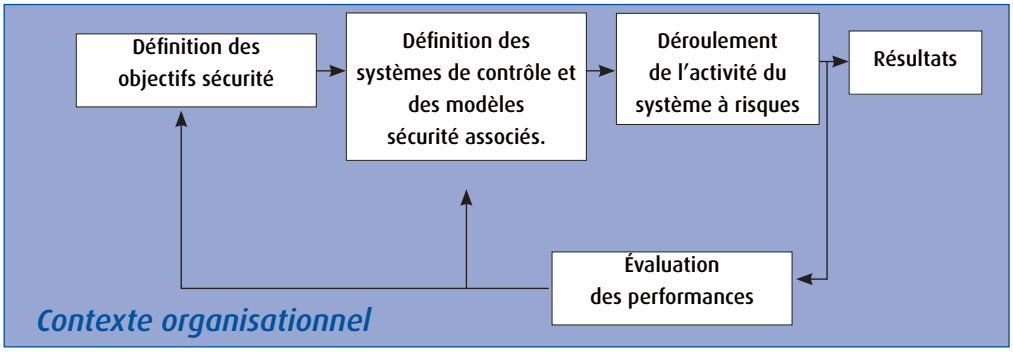


Figure 1 Gestion de la sécurité (inspiré par (Hollnagel, 2006) et (Cambon, 2007)).

❒ Les objectifs sécurité

Définis généralement dans le cadre de la politique sécurité de l'organisation, les objectifs sécurité décrivent les attentes et les grandes orientations fondant la politique sécurité de l'organisation.

❒ Les systèmes de contrôle et le(s) modèle(s) sécurité sous jacents

Le modèle de sécurité identifie l'ensemble des moyens techniques, humains et organisationnels à travers lesquels l'organisation entend exercer un contrôle sur son système à risques pour en piloter la sécurité. Ce modèle reflète la vision que l'organisation a de la sécurité et des moyens de l'assurer. À titre d'exemple, la sécurité peut être vue comme l'absence de risques inacceptables (EPSC, 1996). Le modèle de sécurité doit alors se focaliser sur la détection et réduction des événements susceptibles de contribuer à une séquence accidentelle.

La sécurité peut aussi être vue comme des adaptations continues face à la variabilité naturelle des activités quotidiennes à risques (Hollnagel, 2008). Le focus n'est donc plus mis sur la détection des événements mais sur le développement des capacités d'adaptation. (voir ***fiche 4***).

❒ Les activités à risques

Il s'agit de décrire le périmètre du système à risque que l'on souhaite gérer ainsi que les scénarios accidentels qui y sont associés.

❒ L'évaluation des performances

Elle décrit l'ensemble des outils et approches mises en place pour évaluer les performances sécurité d'un système et les comparer avec les objectifs définis en amont pour former la boucle de contrôle.

De plus, cette boucle est fortement influencée par le contexte organisationnel dans lequel elle évolue. Ce contexte est variable d'un système à un autre et se compose de dynamiques variées : réglementation, contraintes économiques, culture d'entreprise...

En conclusion, c'est l'ensemble composé par la boucle et son contexte organisationnel qui définissent la gestion de la sécurité telle que pensée et pratiquée au sein de chaque système à risques (voir ***fiche 2***).

L'évaluation de performance en gestion de la sécurité

L'évaluation de performance en gestion de la sécurité

Objectifs

Ils ont dit...

« Formuler et, si possible, chiffrer les objectifs puis mesurer les performances réalisées dans l'accomplissement de ces objectifs, voilà bien la finalité de tout outil de gestion »

(Lorino, 1995).

Objectifs

L'évaluation de performance sécurité peut servir les deux catégories d'objectifs suivants :

❒ Vérifier que les systèmes de contrôle décidés sont mis en place et fonctionnent de manière satisfaisante.

Les décalages entre ce qui est prescrit dans le système de gestion des risques et ce qui est fait sur le terrain peuvent s'avérer importants. Ils peuvent résulter d'un déficit d'appropriation des règles sécurité par les opérateurs et managers ou de prescriptions incompatibles avec les réalités du terrain (Amalberti, 2012).

Dans ce contexte, évaluer les performances vise à recenser les points forts et faibles de la gestion quotidienne des risques et ainsi identifier les besoins d'action et orienter les investissements sécurité. Par exemple, évaluer le respect des procédures sur le terrain peut révéler des besoins supplémentaires de formation des opérateurs ou la nécessité de réviser le contenu des procédures pour les rendre plus conformes aux réalités du terrain.

❒ Continuellement réadapter la gestion du risque aux évolutions du système

Les dynamiques techniques, humaines et organisationnelles qui animent les systèmes à risques contribuent à le façonner et à le modifier en continu. Par conséquent, les types et niveaux de risques ainsi que les facteurs influant sur la sécurité évoluent constamment. Si la gestion des risques ne s'adapte pas en conséquence, un écart de plus en plus grand entre la réalité du risque et les représentations que s'en font les managers peut apparaître.

Cela peut aboutir à une illusion de sécurité qui ne se révèle qu'après un accident majeur. Un changement de procédés de fabrication, le départ de collaborateurs expérimentés, la perte de leadership ou une évolution réglementaire sont des exemples de dynamiques qui peuvent modifier le niveau de risque d'un système et questionner aussi bien les systèmes de contrôle en place que les objectifs sécurité définis en amont.

Outils

Nous nous proposons de distinguer dans ce qui suit les pratiques d'évaluation de performance en sécurité selon les deux axes que sont les types d'outils et leurs possibles niveaux de mise en œuvre.

Les types d'outils

Trois grandes catégories d'outils complémentaires peuvent être mobilisées pour mener l'évaluation de la performance sécurité :

❒ Les indicateurs de performance

Un indicateur est une information choisie, associée à un phénomène[2] destinée à en observer périodiquement les évolutions au regard d'objectifs définis. Régulièrement mis à jour, les indicateurs fournissent une représentation concise bien que souvent partielle de l'état du système à risques et de l'historique de son évolution.

Par exemple, s'agissant de la maintenance des Mesures de Maîtrise des Risques, le nombre d'inspections réalisées à temps sur le nombre global d'inspections prévues sur une période de temps donnée est un exemple d'indicateur du déroulement des opérations de maintenance.

[2] Contrairement à un index qui résulte de nombreuses agrégations successives le rendant difficilement associable à un phénomène particulier.

L'évaluation de performance en gestion de la sécurité

Outils

Il permet d'évaluer la capacité de l'organisation à respecter les délais et échéances de maintenance sans pour autant juger de la qualité de ces inspections, de la pertinence de la politique d'inspection/maintenance adoptée ni du niveau de compétence des intervenants.

Les indicateurs sont des outils largement déployés dans l'ensemble des systèmes de gestion. Il en résulte une grande variété d'usages, de compréhensions et de valorisation.

❒ Les audits et questionnaires

La norme ISO 9000 (2005) définit les audits comme des processus méthodiques, indépendants et documentés, permettant d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits.

Les audits et questionnaires sécurité se basent donc sur une liste prédéfinie d'items et de questions pour évaluer la manière dont la gestion quotidienne de la sécurité satisfait les exigences et cadres formels définis ou adoptés par l'organisation (normes, standards, bonne pratiques...).

Les réponses peuvent être binaires (Fait/pas fait, oui/non...) ou graduées à travers un système de scores (qualitatifs ou quantitatifs).

Par exemple, l'évaluation de la culture ou du climat[3] sécurité d'un système à risques est souvent effectuée à travers des questionnaires.

❒ Les diagnostics organisationnels

Si les diagnostics organisationnels se basent aussi sur des items et des modèles de référence, leur objectif est d'aller au-delà des évaluations de conformité.

Il s'agit ici d'utiliser les modèles et items comme autant de pistes d'investigation des pratiques organisationnelles. Le praticien exploitera son expérience et son savoir faire pour sélectionner les aspects à explorer plus en profondeur ainsi que les modalités de cette exploration.

Il devra en retour fournir une prise de recul et une appréciation globale de l'état de santé de l'organisation, de ses points forts et faibles ainsi que des axes d'amélioration à envisager (Romalaer, 2011). Il peut à cet effet utiliser différents outils : entretiens individuels, observations et groupes de travail.

S'agissant des installations à risques, les diagnostics organisationnels peuvent être réalisés en prévention ou en réaction à un accident. Dans le second cas, nous parlerons d'enquête post accidentelle.

Les niveaux de mise en œuvre

❒ Niveau opérationnel

Les évaluations portent sur les composantes techniques du système, les interactions homme/machine et équipes de travail. Il s'agit de s'assurer que les conditions nominales de fonctionnement du système de production définies par les standards ou par l'organisation sont respectées :

- Paramètres (température, pression, vitesse...) de production maintenus dans les limites de sécurité définies.
- Interventions des opérateurs, y compris les prestataires, dans des conditions de sécurité satisfaisantes, dans le respect des procédures et standards prédéfinis et avec un niveau de formation adéquat.

[3] Les concepts de culture et de climat sécurité sont distingués dans le sens où le premier regroupe l'ensemble des croyances et valeurs relatives à la sécurité alors que le second représente une manifestation visible et momentanée du premier.

L'évaluation de performance en gestion de la sécurité

Outils

❒ Niveau tactique

L'évaluation de performance porte sur les processus managériaux susceptibles d'influer sur la performance sécurité du système. À titre d'exemple :

- Les **procédures** définies sont-elles adaptées aux réalités du terrain ? Sont-elles réactualisées quand nécessaire ?
- Les **analyses** de risques ont-elles actualisées et suffisamment approfondies ?
- Les **opérateurs** sont-ils bien formés et leurs connaissances réactualisées ?
- Comment est mené le processus de **retour d'expérience** ? Quel apprentissage en est-il fait ?

Les évaluations menées pour ce niveau visent à nourrir les décideurs des départements HSE ou des directions de site qui s'en serviront pour juger de la qualité du management sécurité et des améliorations à y apporter.

❒ Niveau stratégique

L'évaluation porte ici sur les modalités de mise en place et l'efficacité des stratégies sécurité décidées. En plus des considérations internes à l'organisation, l'évaluation des performances intègre aussi l'environnement de l'organisation : évolutions réglementaires susceptibles d'impacter les modalités de gestion des risques, pressions économiques, perceptions par le public, évolutions technologiques...

A ce niveau, les incertitudes sont plus importantes et les données quantitatives rares. Les évaluations de performance se font donc de manière plus qualitative et à des horizons temporels plus lointains comparativement aux deux niveaux précédents.

La combinaison de ces deux axes fonde la **typologie des outils d'évaluation des performances sécurité** présentée dans le tableau ci-dessous.

	Opérationnel	Tactique	Stratégique
Indicateurs de performance	**Indicateurs opérationnels** intervenant directement dans la gestion du système de production (couche technique et humaine du système).	**Indicateurs de management de la sécurité.** Appréciation de la qualité du système de gestion de la sécurité mis en place.	**Indicateurs stratégiques** ❒ Évaluation sécurité au niveau Corporate ou sectoriel ❒ Appréciation des évolutions sociétales susceptibles d'impacter le niveau de sécurité des systèmes considérés.
Audits & Questionnaires	**Audit opérationnel**	**Audit du système de management**	**Audit stratégique**
	Si la mécanique de l'audit demeure identique, les référentiels, standards et critères d'audit varient selon la thématique abordée et le niveau organisationnel considéré.		
Diagnostic organisationnel	**Evaluation holistique** s'intéressant à ces niveaux et à leurs interactions.		

Tableau 1 : Typologie des outils d'évaluation des performances sécurité

Ces outils d'évaluation de performance sont complémentaires. Les frontières proposées pour les distinguer servent plus un raisonnement théorique puisque la pratique implique un mix d'outils. Ainsi, les scores d'un audit peuvent être considérés comme des indicateurs et les indicateurs comme premiers éléments d'orientation des pratiques d'investigation.

Selon les spécificités organisationnelles et les orientations managériales propres à chaque organisation, une combinaison différente de ces outils peut être mise en place pour composer ce que l'on appellera un système d'évaluation de performance sécurité (SEPS).

L'évaluation de performance en gestion de la sécurité

Outils

Ils ont dit...

« Ce ne sont pas les informations en elles même qui sont importantes, mais les réflexions qu'elles génèrent »

(Skoog, 2007).

Quelle que soit la combinaison d'outils adoptée, le système devra satisfaire les trois fonctionnalités suivantes (Eckerson, 2011) :

- **Mesurer** ⇨ Une ou plusieurs mesures de l'état du système, qualitatives ou quantitatives, devront être fournies.
- **Analyser** ⇨ Combinées à ces mesures, des capacités d'analyse croisée doivent être mises en place. En effet, les mesures réalisées sont des informations qui doivent encore être croisées et interprétées pour aider à la prise de décision.
- **Partager** ⇨ Les décisions prises sur la base de ces mesures doivent être partagées et communiquées conformément à des contraintes précises. D'une part, la communication des résultats doit pouvoir permettre le partage des connaissances au sein de l'organisation, la motivation du personnel à poursuivre l'atteinte des objectifs et la démonstration que les efforts investis par les uns et les autres pour le recueil de l'information influent sur les décisions.

  D'autre part, cette communication doit prendre en compte les contraintes de confidentialité et éviter une diffusion publique dont les résultats pourraient s'avérer contre-productifs pour l'organisation dans la durée.

Enfin, face à la complexité des systèmes à risques, l'évaluation des performances sécurité avec des outils simplistes peut s'avérer préjudiciable aux décideurs qui ne seraient pas conscients de leurs travers.

Plus précisément, cela peut générer les conséquences suivantes :

- Renvoyer au décideur l'illusion de contrôle et de sécurité.
- Focaliser l'attention des décideurs sur un sous ensemble d'aspects au détriment de ceux non représentés ou négligés par les outils (effet œillères).

L'illusion de sécurité

En 2004, la raffinerie de BP Texas city a connu la meilleure performance sécurité de son histoire. Comparativement à l'ensemble du secteur de la raffinerie, cette performance était de 30% meilleure que la moyenne des performances constatées.

La mesure des performances sécurité s'est effectuée dans ce cas sur la base d'indicateurs de risques au poste de travail. Ceux-ci ont été considérés comme représentatifs de la performance sécurité globale du site, incluant la gestion des risques majeurs.

Le 23 mars 2005, l'explosion de l'unité d'isomérisation a entraîné **la mort de 15 salariés et la blessure de 180 autres**.

Les indicateurs de performance sécurité

Le recours aux indicateurs de performance sécurité dans les systèmes à risques majeurs est une nécessité rappelée aussi bien par les normes (ISO 31000), les guides à destination des professionnels (EPSC, 1996), (OCDE, 2008), (CCPS, 2010), (CCPS, 2011), (OGP, 2011) (CEFIC, 2011) ainsi que les retours d'expérience suite à des accidents majeurs (CSB, 2007), (Baker panel, 2007), (HSE, 2010).

Si tous les acteurs de la sécurité des procédés s'accordent sur leur nécessité, de larges divergences demeurent sur leurs rôles, apports et modalités d'utilisation au quotidien. Nous présenterons dans ce qui suit une photo, aussi représentative que possible, des pratiques existantes dans l'industrie et des principaux débats encore ouverts aussi bien chez les praticiens que dans la littérature scientifique.

L'évaluation de performance en gestion de la sécurité

Les indicateurs de performance sécurité

[4] Pour plus d'éléments, voir (Mazri, Delatour, Laclémence & Calcei, 2014).

[5] Dans leurs annexes III.

[6] American petroleum Institute

[7] European Chemical Industry Council

[8] Center for Chemical Process Safety

[9] European Process Safety Center

[10] Une fois que la perte de confinement, et peut être l'accident majeur, ont eu lieu.

Usages des indicateurs sécurité dans l'industrie des procédés- état des lieux

Dresser un état des lieux représentatif des modalités d'utilisation des indicateurs de performance sécurité dans l'industrie est un défi à plusieurs titres. Tout d'abord, l'extrême variété des domaines industriels concernés, des cultures et ressources associées engendre une large diversité des conceptions et pratiques[4]. De plus, les indicateurs demeurent prioritairement des outils de décision à vocation interne à l'organisation ; ils sont donc rarement révélés au grand jour.

Au regard de ces éléments, l'état des lieux dressé ici combinera trois sources d'informations complémentaires, à savoir le cadre réglementaire, les littératures académiques et professionnelles existantes ainsi que nos expériences et collaborations récentes avec le monde industriel sur ces questions.

- Les **cadres réglementaires** existant en Europe et en France se contentent d'insister sur la nécessité de mettre en place des indicateurs sécurité mais ne disent rien sur les modalités de leur sélection ou utilisation. Ils sont à ce titre très faiblement contraignants.

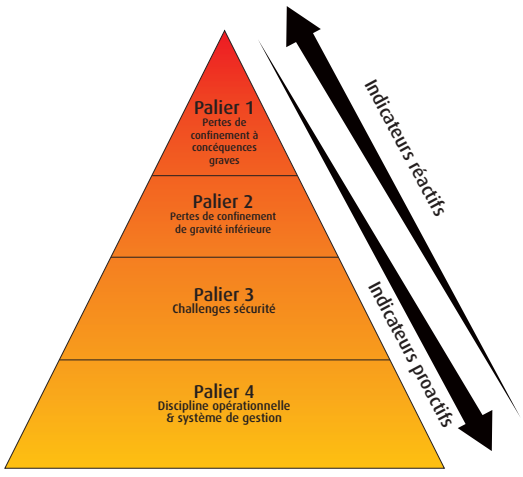
  Ainsi, les **directives Seveso II et III** traitent explicitement[5] de la nécessité d'évaluer les performances sécurité dans le cadre des Systèmes de Gestion de la Sécurité (SGS). De ce fait, bien que le SGS s'impose comme le cadre réglementaire au sein duquel les indicateurs de performance sécurité doivent être développés et utilisés, une totale liberté de choix est laissée aux organisations quant aux modalités pratiques de sélection et d'utilisation des indicateurs.

- C'est donc naturellement du coté des **guides professionnels** que se dessinent les contours des pratiques associées aux indicateurs de performance sécurité. Ces travaux ayant été menés au sein d'associations professionnelles (API[6], CEFIC[7], CCPS[8], EPSC[9]...), nous y retrouvons de manière régulière le souci d'une harmonisation des indicateurs en vue d'assurer un suivi de tendances et un benchmarking au sein de filières industrielles ou de l'ensemble de l'industrie des procédés.

  Malgré la diversité des guides issus de ces organismes, ils partagent de manière forte le modèle pyramidal (voir ***fiche 4***) proposé par l'API (2010). Ce modèle postule un lien statistique fort entre d'une part, des incidents ou événements non désirés de faible gravité et de fréquence élevée (base de la pyramide) avec, d'autre part, des événements de gravité majeure mais de fréquence très faible (sommet de la pyramide).

  Il ressort de ce modèle que l'industrie des procédés peut évaluer sa performance sécurité sur la base de deux types de mesures :

  - La mesure des *pertes de confinement* (paliers 1 et 2 de la pyramide). Ces mesures sont dites **réactives** dans la mesure où elles ne reflètent qu'après coup[(10)] la détérioration du niveau de sécurité. Un effort important d'harmonisation est aujourd'hui toujours en cours pour permettre des mesures homogènes sur l'ensemble de l'industrie.



L'évaluation de performance en gestion de la sécurité

Les indicateurs de performance sécurité

- La mesure d'*événements ou comportements non désirés* (paliers 3 et 4). Ces mesures sont dites proactives car considérées comme pouvant détecter des détériorations de la sécurité avant que les pertes de confinements aient lieu conformément au lien statistique assumé par le modèle. Ces mesures sont reconnues comme propres à chaque industriel et ne pouvant faire l'objet d'une harmonisation (EPSC, 2011).

L'impossible harmonisation des mesures proactives

Harmoniser les mesures proactives, et ainsi résoudre le dilemme du choix des indicateurs, n'est pas envisageable pour les trois raisons suivantes :

- D'un système à un autre, le **modèle de sécurité** adopté varie. En d'autres termes, les moyens par lesquels l'organisation entend exercer son contrôle sur la sécurité de son système peuvent varier d'une entreprise à une autre (voir ***fiche 4***). Or, des modèles de sécurité différents impliquent des besoins différents de mesure de performance, et par conséquent, des indicateurs différents.
- Les **ressources** (temps, argent, compétences) allouées à la mise en place d'indicateurs sécurité peuvent grandement varier d'une organisation à une autre entrainant ainsi des choix et arbitrages spécifiques.
- Enfin, la variété des **cultures** et pratiques d'un système à un autre peuvent rendre l'usage d'un indicateur plus ou moins acceptable par les utilisateurs et les décideurs.

- Bien que le modèle pyramidal soit largement partagé dans les guides, nous constatons toujours une hétérogénéité des modèles et des pratiques associées aux indicateurs.

  Nous pouvons citer à minima les deux catégories de pratiques suivantes :

  - L'utilisation du modèle pyramidal pour traiter conjointement les risques au poste de travail et les risques majeurs dans une vision intégrée. Dans ce cadre, les indicateurs utilisés sont souvent uniquement réactifs et se focalisent sur les statistiques d'accidents au poste de travail.

    Les utilisateurs justifient le recours à ces indicateurs par les niveaux de ressources (temps, compétences...) trop importants que nécessiteraient des indicateurs plus nombreux et/ou plus sophistiqués.
  - Dans d'autres cas, les industriels ont recours dans leurs pratiques quotidiennes à des modèles de sécurité propres différents du modèle pyramidal. Ces modèles leur permettent de :
    - distinguer les indicateurs associés aux risques au poste de travail de ceux dédiés aux risques majeurs ;
    - aller au-delà des mesures de perte de confinement pour identifier les points forts et ponts faibles de leur organisation.

Cet état des lieux démontre, entre autres choses, l'absence d'une vision unique au sein de l'industrie des procédés et la persistance de débats quant aux modalités de définition et d'usage des indicateurs de performance sécurité.

Les débats clé des indicateurs de performance sécurité

Nous identifions cinq débats clés :

- A quoi servent les indicateurs de performance sécurité ?
- Les indicateurs de risques au poste de travail peuvent ils être utilisés pour évaluer la performance au regard des risques majeurs ?

L'évaluation de performance en gestion de la sécurité

A quoi servent les indicateurs de performance sécurité ?

- Quel lien entre le modèle pyramidal (discuté en amont) et le modèle de sécurité utilisé ?
- Quelle différence y a-t-il entre indicateurs réactifs (lagging) et proactifs (leading) ?
- De combien d'indicateurs de performance sécurité a-t-on besoin ?

A quoi servent les indicateurs de performance sécurité ?

Au sein d'un système à risques majeurs, les indicateurs de sécurité servent, plus ou moins bien, trois types de fonctions. Comme nous le verrons dans la suite, certaines de ces fonctions sont souhaitées mais pas toujours réalistes alors que d'autres ne sont pas toujours assumées ni explicites.

Un usage fortement souhaité : informer les managers de ce qui se passe sur le terrain

C'est l'usage le plus reconnu par les gestionnaires de la sécurité. Ceux-ci attendent des indicateurs qu'ils remontent des représentations pertinentes et synthétiques de la réalité quotidienne de la sécurité.

Les informations composant ce **flux ascendant** (depuis le terrain vers le management) peuvent être de natures très diverses : application des plans d'actions décidés, efficacité des mesures de gestion des risques mises en place, niveau d'atteinte des objectifs, respect des règles et procédures, retours d'expériences permettant de réviser les hypothèses de conception ou les pratiques existantes...

De manière générale, ces informations sont classées en fonction de leur caractère **réactif** (reflétant le comportement passé du système) ou **proactif** (anticipant le comportement futur du système).

En comparant les résultats des actions décidées avec les objectifs assignés, cet usage constitue une fonction vitale de la boucle de régulation qu'est la gestion de la sécurité. Dans le même temps, il peut être source de biais importants si les gestionnaires ne perçoivent leur système qu'au travers de ces indicateurs. En effet, comme tout outil de gestion, les indicateurs ne peuvent remonter que certains aspects de la réalité. Par conséquent, ce qui n'est pas dans l'indicateur n'est pas observé et donc pas géré.

L'évaluation de performance en gestion de la sécurité

A quoi servent les indicateurs de performance sécurité ?

Les 7 défis de l'évaluation

'Prendre une photo' synthétique et porteuse de valeur ajoutée est un objectif ambitieux qui nécessite de porter attention aux défis suivants :

❒ Éviter la partialité

Le caractère synthétique est bien la première qualité d'un indicateur. Utilisé régulièrement, il devient un code, une synthèse qui facilite la communication entre acteurs en économisant la nécessité de (ré) expliquer et (re) détailler l'ensemble des éléments qui lui sont sous-jacents. Néanmoins, cela peut aussi constituer sa première faiblesse s'il ne couvre pas l'ensemble des dimensions du système considéré ou si son interprétation peut prêter à confusion et partialité. A terme, ce qui n'est pas décrit par l'indicateur ne sera plus considéré par le gestionnaire, affaiblissant ainsi l'organisation face aux risques. A titre d'exemple, se limiter à comptabiliser le nombre d'incidents et presqu'accidents traités pour évaluer le REX occulte de nombreux aspects de ce processus complexe : l'existence d'une culture de remontée de l'information, qualité des analyses effectuées, apprentissage en résultant...

❒ Adopter des règles d'agrégation validées

L'indicateur peut être une information agrégée. Or, l'agrégation ou combinaison d'informations peut déformer la capacité de l'indicateur à refléter la réalité des phénomènes. Ainsi, la compensation (de certains aspects négatifs par d'autres plus positifs) peut amener l'organisation à systématiquement ignorer ou négliger certaines faiblesses qui deviendront latentes. L'agrégation par les moyennes pondérées ou les approches par scoring peuvent entraîner ces effets. L'agrégation des informations doit aussi être sensible aux variations du système et les refléter aussi fidèlement que possible. Ainsi, si la maille adoptée par l'indicateur est trop large pour détecter certaines fluctuations, elles demeureront ignorées par le gestionnaire de la sécurité.

❒ Éviter la paralysie par l'analyse

A vouloir trop bien faire, l'organisation peut être amenée à ne jamais statuer sur les indicateurs à adopter car chacun d'entre eux sera porteur de faiblesses. Il est nécessaire à ce niveau d'effectuer des compromis et d'attirer l'attention sur les limites des indicateurs adoptés afin que leur interprétation ne dépasse pas leurs champs de validité.

❒ Manipulation : gérer l'indicateur plutôt que le système

Quand la valorisation des personnes au sein de l'organisation est liée à certains indicateurs, la tentation de manipulation est forte. Ainsi, plutôt que d'agir sur le système pour en améliorer les performances et par conséquent les indicateurs, un chemin plus simple serait de manipuler l'indicateur de manière artificielle. A titre d'exemple, il a été constaté que certains opérateurs ou managers ont tendance à moins déclarer les incidents ou pratique dangereuses de leurs collaborateurs quand des bonus financiers sont indexés sur les performances d'équipe.

❒ Fiabiliser les informations

L'adoption de circuits de remontée d'information simples, fiables et vérifiables doit être privilégiée autant que possible. Ainsi, en plus des possibles manipulations volontaires, des procédures de remontée d'information trop lourdes ou difficilement réalisables entraîneront rapidement une démotivation du personnel et à terme, la disparition de l'indicateur.

❒ Réactualiser régulièrement

De la même manière que les systèmes à risques évoluent, les dangers qu'ils génèrent et les vulnérabilités qu'ils démontrent sont aussi des données évolutives. Par conséquent, les systèmes d'évaluation de performance en général, et les systèmes d'indicateurs en particulier, se doivent de suivre cette évolution et de s'adapter. Cela implique de régulièrement s'interroger sur la pertinence du système d'indicateurs mis en place.

❒ Poids pour l'organisation.

Lors de la définition des indicateurs, un paramètre de décision important devrait être le poids qu'ils représentent pour l'organisation en termes de temps et ressources nécessaires pour la collecte, agrégation et interprétation des informations. Plus un indicateur est léger sur ces aspects, plus il aura de chances de survivre.

L'évaluation de performance en gestion de la sécurité

A quoi servent les indicateurs de performance sécurité ?

Un usage souvent informel : refléter les priorités managériales des gestionnaires de la sécurité

Comme le note Broussard (2001), les indicateurs sont porteurs d'un savoir social sur ce que sont les règles et l'identité de l'organisation. A ce titre, une fonctionnalité bien moins reconnue que la précédente est la capacité des indicateurs sécurité à informer le personnel de l'organisation sur les priorités et orientations adoptées par le management s'agissant de la sécurité.

A titre d'exemple, une entreprise à risques qui adopte des indicateurs de culture sécurité renvoie à ses salariés, du moins en théorie, une image de ce qui est attendu de leur comportement et des règles à respecter : placer la sécurité comme dénominateur commun de l'ensemble des échelons organisationnels, valoriser les contributions individuelles dans la construction de cette performance... Une autre entreprise qui focaliserait ses indicateurs sur le nombre de défaillances et erreurs renverra une image plus répressive avec une réduction de la tolérance à l'erreur, et donc à l'apprentissage, et une politique de sanction plus sévère.

Les indicateurs sont donc aussi des outils d'une information descendante sur lesquels les opérateurs terrain peuvent se baser pour lire ou interpréter l'importance que l'organisation accorde à la sécurité et les moyens par lesquels elle souhaite y aboutir.

Comprendre ce mécanisme, souvent caché car informel, est fondamental pour analyser la manière dont les indicateurs sont utilisés au quotidien. Il permet de comprendre pourquoi certains indicateurs peuvent exister sur la documentation des systèmes de gestion de la sécurité sans pour autant avoir une réelle influence sur la vie quotidienne du système.

En effet, si ces indicateurs véhiculent des normes sociales qui sont contradictoires avec d'autres normes ayant un impact plus fort, ils ne dépasseront jamais le statut d'encre sur du papier. Un exemple classique en sécurité est l'équilibre entre la sécurité et la performance économique ou financière.

Dans son rapport d'enquête sur l'accident de Texas City, le Chemical Safety Board (CSB, 2007) a pointé à quel point la performance sécurité était faiblement représentée par rapport à la performance financière : 50% des bonus des salariés étaient déterminés sur la base du « cost leadership » ou capacité à maîtriser les coûts alors que la sécurité ne comptait que pour 10%.

Un usage recommandé : l'apprentissage collectif

Les outils de gestion ne peuvent prétendre représenter exhaustivement la réalité car celle-ci est trop riche et complexe. Plus modestement, ils doivent servir en premier lieu à des apprentissages collectifs (Lorino, 1995) (Hatchuel, 2000) en créant des dynamiques collectives et des motivations d'action communes au sein d'une organisation (voir ***Fiche 4***).

Les indicateurs de performance sécurité ne doivent pas échapper à cette logique.

L'évaluation de performance en gestion de la sécurité

A quoi servent les indicateurs de performance sécurité ?

Ainsi, plutôt que de limiter l'usage des indicateurs à une comparaison entre performances évaluées et objectifs prédéfinis, il s'agit d'entrer dans un cycle continu de diagnostic et d'apprentissage qui reconnaît la complexité de la réalité et la nécessité de continuellement adapter nos savoirs et nos pratiques.

Les conséquences techniques et organisationnelles suivantes sont à considérer :

Diagnostiquer implique :

- la mise en place des capacités organisationnelles nécessaires pour **communiquer**, **échanger** et collectivement **interpréter** les informations remontées par les indicateurs. Ainsi, ceux-ci serviraient plus comme sources permettant d'initier un débat continu, compétent et renouvelé sur la sécurité que comme seule image représentative de l'état du système.
- d'**identifier** des indicateurs dont les interprétations croisées sont susceptibles d'apporter une valeur ajoutée à la compréhension des dynamiques sécurité du système.

Apprendre implique

- le **partage des informations** remontées par les indicateurs et leur échange entre différents niveaux hiérarchiques. Pour que cet échange ait lieu, il est important d'instituer une parole libre basée sur la **compétence** et la **recherche de marges de progrès** plutôt que la désignation d'éventuels coupables.
- d'accepter la possibilité de **changer les pratiques** quand celles-ci s'avèrent inopportunes. Cela implique aussi d'accepter de **changer d'indicateurs** quand ceux-ci s'avèrent moins adaptés à l'évolution de la situation, moins acceptés ou moins utilisés qu'espéré.

  Si l'apprentissage s'effectue de manière satisfaisante, il est même prévisible de devoir changer régulièrement d'indicateurs pour suivre l'évolution des réflexions collectives et continuer à les enrichir.

Puis-je utiliser les indicateurs de sécurité au poste de travail pour évaluer la performance sécurité sur les risques majeurs ?

La réponse est clairement non pour deux raisons :

- Les événements associés aux risques au poste de travail sont, en grande majorité, totalement distincts des mécanismes accidentels associées aux risques majeurs.

  Par exemple, les chutes en hauteur, glissades, stress au travail ou troubles musculo-squelettiques (TMS) constituent des causes importantes de risques au poste de travail mais n'entrent aucunement en ligne de compte dans les scénarios associés à des accidents majeurs.

  A ce titre, relever une amélioration des performances de l'entreprise sur ces aspects n'est en rien révélateur d'une amélioration de la gestion de la sécurité au regard des risques majeurs.

L'évaluation de performance en gestion de la sécurité

Puis-je utiliser les indicateurs sécurité au poste de travail...

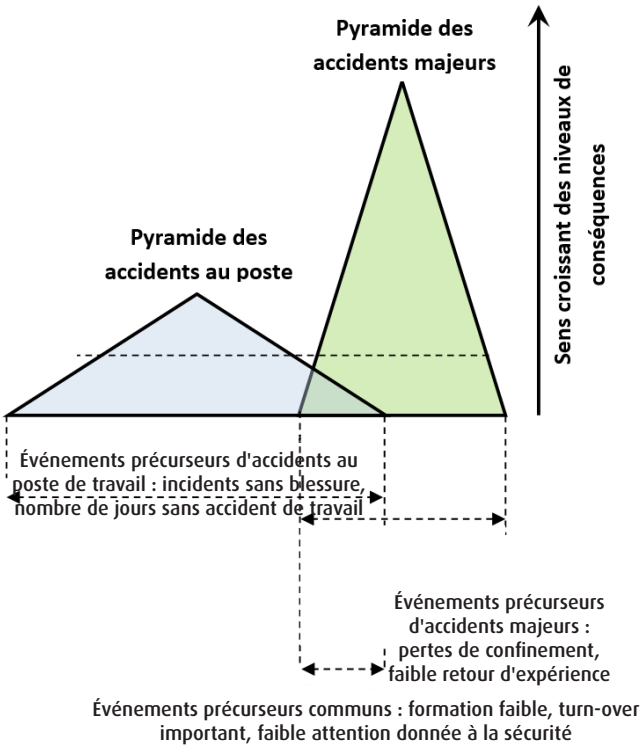


Figure 2 : Distinction entre événements précurseurs pour les risques au poste de travail et les risques majeurs (inspiré d'Hopkins, 2008).

- Les accidents au poste de travail sont bien plus fréquents que les accidents majeurs. De ce fait, si ces deux dimensions étaient considérées conjointement, l'efficacité de l'action managériale commanderait de traiter en priorité les risques au poste de travail au détriment des risques majeurs.

Par conséquent, s'il est envisageable de développer des démarches intégrées de gestion de la sécurité qui considèrent aussi bien la santé/sécurité au poste de travail et la sécurité face aux risques majeurs, il est important d'accorder à chacune de ces dimensions une attention et une réflexion conformes à ses spécificités.

Quel est le lien entre le modèle de la pyramide et mon modèle de sécurité ?

La ***fiche 4*** présente des modèles de sécurité largement reconnus et utilisés dans la gestion des systèmes à risques. La question se pose donc de savoir si le modèle pyramidal partagé dans les différents guides professionnels sur les indicateurs vient concurrencer ou compléter les modèles de sécurité déjà en place au sein des organisations.

Pour répondre à cette question, il est important de rappeler que l'hypothèse marquante du modèle pyramidal est le lien statistique entre incidents et événements de **faible gravité** et accidents **potentiellement graves**.

A ce titre, le modèle est très utile pour effectuer des mesures de performance pour les deux raisons suivantes :

- Il invite à mesurer des **événements** (incidents, événements non désirés...) plus fréquents et donc plus facilement abordables par les approches statistiques classiques au lieu d'événements très rares (pertes de confinements importantes) pour lesquels un suivi statistique est très peu représentatif.
- Il invite à se focaliser sur des événements **antérieurs à l'accident majeur** donnant ainsi des leviers proactifs au gestionnaire de la sécurité.

L'évaluation de performance en gestion de la sécurité

Quelle différence y a-t-il entre indicateurs proactifs et réactifs ?

[11] Dans un monde idéal où le changement de la valeur de l'indicateur est décelé puis correctement interprété et communiqué.

Ils ont dit...

« Un indicateur de résultats pour les uns est un indicateur d'activité pour d'autres »

Neal Williams dans (Eckerson, 2011)

[12] **Railway Safety and Standard Board** : structure multi-acteurs ferroviaires créée en Angleterre suite à la privatisation du secteur qui a entraîné une explosion du nombre d'acteurs de la sécurité ferroviaire.

Ces apports indéniables pour la mesure de performance ne disent rien sur les leviers quotidiens de gestion de la sécurité. Le modèle pyramidal n'est donc pas un modèle de sécurité. Par conséquent, il ne peut entrer en concurrence avec le modèle de sécurité adopté par une organisation. Il vient plutôt en complément pour rappeler que la mesure de performance **ne peut se focaliser uniquement sur les pertes de confinements**, mais qu'elle doit s'intéresser en amont aux mécanismes qui conditionnent la performance sécurité ; mécanismes qui devront justement être décrits dans les modèles de sécurité.

Quelle différence y a-t-il entre indicateurs proactifs (leading) et réactifs (lagging) ?

Les indicateurs sont ici distingués en fonction de leur capacité à anticiper un événement ou à en refléter le déroulement passé. Dans le premier cas, nous parlerons de **proactivité** dans la mesure où la valeur de l'indicateur change avant que l'événement ait lieu permettant ainsi au décideur[11] d'agir avant l'occurrence de l'événement. Dans le cas de la sécurité, un indicateur est dit proactif (Leading ou drive) si sa valeur évolue avant que le niveau de risque ne change (Kjellen, 2009). A titre d'exemple, la baisse du pourcentage de personnel qualifié impliqué dans l'accomplissement d'une tâche donnée est précurseur d'une augmentation du niveau de risque.

Quand l'indicateur ne peut refléter que des événements passés, donc impossibles à corriger, nous parlerons d'**indicateurs réactifs** (lagging) ou indicateurs de résultats (outcome). Dans le cas de la gestion de la sécurité, nous pouvons citer comme exemples : le calcul du nombre d'accidents, le nombre de jours de travail sans accidents, le nombre de pertes de confinement de produits dangereux...

Si la typologie proactif/réactif est largement utilisée dans le domaine des indicateurs de performance sécurité, elle est aussi controversée et demeure encore la source d'ambiguïtés, comme l'illustre le chapitre suivant.

Nombre d'incidents : indicateur proactif ou réactif ?

Comme explicité plus en avant, le caractère réactif ou proactif d'un indicateur se définit relativement à un événement de référence que l'on souhaite détecter. Si l'accident, ou l'Événement Redouté Central (**ERC**) est l'événement de référence, cet indicateur est **proactif** puisqu'il peut pointer une nécessité d'action avant que ces incidents ne se transforment un jour en accidents.

D'un autre côté, si l'événement de référence est la **détérioration du niveau de sécurité** ou l'augmentation du risque, c'est un indicateur **réactif** puisqu'il reflète une dégradation déjà passée même si elle n'a pas encore abouti à un accident majeur. Kjellen (2009) ou EPRI (2000) notent ainsi qu'un indicateur est proactif s'il pointe une évolution de la vulnérabilité du système ; vulnérabilité qui engendrera dans un second temps des incidents ou des accidents.

Par conséquent, nous adoptons dans le cadre de ce guide la vision suggérée par le RSSB[12] (2011) qui propose une vision plus floue au sens mathématique, où chaque indicateur peut être simultanément porteur de capacités proactives et réactives.

Il ne s'agit donc pas de séparer les indicateurs en réactifs d'une part et proactifs d'une autre. Il est plutôt suggéré que chaque indicateur peut apporter des éléments dans les deux sens en fonction des usages qui en sont faits. Le caractère proactif ou réactif d'un indicateur n'est donc pas lié à sa formule, mais plutôt aux modalités de son utilisation.

L'évaluation de performance en gestion de la sécurité

De combien d'indicateurs ai-je besoin pour évaluer les performances sécurité de mon système ?

Le RSSB nous invite ainsi à placer les indicateurs dans un continuum allant de purement proactif à purement réactif (***Figure 3***).

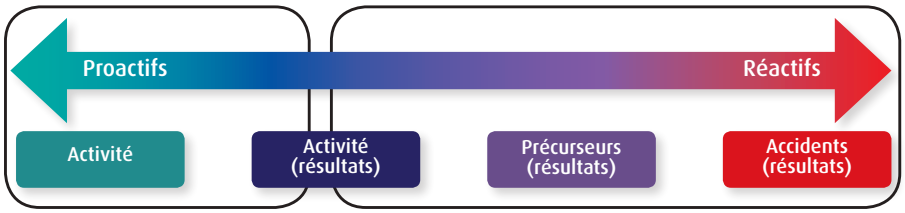


Figure 3 Continuum d'indicateurs proactifs et réactifs par le RSSB (2011)

De combien d'indicateurs ai-je besoin pour évaluer les performances sécurité de mon système ?

La variété des systèmes à risques empêche toute réponse définitive à cette question. Néanmoins, rappelons les éléments suivants :

- Parmi les pratiques industrielles présentées précédemment, celles basées sur la mesure des pertes de confinement semblent très limitées. En effet, elles ne reflètent que des événements passés et ne permettent pas de comprendre les points faibles de l'organisation qui ont engendré ces événements.
- Le choix du nombre d'indicateurs doit être un équilibre subtil entre les contraintes suivantes :
  - Disposer d'un *nombre suffisant d'indicateurs* pouvant être croisés et recoupés afin d'investiguer les forces et faiblesses de l'organisation et dessiner des voies d'amélioration.
  - Ne pas *dépasser les capacités de l'organisation* (temps, compétences, motivation...) pour collecter les données, les traiter et en tirer l'apprentissage collectif nécessaire.

Ce qu'il faut retenir...

- L'évaluation des performances est une **étape clé** de toute démarche de gestion de la sécurité.
- Les indicateurs ne sont **pas les seuls outils** d'évaluation de performance. Ils peuvent être complétés par d'autres approches telles que les audits, questionnaires ou diagnostics organisationnels.
- Malgré d'importants efforts de mutualisation et de partage des pratiques au niveau de l'ensemble de l'industrie des procédés, la variété des systèmes et des visions de la sécurité génère aujourd'hui une **large hétérogénéité** des pratiques opérationnelles.
- Les indicateurs ne sont pas uniquement des outils de remontée d'informations sécurité, ils constituent aussi des **véhicules de communication** des valeurs et priorités définies par l'organisation quant à la gestion de la sécurité. Les indicateurs deviennent donc des outils permettant au personnel opérationnel de se faire une représentation de ce que le management définit comme prioritaire, y compris s'agissant de l'importance de la sécurité au regard des autres dimensions de la vie du système (qualité, satisfaction client, productivité, performance financière...)
- La sécurité des procédés doit être considérée de manière **décorrélée** de la sécurité au poste de travail.
- Un indicateur n'est pas exclusivement réactif ou proactif. Il peut être **l'un et l'autre** à différents degrés en fonction de son contexte d'utilisation.
- Le modèle pyramidal largement répandu dans les guides professionnels sur les indicateurs sécurité permet, dans un premier temps, une **harmonisation** des mesures de performance sécurité basées sur les pertes de confinements. Néanmoins, il insiste sur la nécessité d'**aller plus loin** que la mesure des pertes de confinement pour une évaluation proactive des performances sécurité. Pour autant, il ne fournit **pas de cadre méthodologique** adapté.
- Pour aller plus loin, chaque organisation doit mettre en place une **démarche systématique et organisée** permettant de questionner son modèle de sécurité afin d'en déduire les indicateurs adaptés à son contexte et à sa vision de la sécurité.

La méthode SIPS

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Présentation de la méthode

Présentation de la méthode

Objectifs

La méthode de définition/conception d'indicateurs de performance sécurité déclinée dans cette seconde partie a pour objectif de proposer un **cadre rigoureux et systématique** permettant d'interroger le modèle de sécurité d'une organisation pour en déduire des indicateurs de performance adaptés.

Positionnement

Il existe déjà de nombreuses méthodes d'identification d'indicateurs de performance sécurité (Renvoi ***fiche 5***). Il est donc légitime de s'interroger sur l'intérêt d'en proposer une nouvelle.

La méthode SIPS se distingue des méthodes existantes sur les aspects suivants :

- Les méthodes existantes prennent comme point de départ un modèle de sécurité spécifique et cherchent ensuite à en déduire des indicateurs. De ce fait, adopter une de ces méthodes revient nécessairement à **adopter le modèle de sécurité** sous jacent. Ainsi par exemple :
  - la méthode proposée par Oien (2001) implique d'avoir préalablement adopté une approche d'estimation du risque de type QRA[13],
  - les méthodes HSE (2006) et Tripod-Delta (1994) impliquent d'adopter le modèle de Reason (1997),
  - La méthode CCPS (2011) implique d'adopter le modèle pyramidal
  - la méthode REWI (Oien, Massaiu, & Tinmannsvik, 2012) nécessite de placer la résilience au centre de sa vision de la sécurité.

  Or, les modèles de sécurité adoptés par les organisations sont rarement, pour ainsi dire jamais, entièrement fidèles à un modèle théorique particulier. Ce sont plus des mix de modèles théoriques forgés au fur et à mesure des évolutions réglementaires, culturelles et techniques toujours spécifiques à chaque organisation. Dans un tel contexte, adopter une de ces méthodes revient à **enfermer la vision** d'une organisation dans un espace théorique nécessairement réducteur.

  A titre d'exemple, il est très commun dans le **cadre réglementaire français** que les organisations adoptent l'analyse de risques fondée sur des **arbres d'événements** ainsi que le **SGS** comme bases de leur modèle de sécurité. Dans ce cas, aucune des méthodes précitées ne permet de traduire les leviers d'action sur la sécurité identifiés dans un tel modèle en indicateurs de performances.

  La méthode SIPS propose de ne **pas enfermer** la vision de la sécurité développée par chaque organisation dans un modèle prédéfini. Elle se propose plutôt de doter les organisations d'outils pour interroger leur propre modèle afin de déduire des indicateurs de performance adaptés. Les indicateurs sont alors au service de la sécurité et non l'inverse.

- La méthode suggérée propose la mise en place d'un **système d'indicateurs**. Le terme système désignant un ensemble d'éléments coordonnés en vue d'un objectif prédéfini, le concept de système d'indicateurs implique que ces indicateurs n'ont de sens que si considérés ensemble et leurs valeurs recoupées, croisées et analysées afin de servir l'objectif d'apprentissage collectif.

[13] **Quantitative Risk Assessment**

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Présentation de la méthode

Ainsi, plutôt que de simplement comparer les valeurs remontées par les indicateurs avec des objectifs prédéfinis (management par les chiffres), la méthode SIPS invite à utiliser les indicateurs comme des outils d'une investigation organisée de la complexité des mécanismes sous jacents à la sécurité.

Tel un médecin qui combine plusieurs indicateurs pour juger de l'état général du patient et solliciter, quand c'est nécessaire, des investigations plus spécifiques et plus approfondies, les indicateurs sécurité serviront à construire une représentation globale de l'état du système à risques.

Ils permettront également de déceler les axes d'améliorations ou les éléments nécessitant des investigations plus approfondies à travers d'autres outils complémentaires (audits, diagnostics...).

Description

Sur la base de ces éléments, la méthode SIPS s'organise selon la boucle détaillée en ***Figure 4***. Deux grandes phases sont à distinguer :

- La **phase 1** vise à définir **ce qui doit faire l'objet** d'indicateurs de performance sécurité. En d'autres termes, il s'agit de répondre à la question « que faut-il mesurer ? ». Pour y répondre, il est nécessaire d'explorer, ou à minima de rendre explicite, le modèle de sécurité adopté par l'organisation ainsi que les attentes décisionnelles associées à l'implémentation de ce modèle.
- Les objets à mesurer ainsi définis, la **phase 2** s'intéresse à définir les **outils ou métriques** à utiliser pour approcher au mieux les objets à mesurer identifiés. Il s'agit donc ici de répondre à la question « Comment mesurer ? ».

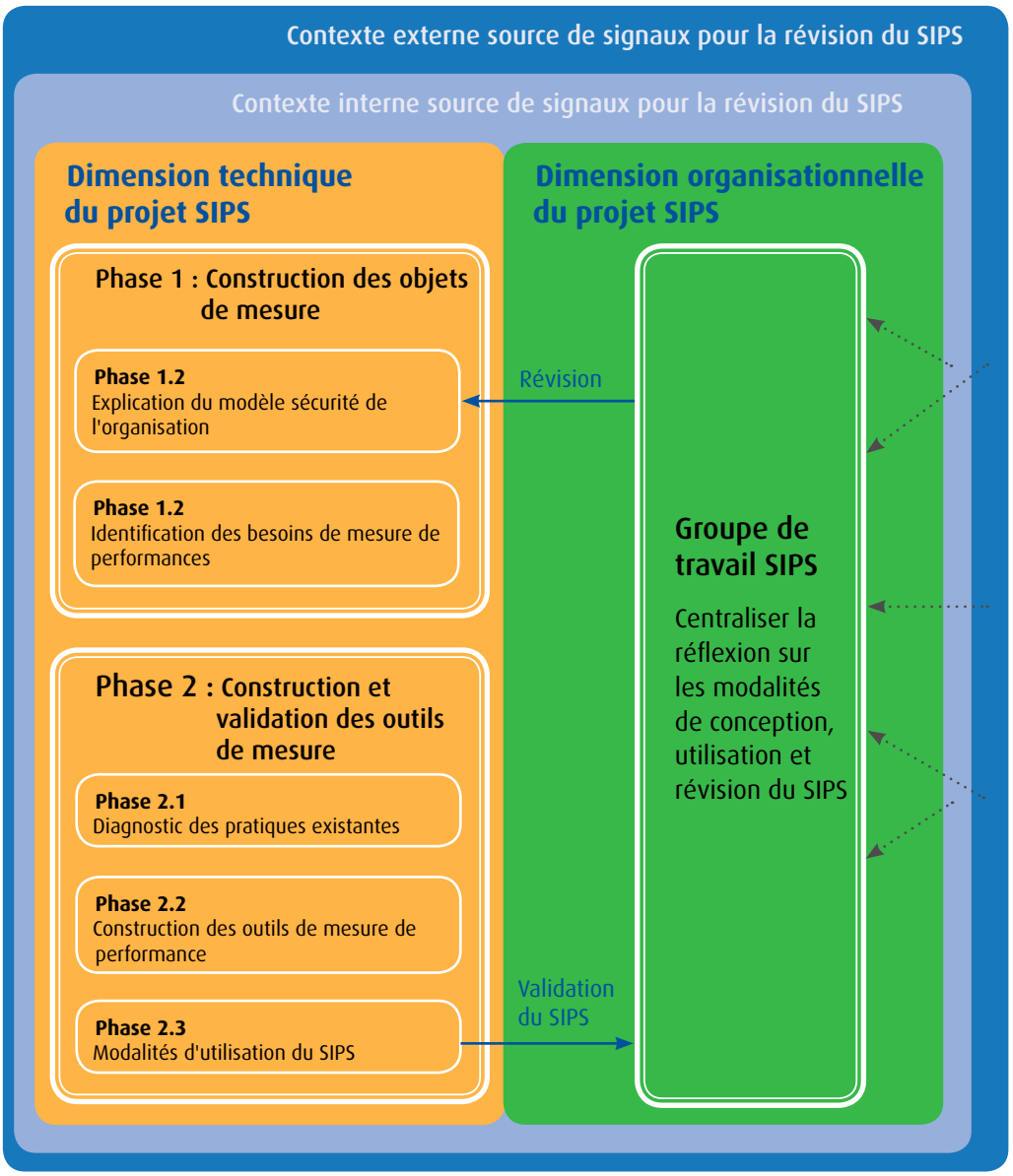
Enfin, les évolutions de l'organisation (internes) et de son environnement (externes) doivent être considérées dans le cadre d'un **cycle continu** de révision et de mise à jour des indicateurs.

Pour faire vivre cette méthode et l'adapter en continu aux évolutions de l'organisation, un **groupe de travail** doit centraliser les processus de conception du SIPS et de suivi de son évolution dans le temps.

La méthode proposée n'est **pas linéaire**. Elle représente plutôt **un cycle** où le SIPS apprend, évolue et s'adapte à l'évolution naturelle du système à risques.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Présentation de la méthode



Signaux internes et externes à prendre en compte pour reviser le SIPS

Figure 4 Schéma de la méthode d'élaboration SIPS

Aspects organisationnels de la méthode : constitution du groupe de travail SIPS

Objectifs

Le SIPS devant s'ancrer dans une optique d'apprentissage en continu, la méthode proposée ne peut s'arrêter à la phase de proposition des indicateurs. Un SIPS peut être valide à un moment donné de la vie de l'organisation mais devra évoluer avec celle-ci si l'on souhaite qu'il reste pertinent.

Par conséquent, la méthode proposée ne vise pas uniquement à proposer un SIPS adapté à une organisation ; elle s'intéresse aussi aux modalités de sa révision dans le temps.

Un préalable nécessaire à cette méthode est donc la constitution du groupe de travail SIPS avec pour mission première de centraliser la réflexion sur les modalités de conception, utilisation et révision du SIPS au sein de l'organisation.

Cette mission générale peut être déclinée en trois activités :

- **Concevoir et réviser.** Pour s'assurer que le SIPS sera effectivement utilisé et approprié par les différents échelons organisationnels concernés, il est

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects organisationnels de la méthode : Constitution du groupe de travail SIPS

important que ceux-ci puissent être représentés et leurs positions prises en compte. Le groupe de travail doit donc être le lieu d'une co-construction des orientations techniques et organisationnelles fondant le SIPS.

- **Communiquer en interne** afin d'expliquer l'apport du SIPS pour la performance sécurité de l'organisation. Il s'agit ici de donner au SIPS les meilleures chances d'être accepté par les acteurs du système et en faire ainsi un des éléments influençant leurs attitudes quotidiennes face aux risques. Plus particulièrement, il est important de s'assurer, et si nécessaire, rechercher l'appui continu du top management pour le projet SIPS.
- **Recueillir** en continu les signaux en interne et en externe de l'organisation sur la nécessité de réviser le SIPS. S'agissant des signaux internes, nous pouvons citer: les difficultés d'utilisation remontées par le personnel, réorganisations, évolution des activités de l'organisation et des risques qui lui sont associés, révision par le top management du modèle de sécurité...

  En termes de signaux externes : Nouveaux référentiels techniques, évolution des bonnes pratiques, évolution de la réglementation, demandes particulières de l'autorité d'inspection...

Plus globalement, le GT doit constituer un espace d'échange privilégié sur la manière dont le SIPS est compris et utilisé par l'ensemble des acteurs de l'organisation, les forces qu'il démontre et les ajustements qui sont nécessaires. C'est bien au sein de ce groupe que l'apprentissage doit avoir lieu pour ensuite être partagé.

Modalités opérationnelles

Des représentations variées et pas toujours cohérentes de la notion de sécurité peuvent cohabiter au sein de la même organisation. Au-delà des différences de représentations classiques entre ceux qui éditent les règles (management) et ceux qui les appliquent (opérateurs), la littérature a pointé la possibilité que plusieurs cultures sécurité coexistent au sein d'une même organisation (Gadd & Collins, 2002).

Par conséquent, le projet SIPS doit constituer une opportunité de création d'un espace critique d'échange et d'interaction entre tous ceux qui influent sur la performance sécurité du système et qui possèdent nécessairement leurs propres représentations. Ainsi, une démarche ascendante et participative qui laisse une place prépondérante à la liberté de parole et à l'expertise opérationnelle en lieu et place d'une démarche descendante basée essentiellement sur les rapports hiérarchiques doit s'instaurer.

Pour servir cette finalité, nous proposons les modalités opérationnelles suivantes :

- Les participants doivent être **représentatifs** des niveaux hiérarchiques et entités appelées à utiliser le SIPS. Les nouveaux acteurs qui peuvent apparaitre en cours de projet peuvent être intégrés à tout moment.
- L'acteur en charge du projet SIPS doit jouer un rôle de **facilitation** et d'**animation** de l'échange afin de permettre la construction, autant que possible, de représentations communes et partagées.
- Il est recommandé d'inclure un **représentant** du **top management** dans le GT. Cela lui permettra de préciser les valeurs auxquelles l'organisation est attachée tout en s'appropriant les réflexions issues du projet. A terme, il pourra constituer un appui fort pour la continuité du SIPS dans l'organisation.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects organisationnels de la méthode : Constitution du groupe de travail SIPS

- Les modalités d'**arbitrage** et de **prise de décision** doivent être prédéfinies. En effet, l'unanimité étant rare, il est nécessaire de définir à l'avance les modalités de décision quand il s'agira de choisir une orientation (adopter ou rejeter un indicateur, réviser ou non un indicateur existant...) même si l'ensemble des membres du GT ne partage pas une vision commune.

Résultats attendus

- Un **espace d'échange critique** entre les concepteurs et utilisateurs des indicateurs performance sécurité.
- Une vision de la sécurité **mieux partagée et mieux communiquée** à tous les niveaux de l'organisation.

Aspects techniques de la méthode : déroulé des phases

Pour aller plus en détail dans le déroulé des différentes phases, nous présentons ici un cas d'étude qui servira de fil rouge illustratif de chacune des phases de travail.

Cas d'étude

Le système étudié est une unité de stockage et dépotage d'isobutylène composée des éléments suivants :

- Deux réservoirs de 32 m³ et 29 m³ d'isobutylène connectés (25 mm de diamètre pour le transfert de la phase gaz et 100 mm pour la phase liquide)
- Une station de dépotage.
- L'ensemble de l'installation est entourée par un grillage pour éviter les intrusions.
- Les réservoirs alimentent deux fois par jour un réacteur chimique distant de 200 m grâce à une pompe volumétrique et une tuyauterie de 32 mm de diamètre.
- Le ravitaillement des réservoirs s'effectue par camion deux fois par semaine par un opérateur formé. Le dépotage est réalisé au moyen d'une seconde pompe volumétrique et de deux flexibles (phases gaz et liquide).

Deux événements redoutés centraux sont identifiés :

- Le BLEVE [14] des réservoirs suite à un incendie.
- Une fuite d'isobutylène qui peut mener à un UVCE [15] ou un feu torche.

Les mesures de maitrise des risques installées et les fonctions de sécurité associées sont présentées en ***Tableau 2*** ci-après.

[14] **Boiling Liquid Expanding Vapor Explosion.**

[15] **Unconfined Vapor Cloud Explosion.**

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

Fonctions de sécurité	Équipements	Actions associées
Éviter les pertes de confinement dans les réservoirs dues au surremplissage ou au dépassement des niveaux de pression	Mesure analogique des niveaux phase liquide dans chacun des réservoirs.	▪ Arrêt de la pompe de dépotage ▪ Activation des alarmes
	Alarme niveau très haut à 90% du volume de stockage dans chaque réservoir	▪ Arrêt de la pompe de dépotage. ▪ Fermeture automatique des vannes du circuit de remplissage. ▪ Activation des alarmes
	Détecteur de pression avec transmission de message d'alerte à 8 bars (Enveloppe du réservoir dimensionnée pour une pression allant jusqu'à 15 bars).	▪ Arrêt de la pompe de dépotage. ▪ Fermeture automatique des vannes du circuit de remplissage. ▪ Activation des alarmes
Limiter les fuites issues des tuyauteries, pompes, brides, joints, valves, piquages..	2 détecteurs de gaz couvrant l'ensemble du système avec déclenchement d'alerte à 20% de LIE.	▪ Arrêt des pompes de dépotage et de ravitaillement du réacteur. ▪ Fermeture automatique des vannes du circuit de remplissage. ▪ Isolation des deux réservoirs. ▪ Activation des alarmes.
Maintenir la température des réservoirs de stockage à un niveau acceptable en cas d'incendie sur ou à proximité du système.	Détecteur incendie et sprinkler automatique.	▪ Arrêt des pompes de dépotage et de ravitaillement du réacteur. ▪ Fermeture automatique des vannes du circuit de remplissage. ▪ Isolation automatique des deux réservoirs. ▪ Activation des alarmes ▪ Déclenchement des sprinklers (10 l/m²/min).

Tableau 2 : Mesures de maîtrise des risques et fonctions de sécurité associées.

Phase 1 : Construction des objets de mesure

La phase 1 se décompose en 2 étapes distinctes :

- ❒ L'explicitation du **modèle de sécurité** de l'organisation.
- ❒ L'identification des **besoins de mesure de performance**.

Étape 1.1 : Explicitation du modèle sécurité de l'organisation

Objectifs

Le modèle de sécurité constitue la fondation du SIPS dans la mesure où il désigne les aspects du système qu'il faut suivre dans le temps pour gérer la sécurité. Il est hautement probable qu'un modèle de sécurité préexiste dans l'organisation. Néanmoins, le modèle officiel ou affiché par le management peut ne pas refléter la réalité des pratiques et comportements quotidiens.

Cette première étape est donc l'occasion de discuter en interne, avec des représentants des différents acteurs de la sécurité, non pas du modèle affiché mais de celui qui est effectivement appliqué dans les faits.

Par conséquent, cette première étape vise à rappeler/confirmer/expliciter le modèle de sécurité qui reflète le mieux la réalité des pratiques et les objectifs de l'organisation.

Modalités opérationnelles

Il n'existe pas un unique « bon » modèle qui soit adaptable à la variété des pratiques et systèmes industriels que l'on peut retrouver dans l'industrie des procédés chimiques (voir ***fiche 4***). Chaque organisation définit celui qui peut au mieux refléter son identité et sa culture tout en servant au mieux les objectifs sécurité qu'elle s'est fixée.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

Dans de nombreux cas, le modèle est déjà clairement établi même si des différences d'opinions sur les modalités pratiques de son application peuvent subsister. Dans ce cas, il s'agira de tirer profit de l'opportunité de l'élaboration du SIPS pour améliorer la mise en pratique du modèle déjà décidé.

Quand ce modèle n'a pas été au préalable clairement défini et établi, le groupe de travail doit aider l'organisation à examiner ses pratiques sécurité. Pour cela, elle peut se référer aux modèles théoriques décrits en ***fiche 4*** comme repères théoriques auxquels elle invitera les participants à comparer les pratiques réelles afin de mieux les cerner.

Les questions décrites ci-dessous peuvent être autant de thèmes de discussion lors de ces échanges :

- ❒ Y a-t-il pour vous une **différence** entre maîtrise des risques et gestion de la sécurité ?
- ❒ En quoi consiste pour vous la **gestion quotidienne** de la sécurité ?
- ❒ Lequel des modèles théoriques présentés en ***fiche 4*** est-il **le plus proche** de vos pratiques quotidiennes ?
- ❒ Pensez vous que le modèle de sécurité actuel doive **évoluer** ? Si oui, quelles modifications y apporter ?

Les réponses à ces questions et les échanges qui s'en suivront ne visent pas à servir une quête de conformité avec des modèles théoriques prédéfinis. Ils doivent plutôt aider l'organisation à analyser la réalité de ses pratiques et de ses représentations concernant la sécurité.

Résultats attendus

Décrire le modèle de sécurité de l'organisation de manière :

- ❒ **Réaliste** dans la mesure où il reflète les pratiques sécurité sur le terrain
- ❒ **Partagée** autant que possible par l'ensemble des membres du groupe de travail. Plus le modèle est partagé, plus le SIPS qui en résultera sera légitime et appliqué.

Application

Dans le cadre du système étudié, le modèle sécurité de l'entreprise se décrit comme suit :

- ❶ La **maîtrise des risques** s'effectue en priorité par :
- ❒ le maintien dans le temps des **performances des barrières de sécurité** identifiées lors de l'analyse des risques.

  Dans le cas présent, la focalisation porte donc sur les différents systèmes asservis décrits en tableau 2, à savoir :

  - Détecteur niveau haut-alarme-arrêt de la pompe de dépotage et fermeture des vannes circuit de remplissage.
  - Détecteur de pression-alarme-arrêt de la pompe de dépotage et fermeture des vannes circuit de remplissage.
  - Détecteur de gaz-alarme-arrêt de la pompe de dépotage et fermeture des vannes circuit de remplissage.
  - Détecteur incendie de la pompe de dépotage et fermeture des vannes circuit de remplissage-déclenchement des sprinklers.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

- Le maintien dans le temps de l'**intégrité mécanique des installations** (réservoirs, brides, joints, flexibles...) permettant d'éviter les pertes de confinement du fait de la corrosion ou de la fatigue mécanique.

❷ S'agissant des aspects **humains et organisationnels**, la gestion de la sécurité est abordée au travers du **SGS** composé des rubriques suivantes :

- Connaissance du risque au travers d'analyses de risques détaillées répertoriant les scénarios accidentels et les barrières de sécurité associées.
- Gestion des habilitations/formations des personnes intervenant sur le site.
- Inspection et maintenance des installations
- Définition et réactualisation des procédures opérationnelles.
- Gestion des modifications.
- Gestion des situations d'urgence.
- Mise en place d'un retour d'expérience.

Il a donc été convenu dans le cadre du groupe de travail d'aborder les rubriques du SGS associées à chacun des objets de mesure que nous identifierons dans la phase suivante.

❸ Enfin, le site (désigné dans la suite comme site A) présente la spécificité d'entièrement sous-traiter sa maintenance à l'entreprise Seveso mitoyenne (Site B). Celle-ci, bien que disposant d'un service dédié, sous-traite à son tour un grand nombre des interventions et inspections réalisées aussi bien sur son site que sur le site A. Cette sous-traitance en cascade est donc un élément contextuel important du modèle sécurité du système.

Nous notons donc que le modèle de sécurité discuté ici est le résultat d'un mix entre une vision théorique de la sécurité et une réalité contextuelle qui impose de s'y adapter. S'agissant des aspects théoriques :

- La focalisation sur le maintien dans le temps des barrières identifiées et de l'intégrité mécanique des installations reflète une vision de la sécurité basée sur l'**absence de risque**s, ou en tous cas, sur le maintien de ces derniers dans les limites jugées acceptables.
- Les rubriques du SGS décrivent les processus à travers lesquels l'organisation définit les **ressources**, **responsabilités** et **plans d'actions** associés à la maîtrise des risques.

S'agissant des aspects contextuels, la sous-traitance en cascade de la maintenance est une spécificité qui, au regard de l'importance des barrières techniques, conditionnera fortement le choix des indicateurs de performance.

Nous notons donc ici que cette vision globale de la sécurité ne se retrouve dans aucun des modèles théoriques décrits en ***fiche 4***. Cela confirme le positionnement de la méthode SIPS qui consiste à comprendre puis interroger le modèle sécurité spécifique de chaque organisation.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

Étape 1.2 : Identification des besoins de mesure de performance

Objectifs

Une fois le modèle sécurité de l'organisation explicité, il s'agit d'en extraire les objets dont les performances devront être mesurées dans le cadre du SIPS. Les objets en question peuvent être de natures très variées : des systèmes techniques, des processus managériaux, des attitudes individuelles, des facteurs organisationnels...

Notons que tous les objets identifiés par un modèle de sécurité ne pourront pas être approchables par des indicateurs en raison notamment de leur complexité. Pour certains objets, la question de savoir s'il est préférable de les mesurer par le SIPS ou par des questionnaires, des audits ou des diagnostics organisationnels peut se poser.

Cette seconde étape vise donc à définir les besoins d'évaluation de performance qui peuvent être traduits en systèmes d'indicateurs de Performance Sécurité.

Modalités opérationnelles

L'étape suggérée comporte les quatre temps suivants :

❶ **Extraire du modèle les objets nécessitant une mesure de la performance**
Identifier de manière exhaustive tout élément dont la variabilité des performances peut avoir un effet sur la sécurité du système.

❷ **Examiner l'opportunité de suivre les performances de ces objets au regard des spécificités de l'organisation et des ressources disponibles**

La complexité des systèmes à risques peut rapidement rendre très longue la liste des objets nécessitant un suivi des performances. Par conséquent, des arbitrages devront être effectués sur les priorités à adopter et celles que l'organisation ne peut assumer au regard des ressources disponibles.

La traçabilité de ces arbitrages est importante dans la mesure où les dimensions de la performance sécurité abandonnées à ce niveau peuvent être reconsidérées lors des mises à jour ou révision du SIPS.

❸ **Évaluer l'opportunité de les mesurer dans le cadre du SIPS.**
Les indicateurs ne sont pas toujours les outils les plus adaptés à la mesure de la performance des objets identifiés. A titre d'exemple, la mesure des attitudes individuelles vis-à-vis de la sécurité est plus facilement approchable par des questionnaires dédiés ou des auto évaluations ; la qualité de la communication sécurité entre équipes est là aussi un objet difficilement approchable par des indicateurs.

Par conséquent, il s'agit ici de trier parmi les objets considérés comme nécessitant un suivi de performance ceux qui demeurent approchables par un SIPS et ceux nécessitant des approches complémentaires de type questionnaires, audits ou diagnostics.

❹ **Valider la liste des objets de mesure avec le management.**
Cela peut nécessiter plusieurs séries d'échanges avant d'aboutir à une vision commune.

La synthèse de cette démarche est présentée en diagramme dans la ***Figure 5***.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

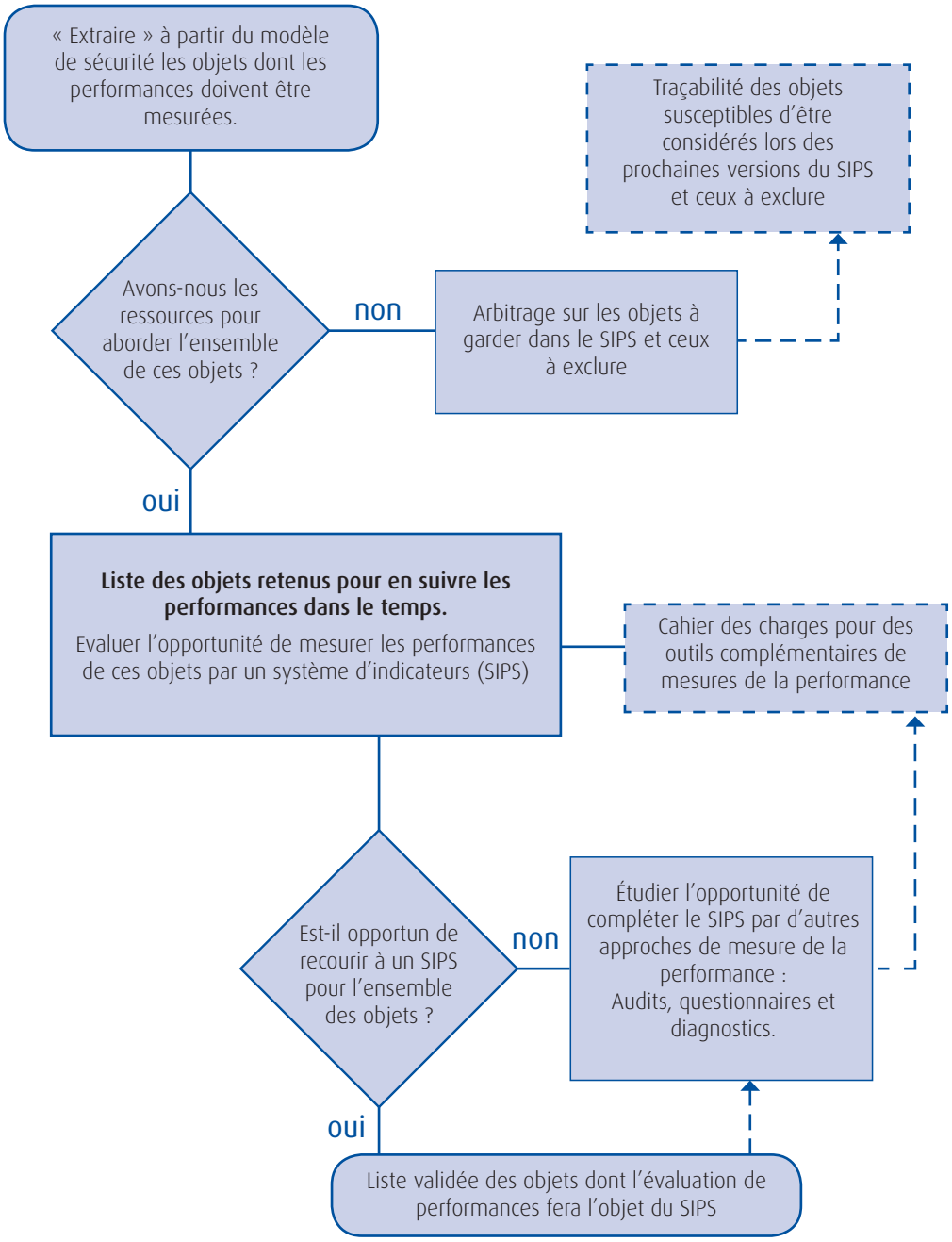


Figure 5 Organigramme d'identification des besoins en termes d'évaluation des performances sécurité

Résultats attendus

- La liste des objets (activités, processus, systèmes techniques...) dont le suivi des performances est jugé nécessaire au regard du modèle de sécurité adopté.
- La liste des objets ne pouvant être abordés au regard du niveau de ressources disponibles en l'état [16] .
- La liste des objets devant être abordés par des outils autres qu'un SIPS.
- La liste des objets dont les performances seront considérées par le SIPS.

[16] **Les objets de cette catégorie ne sont pas destinés à demeurer à l'écart du SIPS. Il s'agit de les inclure à terme soit par une augmentation des ressources soit par une meilleure efficacité du SIPS grâce à l'expérience et l'apprentissage que l'organisation peut acquérir dans le temps.**

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

Application

❒ Extraire du modèle les objets nécessitant un **suivi de performances** dans le temps

L'analyse des arbres d'événements du système considéré a permis d'identifier les éléments techniques et humains intervenant dans l'occurrence des séquences accidentelles.

Pour sélectionner parmi ces éléments ceux susceptibles d'être considérés pour un suivi des performances dans le temps, deux critères ont été considérés :

- L'élément doit avoir un impact sur la sécurité du système.
- Le comportement de l'élément doit être suffisamment évolutif dans le temps pour nécessiter un suivi régulier.

Le ***Tableau 3*** ci-dessous présente les résultats de cette analyse.

Éléments influents pour la sécurité	Modalités d'évolution des performances dans le temps.	Évaluation par le GT de la nécessité d'un suivi des performances dans le cadre d'un SIPS.
Barrières considérées dans les analyses de risques[17] ❒ Détecteur niveau haut. ❒ Détecteur pression ❒ Détecteur gaz ❒ Détecteur feu	Les performances des barrières sont évolutives dans le temps car dépendantes de facteurs tels que la politique de maintenance ou le retour d'expérience.	Oui
Maîtrise de la corrosion/fatigue mécanique	Les performances mécaniques des dispositifs peuvent être fortement évolutives dans le temps, notamment du fait de la corrosion et de la fatigue mécanique	Oui
Conformité aux normes séisme	Les choix de conception du système permettent de répondre aux objectifs fixés par l'arrêté du 04/10/2010. Les contrôles de vieillissement de structure sont planifiés sur des échelles de temps importantes (5 à 10 ans) et ne nécessitent donc qu'un suivi des performances fortement étalé dans le temps.	Non. Un suivi quinquennal ou décennal est suffisant
Mise à terre réservoir Équipements de protection contre la foudre	Ces éléments nécessitent des inspections dans le temps pour s'assurer du maintien de leurs performances.	Oui
Malveillance	La performance des dispositifs mis en place est jugée très peu évolutive, voire passive. Elle ne nécessite donc pas un suivi de performances par des indicateurs.	Non
Zonage ATEX.	Le zonage ATEX est géré dans le cadre du Document Relatif à la Protection Contre les Explosions (DRPCE) annexé au document unique. Celui-ci définit les dispositifs de maitrise des risques et les modalités de leur suivi dans le temps.	Non Les aspects ATEX sont déjà complètement gérés dans le cadre du DRPCE (y compris au moyen d'indicateurs dédiés).
Respect des procédures par l'opérateur Surcharge opérateur dépotage Capacité de réaction opérateur dépotage	Les performances humaines sont reconnues comme pouvant être très variables dans le temps.	Oui

Tableau 3 : Liste des objets dont le suivi de performances est jugé nécessaire au regard du modèle de sécurité.

[17] **Les barrières en question désignent l'ensemble des systèmes asservis décrits précédemment et non pas les détecteurs uniquement. Ces derniers sont néanmoins les seuls cités dans le tableau pour des raisons pratiques.**

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

❒ Examiner l'opportunité de **suivre les performances** de ces objets au regard des **spécificités** de l'organisation et des **ressources** disponibles

Cette seconde étape étudie plus en détail chacun des objets distingués ci-dessus afin de définir les aspects de leurs performances nécessitant un suivi. En effet, chacun des objets décrits précédemment peut faire l'objet d'un suivi sur de nombreux aspects.

A titre d'exemple, le suivi des barrières implique :

- de s'assurer que la *politique de maintenance et d'inspection* (y compris la compétence des intervenants à ce niveau) est adaptée et correctement mise en place ;
- un *retour d'expérience systématique* est réalisé afin de continuellement améliorer la compréhension de leur fonctionnement ;
- Une *gestion des modifications* pour s'assurer que les barrières demeurent adaptées aux évolutions du système.

Pour ce faire, chacun des éléments précédemment identifiés a fait l'objet d'une analyse systématique pour identifier les rubriques du SGS impliquées dans le suivi de sa performance.

Les résultats de cette analyse sont présentés en ***Tableau 4*** ci-après.
Il ressort rapidement de cette analyse que l'étendue des besoins en termes de mesure des performances est plus importante que les ressources envisagées.

De plus, il a été souhaité de restreindre, dans un premier temps, la réflexion sur un ensemble limité d'indicateurs qui pourrait ensuite être élargi de manière graduelle.

Au regard de ces éléments, les arbitrages suivants ont été effectués par le groupe de travail :

- Le retour d'expérience et la gestion des modifications sont des processus transverses à l'ensemble de l'organisation et dépassent le simple cadre du système considéré ici. De ce fait, le suivi de ces deux processus dans le temps fera l'objet d'une **étude dédiée** dans un second temps.

  A ce titre, les rubriques retour d'expérience et gestion des modifications sont identifiées comme deux objets devant faire l'objet d'une réflexion lors des prochains développements du SIPS.

- S'agissant des **aspects humains**, une analyse ergonomique dédiée aux activités de dépotage d'isobutylène a été effectuée à la demande du groupe de travail. Celle-ci a permis de déduire que le **facteur de détérioration** de la performance humaine (respect des procédures, erreur de manipulation, capacités de réaction en cas de fuite...) le plus important demeure l'**augmentation du niveau d'activité**, et plus précisément, la multiplication des dépotages simultanés impliquant d'autres produits.

  De ce fait, il a été décidé que la charge de travail de l'opérateur était un facteur à considérer dans le cadre du SIPS alors que les aspects relatifs au respect des procédures et à l'évaluation des capacités de réaction de l'opérateur seront plutôt considérés dans le cadre des audits menés régulièrement par ailleurs.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

Nous retiendrons donc pour la suite de ce travail que :

- Les objets **ne nécessitant pas** d'être considérés au sein du SIPS sont les suivants :
  - Conformité séisme.
  - Malveillance.
  - Zonage ATEX.
- Les objets de mesure **susceptibles** d'être considérés lors des prochains développements du SIPS :
  - Gestion des modifications.
  - Retour d'expérience.
- Les objets **retenus** pour la suite de la démarche sont :
  - Politique maintenance et inspection des équipements, et notamment les barrières de sécurité.
  - Surcharge des opérateurs dépotage.

❒ Évaluer l'opportunité de les **mesurer dans le cadre du SIPS**.

A ce stade de la réflexion, le GT a considéré que les objets retenus pouvaient tous faire l'objet d'indicateurs de performance.

Il n'est néanmoins pas exclu de revenir sur ce jugement lors des prochaines étapes de la méthode.

Cette proposition a été validée par le management du site.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

Eléments influents pour la sécurité.	Items du SGS							Commentaires
	Connaissance des risques	Habilitations formations	Inspection Maintenance	Procédures opérationnelles	Gestion des modifications	Situations d'urgence	Retour d'expérience	
Barrières de sécurité			√		√		√	Les barrières techniques doivent être inspectées et maintenues dans le temps, leur pertinence réévaluée en cas de modification du système ou si un retour d'expérience apporte un éclairage nouveau quant à leur pertinence.
Maitrise de la corrosion/fatigue mécanique	√		√		√		√	L'intégrité mécanique des installations implique des choix pertinents d'hypothèses de conception (Analyse de risques), une politique de maintenance adaptée ainsi qu'une réévaluation à la lumière d'éventuelles modifications ou de retour d'expérience.
Respect des procédures par l'opérateur dépotage		√		√	√		√	Pour assurer une gestion dans le temps des activités humaines impliquées dans le dépotage d'isobutylène, il est nécessaire de : □ S'assurer que les habilitations et formations sont continuellement remises à jour et en adéquation avec les activités de l'opérateur. □ S'assurer du respect des procédures et de la réadaptation de ces dernières quand cela est nécessaire.
Surcharge opérateur dépotage		√		√	√		√	□ Adapter les formations et procédures en cas de modifications sur le système. □ S'assurer que l'opérateur possède une bonne connaissance des gestes et procédures en situation d'urgence.
Capacité de réaction opérateur dépotage		√		√	√	√	√	□ Mettre en place un retour d'expérience permettant de tirer profit des incidents pour améliorer les formations, procédures ou conditions de travail de l'opérateur dépotage.

Tableau 4 : Les rubriques SGS associées au suivi de performance des éléments identifiés.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

Phase 2 : Construction des outils de mesure

La réponse à ce qui doit être mesuré ayant été apportée, la phase 2 vise à fournir les outils de cette mesure. Avant de présenter la démarche proposée, rappelons ci-dessous les principales contraintes et difficultés associées à cette étape.

- Piloter la performance nécessite plus que des indicateurs qui reflètent l'état du système. Elle nécessite des indicateurs qui fournissent des **capacités explicatives** pour investiguer et diagnostiquer les raisons de la performance et les modalités de son amélioration continue. Par conséquent, il est nécessaire de développer des systèmes d'indicateurs susceptibles d'être recoupés et confrontés pour générer une compréhension nouvelle de l'état du système.
- La proposition d'outils de mesures peut s'accompagner d'un certain nombre de **défis** à surmonter. La **partialité**, les **modalités d'agrégation** ou la **manipulation** en sont quelques exemples.
- L'objectif est de proposer des indicateurs **qui soient utilisés**. En d'autres termes, il est nécessaire que les utilisateurs se les approprient en les reconnaissant comme **légitimes** et **faisant sens** quant à l'objectif de suivi et d'amélioration de la performance sécurité.

Cette phase comprend donc les deux étapes suivantes :

- Diagnostic des pratiques existantes.
- Construction des outils de mesure de performance.

Étape 2.1 : Diagnostic des pratiques existantes

Objectifs

- La première source de connaissance et de bonnes pratiques est l'organisation elle-même. Bien souvent, de manière assez informelle [18], de nombreux acteurs se constituent leurs propres indicateurs pour orienter leurs activités quotidiennes et rationaliser leurs décisions. Explorer, en plus des **pratiques formelles**, les **pratiques informelles** déjà existantes s'agissant des objets de mesure identifiés est donc une première piste de travail.
- Explorer, dans les pratiques existantes, celles qui peuvent constituer un frein à l'appropriation du SIPS. En effet, introduire de nouveaux indicateurs peut entrer **en conflit** avec des pratiques, formelles ou informelles, déjà en place et intégrées dans le mode de travail quotidien de l'organisation. Nous désignerons dans ce qui suit ces pratiques comme des incitations négatives à l'utilisation du SIPS. Celles-ci peuvent être de natures variées. A titre d'exemple, la non prise en compte des performances sécurité dans les évaluations individuelles, et les rétributions financières associées, peut inciter le personnel à mettre de coté le SIPS voire à le manipuler pour qu'il n'entre pas en conflit avec leurs objectifs financiers individuels.

Modalités opérationnelles

La constitution du groupe de travail est déterminante dans cette étape. La connaissance par ses membres des pratiques existantes à différents échelons organisationnels et des attitudes individuelles de leurs collègues constituera la principale source d'information.

Pour que cette information puisse être échangée, discutée et exploitée, deux facteurs clés de succès sont nécessaires :

[18] Dans le cadre des facteurs humains et organisationnels, la notion de « pratiques informelles » peut recouvrir une très large gamme d'attitudes et d'actions. Dans le cas présent, nous parlons de pratiques informelles uniquement pour définir les indicateurs informels utilisés individuellement ou collectivement par le personnel pour se construire une représentation de la situation.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

- ❒ La représentativité dans le groupe de travail de la variété des personnes et des positions hiérarchiques impactées par l'introduction ou modification du SIPS.
- ❒ La liberté de parole permettant aux pratiques informelles d'être partagées au sein du groupe de travail même quand celles-ci entrent en conflit avec les procédures formelles.

Cette étape s'organise comme suit :

1. Identifier collectivement un premier cercle d'**acteurs** concernés par les objets de mesure identifiés.
2. S'assurer que ces personnes ou leurs représentants sont **associés** aux réflexions du groupe de travail. Cela peut s'obtenir à travers d'entretiens ponctuels ou par leur intégration dans le GT.
3. Étudier la **signification** de chaque objet de mesure pour ces personnes et la manière dont elle influence leur travail quotidien.
4. Recenser les **pratiques positives** déjà existantes et les **conflits** que l'introduction du nouvel objet de mesure peut apporter.
5. Discuter, pour chaque objet de mesure, les pratiques positives et la manière de les **valoriser** d'une part, et d'autre part, les possibles incitations négatives existantes et les modalités de leur **dépassement**.

Résultats attendus

Pour chaque objet de mesure, cette étape doit fournir :

- ❒ Un descriptif des **pratiques positives** existantes qu'il serait intéressant de **valoriser**.
- ❒ Un descriptif des **incitations négatives** nécessitant des aménagements organisationnels en préalable à l'introduction du SIPS.

Engagement du top management dans le projet SIPS

Le leadership ou l'engagement du top management sont des marqueurs importants de la volonté de l'organisation au plus haut niveau à placer la sécurité parmi ses préoccupations.

L'étape 2.1 peut nécessiter un appui fort du top management notamment s'il est nécessaire de remettre
en cause des pratiques organisationnelles identifiées comme des incitations négatives au regard du SIPS.

Plusieurs exemples d'actions peuvent être cités : intégrer certains des indicateurs du SIPS dans l'évaluation des performances individuelles, allouer des ressources (notamment du temps) pour nourrir ces indicateurs et les interpréter, définir une politique de sanction équilibrée permettant la remontée d'information...

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

Application

Pour effectuer un état des lieux des pratiques d'indicateurs existantes et des conditions de leur utilisation, des entretiens individuels sont réalisés avec les personnes suivantes :

Personnel du site A

- Au sein du service HSE : responsable HSE, responsable service inspections.
- Au sein du service production : responsable production, personnes rattachées en charge de la maintenance, personne en charge de la planification des achats matières premières.
- Opérateurs dépotage et production.

Personnel du site B

- Responsable service maintenance

Autres personnels : opérateurs sous traitant sur le site.

Il en ressort les éléments suivants quant au fonctionnement quotidien de la sécurité :

- Le service maintenance du site B fonctionne comme une interface entre des clients (les ateliers des sites A et B) et les fournisseurs de services (2 sous traitants avec des contrats annuels). Une réunion d'arbitrage quotidienne est organisée pour recenser les demandes d'intervention remontées par les chefs d'ateliers et définir une première hiérarchisation des priorités d'intervention. Cette hiérarchisation est ensuite discutée avec les sous-traitants au regard de leur disponibilité et du nombre d'heures d'intervention annuel fixé contractuellement. Il en résulte souvent des compromis différents des demandes émises par les chefs d'ateliers.
- Un autre type d'arbitrage est effectué au sein même du site A en vue de déterminer les équipements devant bénéficier de maintenance préventive et ceux gérés par une maintenance curative. Là aussi, l'arbitrage doit prendre en compte la sécurité, les coûts de maintenance et la disponibilité de l'appareil de production.
- Le service dispose d'un logiciel de GMAO recensant l'ensemble des équipements, les modalités de maintenance associées ainsi que les interventions planifiées / réalisées.
- Les barrières techniques identifiées dans l'EDD font l'objet d'un suivi dédié qui recense :
  - L'ensemble des interventions de maintenance.
  - Des compte rendus d'incidents sont réalisés et archivés pour toute panne ou défaut d'activation lors d'une sollicitation.
  - Quand le fonctionnement du système est maintenu même en cas de défaillance d'une barrière, le mode dégradé est enclenché. Une traçabilité du nombre et durée d'occurrence de modes dégradés est effectuée.
- Le service inspection est en charge de la gestion des sous-traitants effectuant les inspections suite à travaux et dans le cadre de la maintenance préventive. Il s'agit donc ici d'évaluer les respects des calendriers de maintenance et la qualité des interventions réalisées.
  Pour ce faire, des inspections durant le chantier et à sa conclusion sont

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

réalisés. De plus, Les 3 personnes du service ont pour objectif de réaliser à minima 2 audits sécurité impromptus par an sur le respect des conditions de sécurité lors des chantiers.

- Le service production tient un relevé détaillé de la disponibilité de l'appareil de production. Plus précisément, les indicateurs suivants sont déjà en place : Nombre d'arrêts programmés et non programmés par réacteur, temps de production réel, catégorie des causes d'arrêt, taux d'arrêt des réacteurs pour maintenance.
- Enfin, les ravitaillements en matières premières se décident en fonction des contraintes de production et de coûts et n'intègrent pas du tout les contraintes sécurité relatives à la surcharge des opérateurs de dépotage (arrivée instantanée de plusieurs camions nécessitant des dépotages simultanés).

Il ressort de ces éléments que deux contraintes fortes pèsent sur les arbitrages sécurité réalisés :

- Le maintien des demandes d'intervention des sous-traitants dans les limites contractuelles définies en début d'année afin d'éviter le dépassement du budget annuel de maintenance.
- Assurer une disponibilité maximale de l'appareil de production en minimisant les arrêts pour maintenance préventive ou curative.

Les intervenants, y compris les opérateurs, ont souligné le caractère ouvert et constructif des échanges sur la sécurité.

Ils donnent pour preuve les éléments suivants :

- Participation des opérateurs à la rédaction et révision des procédures sécurité ;
- Information régulière sur les décisions et actions entreprises suite à la remontée d'événements ou d'incidents ;
- Une approche généralement constructive recherchant à trouver une solution satisfaisante plutôt que d'identifier des coupables ;
- Un très faible turnover des opérateurs et des managers permettant l'instauration d'un certain niveau de confiance ainsi que des équipes de travail expérimentées.

Au regard de ces éléments, le GT s'est accordé sur le fait que la maîtrise ou réduction des coûts de maintenance et la maximisation de la disponibilité de l'appareil de production pouvaient constituer des incitations négatives pour la prise en compte de la sécurité.

Par conséquent, et pour assurer des arbitrages équilibrés entre l'ensemble de ces aspects, il a été décidé de dédier des indicateurs à l'évaluation de la qualité de ces arbitrages au regard de la sécurité.

L'objectif ici est de déceler et stopper d'éventuelles dérives dans le temps qui résulteraient d'une rupture des équilibres entre production et sécurité.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

Étape 2.2 : Construction des outils de mesure de performance

Objectifs

Définir les modalités opérationnelles de mesure de performance des objets retenus en phase 1.

Modalités opérationnelles

Construire un SIPS est la recherche d'un subtil équilibre entre deux contraintes. D'une part, il s'agit de couvrir autant que possible l'**ensemble des facettes** des objets que l'on souhaite mesurer et d'autre part, tenter de **minimiser** le poids de l'indicateur pour l'organisation en termes de **ressources** (temps, information, sollicitation du personnel, difficulté d'interprétation...).

S'agissant de l'objectif de couverture, nous proposons d'étudier pour chaque objet les trois dimensions ou facettes suivantes :

- Les **indicateurs de résultat** permettent d'apprécier le nombre, la qualité et le type de résultats associés à l'objet mesuré. Prenons comme illustration l'objet « processus de retour d'expérience ». L'évaluation des résultats d'un tel processus peut s'effectuer de différentes manières :
  - nombre d'événements ou incidents traités,
  - nombre de recommandations issues du retour d'expérience,
  - pourcentage des recommandations appliquées,
  - nombre de récurrence d'incidents similaires après la finalisation du retour d'expérience...
- Les **indicateurs de fonctionnement** renvoient des informations quant aux modalités de déroulement des différentes étapes composant l'objet. Si nous reprenons l'exemple du retour d'expérience, les indicateurs de fonctionnement suivants peuvent être considérés :
  - nombre d'incidents déclarés par an,
  - pourcentage des incidents déclarés et effectivement traités par le retour d'expérience,
  - variété des données d'entrée [19] ...
- Les **indicateurs d'écosystème** décrivent le caractère plus ou moins favorable du contexte technique et organisationnel composant l'écosystème dans lequel l'objet évolue.

  Le retour d'expérience, aussi rigoureux soit-il, peut souffrir d'un écosystème défavorable, composé par exemple d'une politique de sanction sévère entravant la remontée d'informations ou d'une faible prise en compte des apprentissages remontés par le REX.

  Il est à noter ici que les indicateurs d'écosystème vont souvent pointer des aspects stratégiques de la vie de l'organisation dont les impacts peuvent aller bien au-delà des systèmes considérés, ou même bien au-delà de la sécurité.

  En cela, nous sommes bien en accord avec la vision développée par Reason (1997) où les choix stratégiques sont décrits comme ceux susceptibles d'avoir le plus d'impacts sur la sécurité du système.

[19] Élargir le retour d'expérience à des incidents ayant lieu sur d'autres sites du même groupe ou à des sites semblables mais appartenant à des entreprises différentes contribue à améliorer la qualité du retour d'expérience.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

La seconde contrainte (poids pour l'organisation) doit être considérée à travers les paramètres suivants :

- ❒ Tirer profit autant que possible des indicateurs formels ou informels déjà existants dans l'organisation, quitte à en généraliser l'usage ou à en modifier quelques paramètres.
- ❒ Favoriser des indicateurs simples qui nécessitent peu de ressources pour collecter l'information.
- ❒ Si le nombre d'indicateurs par objet est trop important, le groupe de travail peut décider de sélectionner un sous ensemble d'indicateurs et le faire varier de manière régulière.

L'INERIS propose de prendre en compte ces contraintes selon la démarche suivante :

1. Identifier pour chaque objet de mesure des indicateurs candidats sur la base d'un brainstorming aussi large que possible impliquant a minima les membres du groupe de travail. Les pratiques existantes à l'intérieur ou à l'extérieur de l'organisation, les réflexions individuelles ou les travaux scientifiques sont autant de sources à considérer.
2. Organiser, pour chaque objet, les indicateurs identifiés selon leur type (indicateurs de résultats, de fonctionnement et d'écosystème). Il est recommandé d'équilibrer [20], autant que possible, ces trois catégories ou, a minima, d'avoir un indicateur par catégorie.
3. Décrire chacun de ces indicateurs de manière à apprécier les aspects couverts de ceux qui ne le sont pas. A titre d'exemple, le nombre d'inspections réalisées sur le nombre prévu permet d'apprécier le respect du planning mais pas la qualité des inspections ni la pertinence de la politique maintenance mise en place.
4. Sélectionner, au regard des points forts et faibles de chaque indicateur, la combinaison apportant le meilleur rapport couverture/effort pour l'organisation. Cette combinaison peut être révisée de manière régulière (voir phase 3) et permettre ainsi d'aborder successivement différentes facettes du système à risques.
5. Il peut s'avérer nécessaire de revenir en arrière (phase 1) si un objet de mesure se révèle, après expérience, trop difficile à aborder par des indicateurs. Le groupe de travail doit réactualiser ses choix en fonction de l'évolution de ses connaissances sur les modalités d'évaluation des performances.
6. Valider le SIPS avec le top management. Cela passe par la présentation a minima des éléments suivants :
   - Liste des indicateurs composant le SIPS.
   - Liste des choix méthodologiques effectués et leurs justifications.
   - Aspects de la performance sécurité couverts par le SIPS et ceux qui ne le sont pas.
   - Représentation du coût [21] pour l'organisation en termes de temps de travail et investissements.

Les échanges avec le top management peuvent mener à réviser le SIPS ou même à revenir sur certaines orientations adoptées lors des étapes antérieures.

[20] S'agissant des indicateurs de l'écosystème, il est raisonnable d'espérer identifier des éléments communs pour différents objets. A titre d'exemple, l'engagement du top management pour le respect de l'équilibre sécurité/production ou une culture de sécurité adaptée peuvent être des paramètres récurrents dans la constitution d'écosystèmes favorables à différents indicateurs.

[21] Il ne s'agit pas nécessairement d'un coût monétaire. Il s'agit plutôt d'apprécier, qualitativement ou quantitativement, la consommation de ressources nécessitée par l'utilisation du SIPS.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

La carte d'identité d'un indicateur.

Il ne suffit pas de nommer un indicateur ou d'en écrire la formule pour le décrire. En effet, décrire un indicateur nécessite d'aborder des aspects complémentaires : ses limites, ses modalités d'interprétation, la fréquence à laquelle il doit être mesuré, les modalités de sa réactualisation dans le SIPS... Ces dimensions sont à considérer pour évaluer la pertinence d'un indicateur au regard des contraintes de couverture et de poids pour l'organisation.

Suivant les travaux de Mazri et al (2012) pour décrire les éléments constitutifs de la carte d'identité d'un indicateur, quatre rubriques sont à documenter (voir ***Tableau 5*** ci-après) : informations générales, informations techniques, informations organisationnelles et système d'information.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

Informations générales	
Nom	Un nom et une codification uniques doivent être donnés à chaque indicateur pour éviter les confusions.
Description et objectifs	Décrire ce que l'indicateur couvre et ce qu'il ne couvre pas au regard de l'objet considéré (apports et limites).
Source	Pratique existante en interne, brainstorming, bonnes pratiques sectorielles, références bibliographiques.
Informations techniques	
Formule et unité	Un indicateur peut être qualitatif, semi quantitatif ou quantitatif. Dans les deux premiers cas, nous parlerons de modalités d'agrégation des paramètres. Dans le dernier cas, il s'agit de décrire la formule de calcul ainsi que l'unité associée.
Valeurs Min, Max et cible.	Que l'échelle choisie soit qualitative ou quantitative, il est important de la caractériser (valeur minimale possible, valeur maximale possible) ainsi que la valeur ou l'intervalle cible représentatif d'une performance satisfaisante.
Fréquence de mesure	A quel intervalle de temps faut-il effectuer les mesures ?
Indicateurs associés	La valeur d'un indicateur ne doit pas être analysée seule mais dans un réseau (système) d'indicateurs. Il s'agit donc d'identifier ici la liste des indicateurs dont les valeurs doivent être croisées avec celui-ci.
Informations organisationnelles	
Gestionnaire de l'indicateur	Personne référence en charge de la gestion au jour le jour de l'indicateur.
Sources des données d'entrée	Description des sources (système d'information ou personnes) fournissant les données d'entrée pour le calcul de la valeur de l'indicateur.
Modalités d'interprétation	Identifier les personnes ayant les connaissances nécessaires à l'interprétation de l'indicateur et fournir, si possible, des orientations quant aux modalités de cette interprétation.
Modalités de communication	Définir les personnes en interne et en externe ayant accès aux valeurs de l'indicateur. Distinguer plus particulièrement celles appelées à prendre des décisions sur leur base.
Modalités de révision (réactualisation)	Les évolutions de l'organisation pouvant rendre un indicateur caduque, des modalités de réactualisation de chaque indicateur doivent être définies.
Système d'information	
Disponibilité d'outils opérationnels	Lister les outils opérationnels, s'ils existent, permettant de simplifier le recueil des données, le calcul et la communication de l'indicateur.
Niveau d'adéquation avec le système d'information	Évaluer la compatibilité de l'indicateur (notamment de ses données d'entrées) avec les données déjà mises à disposition par le système d'information.

Tableau 5 : Carte d'identité d'un Indicateur de Performance Sécurité.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

Résultats attendus

Un système d'indicateurs de performance sécurité adapté conciliant objets de mesure pointés par le modèle de sécurité et contraintes spécifiques de l'organisation.

Application

Le brainstorming au sein du groupe de travail a permis de définir les besoins suivants en termes d'indicateurs et les objectifs qui leur sont associés :

❒ Indicateurs de résultats

Le SIPS doit permettre d'évaluer les résultats des choix faits en termes de politique de maintenance. Ces résultats s'évaluent selon les éléments suivants :

- Évaluation de la disponibilité de l'appareil de production. Cela prend en compte les arrêts dus à des pannes (curatif) ou à des interventions planifiées (préventif).
- Disponibilité des barrières de sécurité et minimisation des modes dégradés.
- Intégrité mécanique de l'ensemble du système manipulant l'isobutylène.

❒ Indicateurs de fonctionnement

Le SIPS doit permettre d'observer les éléments suivants:

- Les arbitrages décrits précédemment sont au cœur de la gestion quotidienne de la sécurité, que ce soit au sein du site A à travers les équilibres adoptés entre maintenance préventive et curative ou au sein du site B à l'interface entre les demandes des chefs d'ateliers et les disponibilités des sous-traitants. Le GT souhaite développer des **capacités de suivi des tendances** adoptées lors de ces arbitrages et d'en évaluer les effets sur la sécurité.
- Évaluer **en continu** la **qualité des interventions** réalisées par les sous-traitants ainsi que le respect des référentiels sécurité internes lors de ces interventions.
- Suivre **en continu** l'évolution de la **charge de travail** des opérateurs dépotage et s'assurer qu'elle ne va pas à l'encontre de la sécurité.

❒ Indicateurs d'écosystème

Deux aspects ont été considérés d'importance quant aux conditions organisationnelles permettant aux activités du système [22] de se dérouler dans des conditions satisfaisantes.

La première demeure le **montant des ressources rendues disponibles** pour la maintenance. Les ressources considérées ici prennent aussi bien en compte le nombre total d'heures d'intervention défini dans les contrats de sous-traitance que les budgets internes permettant de mettre en place une politique de maintenance plus favorable au préventif qu'au curatif.

La seconde est l'importance de garder un **dialogue ouvert et constructif** entre l'ensemble des acteurs décrits précédemment. Pour cela, il a été convenu que le maintien d'une politique de sanction équilibrée basée sur la recherche de solutions constructives et non pas de coupables était garante d'un dialogue constructif et d'une remontée d'informations fiable.

Le ***Tableau 6*** présente les indicateurs proposés pour chacune de ces trois catégories de besoins.

[22] Les facteurs d'écosystème vont bien évidemment avoir des impacts allant bien au-delà de ce système puisqu'ils remontent à des choix faits au niveau stratégique de l'organisation. Ces choix sont donc, par définition, impactant pour de nombreuses dimensions de la vie de l'organisation.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

Catégories d'indicateurs de performance sécurité	Besoins et objectifs de la mesure	Indicateurs proposés et leurs descriptions
Indicateurs de résultats	Disponibilité de l'appareil de production	**Taux moyen de disponibilité opérationnelle des équipements (DOM)** Moyenne (DOM) des disponibilités opérationnelles individuelles (Doi) des références en GMAO. $Do_i = \frac{MTBF}{MTBF+MTTR}$ ■ MTBF : Temps moyen de fonctionnement entre les pannes. ■ MTTR : Temps moyen jusqu'à réparation. Au-delà de la disponibilité des réacteurs suivie par la production, cet indicateur vise à évaluer la disponibilité de l'ensemble des références considérées dans la GMAO.
	Disponibilité des barrières de sécurité	**Taux moyen de disponibilité opérationnelle des barrières de sécurité considérées (DO_{MB})** Il s'agit d'un zoom de l'indicateur ci-dessus sur les barrières de sécurité qui se justifie par l'attention particulière portée sur ces équipements au regard de leur importance pour la sécurité.
	Intégrité mécanique	**Nombre de pertes de confinements** Proposé par le CCPS sous la dénomination PSI (Process Safety Incidents), cet indicateur mesure le nombre et la gravité des incidents associés à des pertes de confinement. Les modalités de calcul sont précisées en ***fiche 6***
Indicateurs de fonctionnement	Caractère favorable des arbitrages maintenance effectués quotidiennement	**Conflits de ressources maintenance 1 (CRM_1)** Cumul des dépassements des délais d'intervention demandés par les chefs d'ateliers. $CRM_1 = \sum_N DI_F - DI_D$ ■ DI_F : Date d'intervention finalisée. ■ DI_D : Date d'intervention demandée. ■ N : Ensemble des demandes d'intervention émises par les chefs d'ateliers sur une période donnée. Cette mesure permet d'apprécier les décalages entre les échéances d'intervention demandées par les chefs d'ateliers et les délais effectifs déterminés par la disponibilité des ressources.
		Conflits de ressources maintenance 2 (CRM2) Equilibre préventif/curatif $CRM_2 = \frac{NH_P}{NH_T}$ ■ NH_P : Nombre d'heures d'intervention maintenance consacrées au préventif ■ NH_T : Nombre d'heures d'intervention maintenance total. Cette mesure permet de refléter un état des lieux global des équilibres en place entre préventif et curatif dans la politique de maintenance.
		Conflits de ressources maintenance 3 (CRM3) Équilibre préventif/curatif $CRM_3 = \frac{DP_A}{DP_T}$ ■ DPA: Demandes de Passage du curatif au préventif Acceptées par la direction lors des arbitrages budgétaires annuels. ■ DPT : Total des Demandes de Passage du curatif au préventif émises par le service maintenance. Cette mesure est complémentaire de CRM2 dans la mesure où elle reflète les efforts consentis par la direction pour favoriser le développement du préventif sur le curatif.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

Indicateurs de fonctionnement	Qualité des interventions réalisées par les sous-traitants	**Performance des sous-traitants 1 (PST1)** $PST_1 = \frac{NA_S}{NA_T}$ ■ NAS : Nombre d'audits sécurité de chantiers réalisés et satisfaisants. ■ NAT : Nombre total d'audits sécurité de chantiers réalisés. Ces audits sont déjà en place au sein du site et réalisés par le service inspections. Ils peuvent intervenir aussi bien durant le chantier pour évaluer les conditions opérationnelles et le respect des procédures préalables au lancement du chantier (Plan de prévention, permis de travail...) qu'à la conclusion du chantier (qualité des travaux réalisés, conditions de clôture de chantier...)
		Performance des sous-traitants 2 (PST2) $PST_2 = \frac{NA_T}{NA_P}$ ■ NA_P : Nombre d'audits prévus par la planification annuelle. Cet indicateur est complémentaire du PST_1. En effet, le PST_1 n'a de sens que si l'on dispose d'un nombre d'audits représentatif et aussi conforme que possible au planning d'audits défini.
	Charge de travail des opérateurs dépotage	**Charge de Travail opérateurs de dépotage (CT) CT= (μ, σ)** Tel que : ■ μ : Moyenne du nombre quotidien de camions nécessitant une opération de dépotage. ■ σ : Écart-type du nombre quotidien de camions nécessitant une opération de dépotage. Cette mesure englobe l'ensemble des opérations de dépotage et pas seulement celles relatives à l'Isobutylène afin de développer une vision de la charge de travail globale des opérateurs dépotage. Cette mesure présente les avantages suivants : ■ Donnée disponible facilement (recensement des camions au centre d'accueil du site) ■ La moyenne permet d'apprécier si la charge globale sur une période donnée est au dessus des ressources disponibles (nécessité de personnel supplémentaire). ■ L'écart type permet d'identifier les éventuels pics d'activité qu'il s'agit de réguler soit au travers d'une meilleure planification des ravitaillements (service achat) ou en prévoyant des ressources supplémentaires ponctuelles.
Indicateur d'écosystème	Évolution du budget annuel maintenance	**Budget Maintenance (BM)** **Budget maintenance annuel sur l'ensemble du site** La sécurité du système étudié étant fortement conditionnée par la maîtrise de son intégrité mécanique, les évolutions du budget maintenance de l'ensemble du site, notamment au regard d'éventuelles baisse ou augmentation de l'activité, doivent être observés car un grand nombre des indicateur de fonctionnement et de résultats décrits ci-dessus en sont dépendants.
	Politique de sanction de l'organisation	**Évaluation de la politique sanction par les salariés (PS)** Un questionnaire est distribué annuellement aux salariés afin de recueillir leurs perceptions, de manière anonyme et qualitative, sur de nombreux aspects de la vie de l'organisation, y compris la sécurité. La perception de la politique de sanction y est abordée. Il a aussi été évoqué la possibilité d'effectuer des évaluations de cette dimension d'importance pour de nombreux autres aspects de la sécurité au travers de diagnostics organisationnels.

Tableau 6 : Exemples d'indicateurs proposés pour chacun des objets identifiés

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

Les indicateurs proposés ci-avant appellent les remarques suivantes :

- Les **métriques** décrites ci-dessus sont les résultats d'arbitrages entre leur capacité à représenter fidèlement le besoin de mesure exprimé d'une part et l'accessibilité des données nécessaires à son calcul.

  Dans certains cas, des indicateurs plus précis n'ont pas été validés car nécessitant des informations non disponibles en l'état actuel du système d'information de l'organisation. Ils gardent néanmoins le statut d'indicateurs candidats dont l'opportunité d'utilisation sera réévaluée par le GT en cas d'évolution du système d'information.

- Une analyse des **biais et limites** de chaque indicateur a été fournie aux décideurs. A titre d'exemple, l'indicateur CRM3 basé sur le nombre de demandes de passage de curatif en préventif validés par la direction peut faire l'objet de manipulation en ne remontant officiellement que les demandes susceptibles d'être acceptées.

  Nous reconnaissons volontiers qu'aucun système d'indicateurs n'est complètement fiable ou non manipulable. Néanmoins, le système proposé ci-dessus présente à notre sens une fiabilité plus importante en permettant de **recouper** des indicateurs de fonctionnement, de résultats et d'écosystème qui offrent des **éclairages différents** sur le système.

  Si un éclairage seul peut facilement faillir, une faillite simultanée des trois éclairages est moins probable. Ainsi, une manipulation de l'indicateur CRM3 pourrait être compensée par l'augmentation des ressources sur le curatif au détriment du préventif (CRM2) ou par une détérioration de l'évaluation annuelle de la politique sécurité par les salariés (indicateur PS).

- Individuellement, chaque indicateur ci-dessus ne fournit qu'une information très partielle de la réalité du système. A ce titre, Il ne peut être considéré comme représentatif de la complexité des mécanismes qui façonnent la performance quotidienne en sécurité. Néanmoins, leur **analyse croisée** peut constituer un moyen d'investigation et d'amélioration de la compréhension des forces et faiblesses du système.

  A titre d'exemple, une baisse du taux moyen de disponibilité des équipements (DOM) peut questionner de nombreux aspects de la maintenance :

  - est-ce du fait de la *faiblesse des ressources* ?
  - est-ce une simple *variation statistique non significative* ?
  - est-ce en raison d'un *mauvais équilibre préventif/curatif* ?
  - est-ce en raison d'*inspections et d'interventions de mauvaise qualité* ?

  Le croisement de cet indicateur de résultats avec les informations remontées par les indicateurs de fonctionnement est de nature à orienter les investigations pour déceler les aspects du système derrière cette baisse et déclencher les **actions adaptées** si le diagnostic est clair ou déployer des outils plus approfondis et plus ponctuels (audit, diagnostic) si jamais cela s'avère nécessaire.

Les indicateurs proposés doivent donc être déployés de manière coordonnée afin de constituer un système de mesure couvrant les différents aspects de la vie du système.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

Étape 2.3 : Modalités d'utilisation du SIPS

Objectifs

L'organisation doit s'assurer que le SIPS s'ancre dans une approche de pilotage basée sur un cycle continu de diagnostic et d'apprentissage plutôt que sur une comparaison des performances avec une norme prédéfinie (voir ***fiche 3***).

Modalités opérationnelles

Cette étape s'adresse essentiellement aux décideurs dans l'organisation intéressés par le SIPS pour définir des priorités et prendre des décisions.

Nous proposons d'organiser cette étape selon les modalités suivantes :

1. La carte d'identité proposée précédemment (voir ***encadré p41***) définit les **modalités de communication associées** à un indicateur et identifie les **acteurs intéressés** par la prise de décision sur la base des valeurs fournies. Ce sont ces acteurs qui doivent être consultés lors de cette phase.
2. Dans le meilleur des cas, ces acteurs ont pris connaissance des évolutions du projet SIPS et ont fait part de leurs besoins en termes d'appui à la prise de décision soit à travers leurs représentants dans le groupe de travail ou au travers les entretiens menés en étape 2.1.

   Si cela n'a pas été le cas ou ne l'a été que partiellement, un séminaire de travail peut être envisagé afin de présenter le SIPS et discuter des modalités de leur utilisation au quotidien.
3. Détailler avec les décideurs les **modalités de diagnostic et d'interprétation** possibles des indicateurs proposés. A ce niveau, il est important d'insister sur les aspects suivants :
   - Modalités de **croisement** des indicateurs et significations associées. Un travail sur des cas pratiques est conseillé.
   - Présentation des limites du SIPS et de ses complémentarités avec d'autres outils d'évaluation des performances tels que les audits et les diagnostics organisationnels.
   - Possibilité de **partager leurs expériences** et difficultés personnelles quant à l'utilisation du SIPS dans le cadre du groupe de travail.

Résultats attendus

- A minima, la **compréhension** par les décideurs concernés des modalités d'utilisation du SIPS.
- Au mieux, gagner l'**adhésion** des décideurs et la reconnaissance de l'intérêt du SIPS pour améliorer leur gestion quotidienne de la sécurité.
- améliorer leur **gestion quotidienne** de la sécurité.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Aspects techniques de la méthode : déroulé des phases

Ce qu'il faut retenir de la phase 2

- La phase 2 vise à construire un SIPS adapté à la liste d'objets définie par la phase 1. Pour cela, elle doit prendre en compte deux contraintes principales que sont la **couverture des différentes dimensions des objets de mesure** et la **minimisation du coût du SIPS** pour l'organisation.
- Le terme « conception du SIPS » est employé en lieu et place d'identification ou de définition car il s'agit d'une **construction intellectuelle** et non pas d'une sélection parmi un ensemble d'indicateurs standards déjà prédéfinis.
- Le groupe de travail doit **diversifier ses sources d'inspiration** lors de la construction du SIPS. Les pratiques **formelles** ou **informelles** déjà en cours au sein de l'organisation, les pratiques développées par d'autres organisations ou les recommandations fournies par la littérature scientifiques sont des sources à considérer.
- Le groupe de travail doit veiller à **équilibrer le type d'indicateurs** construits pour chaque objet. C'est la combinaison d'indicateurs de chacune des trois catégories (résultats, fonctionnement et écosystème) qui permettra des croisements et interprétations d'intérêt pour l'organisation.

La méthode SIPS (Système d'Indicateurs Performance Sécurité)

Conclusion

Conclusions générales et perspectives

La littérature des indicateurs sécurité embrasse aujourd'hui l'ensemble des technologies à risques et représente une gamme d'outils largement utilisée par les managers sécurité. A ce titre, il ne s'agit plus de s'interroger sur leur pertinence mais plutôt sur les modalités de leur utilisation.

Ces modalités doivent, d'une part, éviter d'enfermer la sécurité dans des chiffres qui n'en sont qu'une caricature et, d'autre part, attirer l'attention des managers sur les vrais problèmes quand ceux-ci se cachent dans les méandres de l'organisation et du flot quotidien des informations.

Face à ces objectifs ambitieux, le présent guide est une première pierre qui propose de poser les bases techniques et organisationnelles d'une méthode pour l'identification/conception d'indicateurs performance sécurité. Il permet d'approfondir les notions de sécurité, d'indicateur et de performance.

Il permet aussi d'organiser la démarche intellectuelle d'exploration de ces concepts à la recherche des indicateurs les plus adaptés au modèle et visions de la sécurité propres à chaque organisation.

Les éléments organisationnels discutés ont permis de préciser le cahier des charges et modalités opérationnelles du groupe de travail en charge d'identifier, implémenter et réviser les indicateurs. Nous avons ainsi pu mettre en lumière que l'intérêt des indicateurs ne réside pas uniquement dans les **informations** qu'ils remontent, mais aussi dans les **échanges** et **discussions** qu'ils créent au sein de l'organisation. Ces échanges créent l'espace critique permettant à l'organisation de sans cesse se renouveler face à des vulnérabilités toujours mouvantes.

Cette première pierre est appelée à être complétée dans l'avenir, notamment sur les aspects suivants :

- Offrir aux lecteurs une large variété de **cas pratiques** plus représentative de la diversité des modèles et pratiques sécurité au sein des industries à risques.
- Aller plus loin dans l'**accompagnement** des utilisateurs dans la construction et justification des arbitrages qui, tels que décrits au long de ce guide, vont de pair avec le déploiement de ce types de méthodes.
- Développer une meilleure **articulation** entre les indicateurs et autres outils d'évaluation des performances tels que les diagnostics ou audits avec l'objectif de fournir aux managers des représentations de plus en plus pertinentes de leurs systèmes à niveau de ressources constant.

Cependant, il est important de noter que le développement des indicateurs et la réalisation des promesses qui leur sont associées ne peut être dissocié du développement des systèmes d'information au service de la sécurité.

En effet, si la qualité ou la logistique sont des domaines qui ont largement profité des développements des nouvelles technologies d'information et de communication (NTIC), la sécurité semble encore en recul à ce niveau.

Or, la complexité et la richesse des mécanismes constitutifs de la sécurité impliquent des informations toujours plus détaillées et recoupées pour attirer l'attention des managers sur les vraies questions et éviter ainsi d'apporter les bonnes réponses aux mauvais problèmes.

Bibliographie

Bibliographie

Amalberti, R. (2012). *Piloter la sécurité*. Springer Verlag France.

Ansoff, H. I. (1975). *Managing strategic surprise by response to weak signals.* California management review XVIII(2), 21-33.

API. (2010). ANSI/API *recommended practices 754: Process safety indicators for the refining and the Petrochemical industry. First edition. USA :* American petroleum Institute.

API. (2010). *Process Safety performance indicators for the refining and petrochemical industries. ANSI/API recommended practice 754.* Washington : API publishing services.

Baker panel. (2007). *The report of the BP US refineries independent safety review panel.*

BARPI. (2006). *Explosion de la poudrerie de Grenelle*. Fiche ARIA 5692. Paris.

Boussard, V. (2001). *Quand les règles s'incarnent. L'exemple des indicateurs pregnants.* Sociologie du travail (43) , 533-551.

BP. (2010). *Deepwater Horizon accident investigation report.*

Cambon, J. (2007). *Vers une nouvelle méthodologie de mesure de la performance des systèmes de management de la santé-sécurité au travail.* Thèse de doctorat de l'Ecole Natonale Supérieure des Mines de Paris.

CCPS. (2007). *Center for Chemical Process Sfaety.* Guidelines for Risk Based process Safety. John Wiley.

CCPS. (2010). *Guidelines for Process Safety Metrics.* New Jersey: Willey.

CCPS. (2011). *Guidelines for process safety metrics.*

CEFIC. (2011). *Guidance on process safety performance indicators.*

Cooper, M. D. (2000). *Towards a model of safety culture.* Safety science 36 , 111-136.

CSB. (2007). *BP Texas city final investigation report.*

Delatour, G., Laclemence, P., Calcei, D., & Mazri, C. (2014). *Systèmes de gestion de la sécurité. Quel espace critique pour la décision d'anticipation?* IMDR. Dijon.

DHSG. (2011). *Final report on the investoigation of the Macondo Well Blowout.*

Eckerson, W. (2011). *Performance dashboards. Measuring, monitoring, and managing your business.* Second edition. New jersey : John Wiley and Sons.

EPRI. (2000). *Guidelines for trial use of leading indicators of human performance.* Interim report. Palo alto.

EPSC. (2011). *Process safety leading and lagging metrics.*

EPSC. (1996). *Safety performance measurement.* IchemE.

Bibliographie

Gadd, S., & Collins, A. M. (2002). *Safety culture :* A review of the literature. HSL/2002/25.

Grote, G. (2012). *Safety management in different high-risk domains : All the same?* Safety science (50) , 1983-1992.

Guldenmund, F. W. (2000). *The nature of safety culture :* a review of theory and research. Safety science (34) , 215-257.

Hale, A. R., Heming, B. H., Carthey, J., & Kirwan, B. (1997). *Modelling of safety management systems.* Safety science 26(1) , 121-140.

Hatchuel, A. (2000). *Quel horizon pour les sciences de gestion? Vers une théorie de l'action collective.* Dans A. David, A. Hatchuel, & R. Laufer, Les nouvelles fondations des sciences de gestion (pp. 7-43). Paris : Editions Vuibert.

Heinrich, H. W. (1950). *Industrial accident prevention :* A scientific approach. 3rd edition. new York: McGraw Hill.

Hollnagel, E. (2006). *Achieving system safety by resilience engineering.* Conference on system safety. London.

Hollnagel, E. (2004). *Barriers and accident prevention.* Burlington : Ashgate.

Hollnagel, E. (2008). *Safety management - Looking back or looking forward.* Dans E. Hollnagel, C. P. Nemeth, & S. Dekker, Resilience engineering perspectives. Volume 1 (pp. 63-78). Aldershot : Ashgate.

Hopkins, A. (2012). *Safety indicators for offshore drilling.* A working paper for the CSB inquiry into the Macondo blowout.

Hovden, J. Albrechtsen, E., & Herrera, I. A. (2010). *Is there a need for new theories, models and approaches to occupational accident prevention.* Safety science (48) , 950-956.

HSE. (2006). *Developing process safety indicators.* A step by step guide for chemical and major hazard industries. HSE Books.

HSE. (2010). *Reports and recommendations arising from the competent authority's response to the Buncefield incident.*

Hudson, P. T., Reason, J., Wagenaar, W. A., bentley, P. D., Primrose, M., & Visser, J. (1994). Tripod-Delta: *proactive approach to enhanced safety*. Journal of Petroleum technology 46(1) , 58-62.

ICAO. (2006). Safety management manual.

IRGC. (2010). *The emergence of risks.* Contributing factors. Genève.

ISO. (2005). Norme ISO 9000. *Systèmes de management de la qualité* - Principes essentiels et vocabulaire. Genève: ISO.

Kaplan, R. S., & Norton, D. P. (2007). *Using the balanced scorecard as a strategic management system.* Harvard Business review , 1-14.

Kaplan, R., & Norton, D. (1996). *The balanced scorecard: Translating strategy into action.* Harvard business school press.

Bibliographie

Kjellen, J. (2009). *The safety measurement problem revisited.* Safety science (47) , 486-489.

Le Coze, J. C. (2013b). *Outlines of a sensitising model for industrial safety assessment.* Safety science (51) , 187-201.

Leveson, N. G. (2011). *Engineering a safer world. Systems thinking applied to safety.* London: The MIT Press.

Lorino, P. (1995). Comptes et récits de la performance. Paris : Editions d'Organisation.

Mazri, C., Jovanovic, A., & Balos, D. (2012). *Descriptive model of indicators for Environment, health and Safety management .* Chemical Engineering transactions (26) .

Mearns, K., Whitaker, S. M., & Flin, R. (2003). *Safety climate, safety management practice and safety performance in management environments.* Safety science (41) , 641-680.

Mitrof, I. I., Pauchant, T., Finney, M., & Pearson, C. (1989). *Do (some) organizations cause their own crises ? The cultural profile of crisis-prone vs crisis-prepared organizations.* Industrial crisis Quarterly (3), 269-283.

OCDE. (2008). *Guidance on performance safety indicators related to chemical accident prevention*, preparedeness and response for industry (2nd edition). Paris.

OGP. (2011). *Process safety. Recommended practices on key performance indicators.* Rapport N°456.

Oien, K. (2001). *Risk indicators as a tool for risk control.* Reliability engineering and system safety 74 (2) , 129-145.

Oien, K., Massaiu, S., & Tinmannsvik, R. K. (2012). *Guidelines for implementing* the REWI method.

OSHA. (2000). *Process safety management* (OSHA 3132).

Perrow, C. (1984). *Normal accidents.* New York : Basic books.

Phimister, J, Bier, V. M., & Kunreuther, H. C. (2001). *Accident precursors analysis and management.* Washington DC : The National Academies Press.

Rasmussen, J. (1997). *Risk management in a dynamic society :* A modelling problem. Safety science 27 (2/3) , 183-213.

Rasmussen, J., & Svedung, S. (2000). P*roactive risk management in dynamic society. Karlstad:* Swedish rescue services agency.
Reason, J. (1990). *Human error.* Cambridge UNiversity Press.

Reason, J. (1993). *Managing the management risk : New appraoches to organisational safety.* Dans B. Wilpert, & T. Qvale, Reliability and safety in hazardous work systems. (pp. 3-23). Hove: LEA.

Reason, J. (1997). *Managing the risks of organisational accidents.* Burlington : Ashgate.

Bibliographie

Romalaer, P. (2011). Organisation : *panorama d'une méthode de diagnostic.* Paris: Document de travail. Université paris Dauphine.

RSSB. (2011). *measuring safety performance.*

Segrestin, D. (2004). *les chantiers du manager.* Paris : Armand Colin.

Storseth, F., Tnimannsvik, R. K., & Oien, K. (2009). Building safety by resilient organisation- *A case specific approach.* European Safety and Reliability Association Annual Conference. Prague.

Turner, B. (1976). *The organizational and Interorganizational development of disasters.* Administrative science quarterly 21(3) , 378-397.

Vaughan, D. (1997). *The challenger launch decision :* Risky technology, culture and deviance at NASA. Chicago: University of Chicago press.

Vinnem, J. E. (2003). *Operational safety of FPSO shutter tank collision risk summary report.* NTNU, Norway : Research report 113.

Weick, K. E. (1987). *Organizational culture as a source of High reliability.* California Management Review (29) , 112-127.

Weick, K., Sutcliffe, K., & Obstfeld, D. (1999). *Organizing for reliability : processes of collective mindfulness.* research in organizational behavior, 81-123.

Weinberg, G. (1975). *An introduction to general systems thinking.* New york : John Wiley.

Woltjer, R., & Hollnagel, E. (2007). *The Alaska Airlines flight 261 accident : A systemic analysis of functional resonance.* Proceedings of the 2007 International symposium on aviation psychology, (pp. 763-768). Dayton.

Fiches d'approfondissement

Fiche 1

Complexité des systèmes sociotechniques à risques

Complexité des systèmes sociotechniques à risques

L'analyse approfondie des mécanismes sous jacents aux accidents majeurs met systématiquement en évidence l'implication et l'interaction de facteurs d'origines diverses (Reason, 1993) ; (Weick, Sutcliffe, & Obstfeld, 1999) ; (Rasmussen & Svedung) :

- Techniques : machines, logiciels, procédés.
- Humains : interactions homme-machine et collectifs de travail.
- Organisationnels : interactions entre acteurs dans le cadre de systèmes de règles formelles ou informelles régissant le fonctionnement du système. Celles-ci peuvent résulter de contraintes réglementaires ou de choix effectués par les acteurs eux même.

De Grenelle (1794) à Macondo (2010)

L'histoire des accidents majeurs est riche en illustrations de la multiplicité et de l'imbrication de facteurs techniques, humains, organisationnels et réglementaires sous jacents aux séquences accidentelles.
L'explosion de la poudrière de Grenelle en 1794 a suivi une évolution du processus de broyage des ingrédients visant à améliorer la productivité. En l'absence d'analyse de risques de ce nouveau procédé et la non prise en compte des multiples alertes lancées par le responsable production, l'accident eut lieu (BARPI, 2006).

Près de deux siècles plus tard, la catastrophe de Bhopal (1984) révèle la multiplicité des défaillances à toutes les échelles du site : Faible niveau de formation du personnel, autorités d'inspection absentes (15 inspecteurs pour 8000 sites), modifications de procédures sans évaluation de leurs impacts sur la sécurité, fiabilité des appareils en deçà des normes de conception ainsi que la désactivation de certaines barrières de sécurité. Enfin, la catastrophe de Macondo (2010) a elle aussi pointé la concomitance d'une multitude de facteurs : Désactivation de barrières de sécurité, faible retour d'expérience alors que plusieurs remontées d'hydrocarbures avaient été constatées les jours précédant l'accident, absence d'indicateurs sécurité adaptés aux activités de forage (Hopkins, 2012), non identification de la séquence accidentelle ayant abouti à la catastrophe, mauvaise interprétation des résultats des tests par les opérateurs de forage ainsi que de nombreuses difficultés de communication entre les trois opérateurs présents sur la plateforme (BP, Halliburton et Transocean) (BP, 2010) (DHSG, 2011).

Cette constatation a depuis longtemps fondé de nombreux développements théoriques relatifs à la gestion de la sécurité. Ainsi, pour dépasser la focalisation sur les défaillances techniques ou humaines, les systèmes à risques sont décrits comme sociotechniques (Rasmussen, 1997) pour refléter la multiplicité et la diversité des mécanismes participants à l'occurrence accidentelle.

Cet enrichissement de la compréhension des mécanismes de la sécurité a aussi permis de mettre le doigt sur l'existence de multiples signes annonciateurs d'un accident. Plusieurs terminologies désignent ces signes : signaux faibles (Ansoff, 1975), incidents, presque accidents, précurseurs (Phimister, Bier, & Kunreuther, 2001), conditions latentes (Reason, 1997) ou messages de lanceurs d'alerte.

Fiche 1

Complexité des systèmes sociotechniques à risques

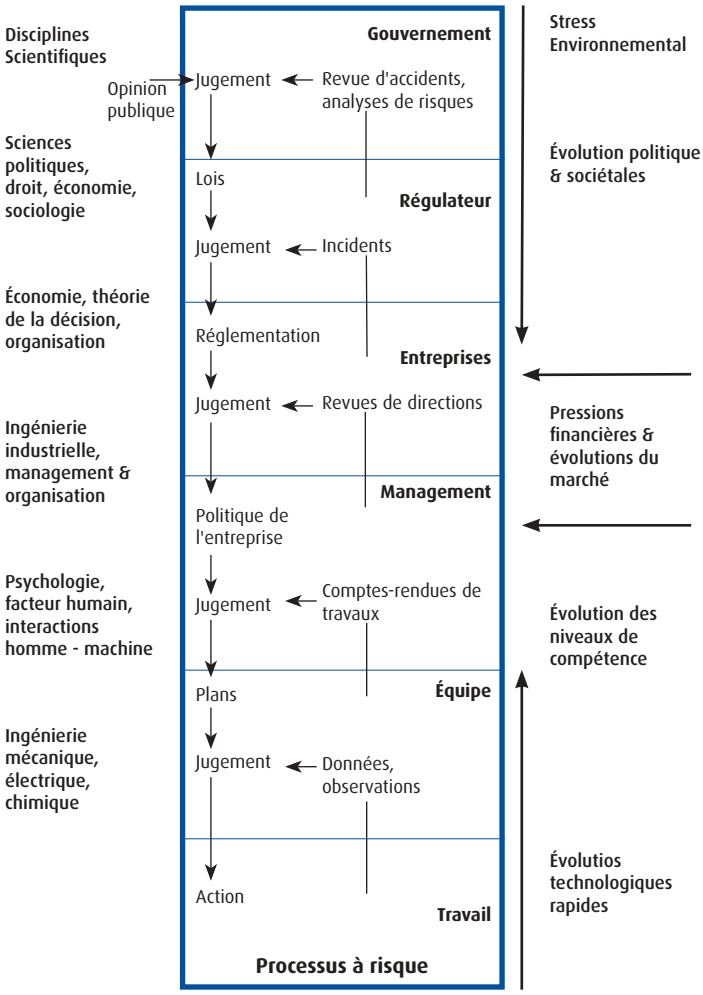


Figure 6 Système sociotechnique selon Rasmussen et Svedung (2000)

Si ces événements peuvent a posteriori être relativement facilement reliés à la séquence accidentelle, il en est tout autre en amont de l'accident pour les raisons suivantes :

- Les mécanismes socio techniques peuvent être **nombreux**, **interdépendants** et **transverses** à de nombreux niveaux organisationnels. De ce fait, il devient rapidement difficile de les tracer et d'exercer un contrôle dessus. A titre d'exemple, le modèle des interactions socio techniques de Rasmussen & Svedung (2000) décrit l'imbrication de multiples niveaux décisionnels allant de l'opérateur jusqu'aux orientations réglementaires définies au niveau national.
- Le **développement des systèmes d'information** au sein des entreprises peut entraîner une surcharge d'information dépassant les capacités d'interprétation et d'analyse des décideurs. Noyés dans cette masse d'information, ces signes ne sont pas détectés par les bonnes personnes ou celles-ci les interprètent mal.
- Les **signes précurseurs** sont souvent désignés comme **faibles** car leur résonnance au sein de l'organisation est réduite, leurs développements incertains et leurs interprétations ambigües [23] . Ainsi, même détectés, ces signes précurseurs constituent souvent une assise décisionnelle faible au regard des résistances au changement et de l'inertie que les organisations peuvent expérimenter.

  De nombreux travaux (Rasmussen, 1997) (Vaughan, 1997) ont démontré que les organisations peuvent **s'accommoder** de ces signaux et les intègrent dans la « normalité » de la vie organisationnelle, créant ainsi une lente mais irrévocable érosion vers de nouvelles formes de vulnérabilités.

[23] Pour plus de détails, voir Rossel (2009)

Fiche 1

Complexité des systèmes sociotechniques à risques

Bibliographie

Ansoff, H. I. (1975). *Managing strategic surprise by response to weak signals.* California management review XVIII(2) , 21-33.

BARPI. (2006). *Explosion de la poudrerie de Grenelle.* Fiche ARIA 5692. Paris.

BP. (2010). *Deepwater Horizon accident investigation report.*

DHSG. (2011). *Final report on the investoigation* of the Macondo Well Blowout.

Hopkins, A. (2012). *Safety indicators for offshore drilling.* A working paper for the CSB inquiry into the Macondo blowout.

Phimister, J., Bier, V. M., & Kunreuther, H. C. (2001). *Accident precursors analysis and management.* Washington DC: The National Academies Press.

Rasmussen, J. (1997). *Risk management in a dynamic society: A modelling problem.* Safety science 27 (2/3) , 183-213.

Rasmussen, J., & Svedung, S. (2000). Proactive risk management in dynamic society. Karlstad: Swedish rescue services agency.

Reason, J. (1993). *Managing the management risk*: New appraoches to organisational safety. Dans B. Wilpert, & T. Qvale, Reliability and safety in hazardous work systems. (pp. 3-23). Hove: LEA.

Reason, J. (1997). *managing the risks of organisational accidents.* Burlington: Ashgate.

Rossel, P. (2009). *Weak signals as a flexible framing space for enhanced management and decision making.* Technology Analysis and Strategic Management, 21(3), 307-320.

Vaughan, D. (1997). *The challenger launch decision: Risky technology, culture and deviance at NASA.* Chicago: University of Chicago press.

Weick, K., Sutcliffe, K., & Obstfeld, D. (1999). *Organizing for reliability: processes of collective mindfulness.* research in organizational behavior , 81-123.

Fiche 2

Défis associés aux boucles de régulation

Défis associés aux boucles de régulation

L'analyse des usages et applications des boucles de régulation fait ressortir un certain nombre de défis récurrents qui s'appliquent aussi à la gestion des risques. Ces défis sont les suivants :

La dépendance aux modèles

La mise en place d'une boucle de régulation implique le choix d'un modèle de sécurité qui dicte les moyens de contrôle à mettre en place. Or, tout ce qui n'est pas dans le modèle n'est pas régulé et échappe donc à la maîtrise que le gestionnaire peut exercer sur le système. En d'autres termes, toute gestion de la sécurité aura les faiblesses et limites du modèle de sécurité qu'elle exploite. Hollnagel (2008) décrit cette dépendance comme le « talon d'Achille » de la gestion de la sécurité.

Le paradoxe du régulateur

La principale donnée d'entrée de toute boucle de régulation est l'ensemble des écarts entre les objectifs définis et les performances constatées. Or, une bonne performance suppose une réduction de ces écarts et donc des données de moins en moins significatives statistiquement.

Cela est particulièrement vrai pour la sécurité des procédés où :

- la **probabilité très faible des événements** rend statistiquement peu représentatives les petites modifications que l'on peut constater d'une année à une autre. Il devient donc difficile pour le manager de distinguer une réelle modification des performances sécurité d'une simple variation statistique inhérente à tout phénomène aléatoire comme les accidents majeurs.
- L'absence d'**événements ou de décalages détectés** par la boucle de régulation a tendance à être perçue comme une performance sécurité satisfaisante, engendrant ainsi une **sensation** de confort ou pire, une baisse des ressources, dommageables pour la sécurité.

L'équilibre entre efficacité et ressources consommées

Concevoir la « bonne » boucle de régulation n'est pas tout, encore faut-il la maintenir dans le temps en lui allouant les ressources nécessaires. Un équilibre est à trouver entre des boucles de régulation couvrant autant que possible l'ensemble des dimensions du système (efficacité) tout en minimisant le poids pour l'organisation en termes de consommation de ressources et d'altération d'activités annexes. Un exemple simple peut se trouver dans la nécessité d'arrêter ou de ralentir la production lors des inspections des barrières techniques de sécurité.

Les multiples finalités de la boucle de régulation

Il est attendu des boucles de régulation, en plus de constater des décalages, d'apporter aux décideurs des capacités prédictives et exploratoires. Les capacités prédictives impliquent une capacité d'anticipation des évolutions du système.

Dans le cas de la sécurité, cela est rendu particulièrement difficile du fait de la complexité des systèmes sociotechniques rendant leurs comportements futurs non entièrement prédictibles par la description de leurs comportements passés.

De plus, certains systèmes à risques peuvent connaitre des périodes de latence entre l'occurrence d'un évènement et la perception de ses conséquences (IRGC, 2010). Les capacités exploratoires impliquent d'apporter aux décideurs la capacité de comprendre les causes profondes des décalages afin de calibrer leurs actions.

Fiche 2

Défis associés aux boucles de régulation

Là aussi, le caractère non linéaire des relations cause-effet et les boucles de rétroaction positives associées aux systèmes sociotechniques constituent des obstacles importants

Bibliographie

Hollnagel, E. (2008). Safety management - *Looking back or looking forward.* Dans E.

Hollnagel, C. P. Nemeth, & S. Dekker, Resilience *engineering perspectives.* Volume 1 (pp. 63-78). Aldershot: Ashgate.

IRGC. (2010). *The emergence of risks.* Contributing factors. Genève.

Fiche 3

Du concept de performance

Ils ont dit...

«Une Entreprise sans profits ne peut vivre mais une Entreprise qui ne vit que pour le profit en mourra »

Henri Ford.

Ils ont dit...

«Il n'est plus possible d'avoir une personne apprenante pour l'ensemble de l'organisation, il n'est simplement plus possible d'imaginer la solution d'en haut »

(Lorino, 1995)

Du concept de performance

La performance est un concept qui a aujourd'hui envahi l'ensemble des dimensions de la vie de l'organisation. Même si la performance financière demeure la plus influente et la plus fédératrice (Kaplan & Norton, 1996), d'autres dimensions viennent s'agencer autour : la sécurité, la fiabilité, la responsabilité sociétale ou l'image sont autant d'axes d'évaluation des performances organisationnelles non réductibles à l'évaluation financière.

Par conséquent, ne pouvant être représentée sur une échelle unique, la performance est considérée comme un concept multidimensionnel recourant à des tableaux de bords où de multiples indicateurs de natures diverses peuvent se côtoyer.

Exemple de tableau de bord multidimensionnels : Les tableaux de bord équilibrés (Balanced scorecards)

Le concept de Balanced Score Card (tableaux de bord équilibrés) a été élaboré par Kaplan et Norton (1996) (2007) pour refléter le besoin de dépasser la simple perspective financière lors des prises de décisions stratégiques. Cet outil est aujourd'hui très largement utilisé dans les industries et services.
Quatre perspectives y sont considérées :

- La perspective financière traduit les attentes des investisseurs en matière de performance financière
- La perspective client s'intéresse à considérer les critères de satisfaction des utilisateurs des services/produits proposés
- La perspective interne est orientée vers l'identification des processus internes clés permettant à l'organisation de maintenir ou d'améliorer ses positions.
- La perspective innovation et apprentissage évalue les capacités de l'organisation à continuer à apprendre et à créer de la valeur.

En plus d'être multidimensionnel, le concept de performance doit intégrer les facteurs de complexité et d'incertitudes. La complexité de l'organisation est ici vue en termes de variété et de multiplicité des activités, connaissances et pratiques mobilisées pour produire de la valeur.

Cette variété est elle même combinée à l'existence de niveaux d'autonomie à tous les échelons que chaque acteur exerce non seulement parce qu'il en a la possibilité mais aussi parce que la variabilité naturelle de ses activités l'exige (Amalberti, 2012). Par conséquent, il devient impossible pour le décideur de prétendre construire des représentations suffisamment riches et complètes pour entièrement définir les modalités de contrôle de l'organisation.

Le constat d'incertitudes précise que les activités de l'organisation ainsi que son environnement peuvent suivre des évolutions si rapides qu'il n'est pas envisageable d'en centraliser entièrement la planification. Bien au contraire, il est souhaitable, à tous les échelons, de laisser les capacités d'interprétation et d'adaptation qui permettront à l'organisation de s'adapter aux circonstances.

Ainsi, Lorino (1995) et Segrestin (2004) recommandent de passer d'une vision où la performance est contrôlée par des modèles centralisés et systématiquement comparée à une norme prédéfinie, à une vision où la performance est pilotée. Dans cette seconde posture, les interprétations individuelles sont reconnues comme justifiées et nécessaires pour le fonctionnement du système.

Néanmoins, elles sont en amont encadrées par des règles qui laissent des possibilités d'interprétation tout en posant des limites à ne pas dépasser. Ainsi, plutôt que de contrôler la performance par une mesure et une comparaison à une norme, on cherchera plutôt à l'influer et à la placer dans un cycle de diagnostic et d'amélioration continue.

Fiche 3

Du concept de performance

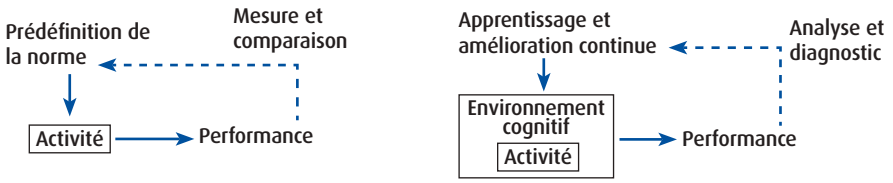


Figure 7 : Comparaison des schémas de contrôle (à gauche) et de pilotage (à droite) de la performance (inspiré de (Lorino, 1995))

A titre d'exemple, cela reviendrait à remplacer des procédures de travail préétablies et fermées qui ne peuvent être adaptées à l'ensemble des situations à la définition d'un cadre précisant les règles de sécurité à ne pas enfreindre. L'opérateur peut ainsi évoluer librement et s'adapter à la variabilité naturelle de ses conditions de travail tant qu'il ne viole aucune des règles de sécurité du cadre qui lui est fourni.

Dans un tel contexte, les gestionnaires de la performance n'exercent plus un contrôle, mais un méta contrôle sur les différentes interprétations et adaptations effectuées sur le terrain (Lorino, 1995).

Une conséquence importante d'une telle évolution est le passage de la simple mesure de la performance qui se compare à une norme à l'exercice continu d'analyses et de diagnostics basés sur la variété des interprétations existant dans l'organisation.

Pour ce faire, des schémas plus participatifs impliquant l'ensemble des échelons de l'organisation sont nécessaires. Ces schémas visent à effectuer les analyses causales nécessaires à la compréhension des évolutions et changements des performances et y apporter les modifications nécessaires tout en assurant un apprentissage partagé entre les différents niveaux organisationnels.

Cela permet non seulement de créer les échanges nécessaires entre opérateurs et managers ; mais invite aussi ces derniers à s'éloigner de la « simple » vérification de l'application des normes ; plus souvent désignée comme le management par les chiffres.

Par conséquent, nous considérerons que la performance :

- est un concept **multidimensionnel** qui ne peut être réduit à une échelle unique (monétaire, nombre d'accidents...), sous peine d'hyper simplification d'une réalité bien plus riche ;
- ne doit **pas être uniquement** mesurée et comparée à une norme. Elle doit être analysée et communiquée au sein de l'organisation ;
- ne peut **plus être verticalement dictée** et normée du fait des hauts niveaux d'incertitudes et de complexité des activités organisationnelles ;
- se doit d'être considérée dans un **cycle continu** d'analyse et diagnostics impliquant et confrontant de multiples représentations.

Bibliographie

Amalberti, R. (2012). *Piloter la sécurité.* Springer Verlag France.

Kaplan, R. S., & Norton, D. P. (2007). *Using the balanced scorecard as a strategic management system.* Harvard Business review , 1-14.

Kaplan, R., & Norton, D. (1996). *The balanced scorecard: Translating strategy into action.* Harvard business school press.

Lorino, P. (1995). *Comptes et récits de la performance.* Paris: Editions d'Organisation.

Segrestin, D. (2004). *les chantiers du manager.* Paris: Armand Colin.

Senge, p. (1990). *The fifth discipline. Londres* : Century business.

Fiche 4

De la définition de la sécurité à la définition des modèles de sécurité

De la définition de la sécurité à la définition des modèles de sécurité

Qu'est ce que la sécurité ?

Malgré l'extrême variété des définitions de la notion de sécurité, nous pouvons distinguer deux écoles de pensée et de compréhension de la notion de sécurité :

❒ La sécurité en tant qu'inverse du risque.

Nous retrouvons ici les approches consistant à définir la sécurité comme l'absence de danger (EPSC, 1996) ou le maintien des risques en dessous d'un niveau jugé comme acceptable (ICAO, 2006).

La sécurité est ici paradoxalement définie comme une absence et non pas une présence. Plus précisément, l'absence d'événements susceptibles de porter atteinte aux enjeux ou de la mise en place d'un système de contrôle qualité permettant de maintenir ces événements à un niveau d'intensité et de fréquence acceptables.

Cette vision est aujourd'hui prédominante dans les pratiques de gestion des risques. Elle fonde les cadres d'analyse des risques qui cherchent à identifier l'ensemble des défaillances (techniques ou humaines) et de leurs combinaisons pouvant aboutir à l'occurrence d'une séquence accidentelle. Dans un second temps, elles s'intéressent à entraver le déroulement de cette séquence par la mise en place de barrières de sécurité. Enfin, ces mesures sont gérées dans le temps pour s'assurer du maintien de leurs performances.

Une telle vision est :

- *analytique* dans le sens où les installations sont décomposées et les activités humaines discrétisées avant d'en analyser les modes de défaillance possibles ;
- *centrée sur la notion de défaillance* qui distingue les fonctionnements et comportements conformes aux normes des autres. Par conséquent, la sécurité ne peut être compromise que suite à une ou plusieurs défaillances ;
- *fortement dépendante* de la capacité à *couvrir exhaustivement les différentes possibilités de défaillance*. La défaillance ou la combinaison de défaillances non identifiées ne sont pas gérées.

❒ La sécurité comme produit de l'organisation dans son contexte.

Weick (1987) décrit la sécurité comme un « non événement dynamique ». Si l'on retrouve ici la caractérisation de la sécurité comme une absence d'événements, l'accent est mis sur la variabilité des conditions antérieures ayant amené l'absence d'événements préjudiciables. Ainsi, cette absence d'événements n'est pas le résultat d'une conformité continue à une norme ; c'est plutôt un ensemble de mécanismes évolutifs mais dont les combinaisons sont demeurées dans les limites de l'acceptable.

En allant plus loin, Hollnagel (2006) définit la sécurité comme un produit de la capacité des personnes à s'adapter à la variabilité de leurs conditions opératoires. La complexité de ces conditions dans lesquelles les activités sont menées et les décisions prises ne pouvant être entièrement prévue dans les normes, les opérateurs et décideurs dans les systèmes à risques se doivent d'adapter leurs comportements à la variabilité des conditions réelles.

Ce ne sont plus uniquement les défaillances qu'il s'agit d'identifier ; ce sont aussi les capacités d'interprétation et d'adaptation déployées par l'homme pour gérer les situations quotidiennes qu'il faut valoriser.

Cette approche pointe les possibilités d'accidents qui ne sont pas dues à des défaillances particulières, mais à la variabilité des performances individuelles qui, à un instant donné, peuvent se combiner de manière à générer un accident.

Ils ont dit...

« L'accident de demain ne résultera d'aucune panne particulière, d'aucune erreur mais d'une érosion qui aura affaibli les composants. L'ampleur de variation des conditions de travail d'un jour aura suffit à dépasser les seuils de couplage favorable »

(Amalberti, 2012).

Fiche 4

De la définition de la sécurité à la définition des modèles de sécurité

Cette optique n'est pas sans rappeler l'approche centrée sur le pilotage de la performance plutôt que sur son contrôle par la prédéfinition de normes à atteindre.
La variabilité des conditions réelles est ici aussi reconnue et le dirigeant est invité à axer son travail sur la définition d'un espace de contraintes sécurité dans lequel les acteurs peuvent évoluer plutôt que de les enfermer dans des procédures et normes trop strictes.

Deux visions de la sécurité : contradictoires ou complémentaires ?

Il ne s'agit pas de préférer une vision à une autre. Il s'agit plutôt de comprendre une évolution du concept de sécurité qui suit, à intervalles plus ou moins proches, les évolutions des systèmes à risques. Ainsi, la sécurité comme inverse du risque a permis de grandes et indéniables avancées dans la sécurité. Néanmoins, de nombreux facteurs appellent à compléter cette vision et à chercher de nouveaux gisements d'amélioration :

- La persistance des accidents majeurs dans les systèmes ayant mis en place ce type d'approches.
- Des systèmes à risques de plus en plus complexes avec des environnements sociétaux (technologiques, économiques, sociaux et réglementaires) fortement évolutifs. En conséquence, les marges de sécurité sont de plus en plus réduites et les possibilités d'instauration de routines de moins en moins faisable.
- Une acceptabilité des risques et des accidents de plus en plus réduite dans nos sociétés. Ainsi, bien que l'accident de Tchernobyl (1986) ait eu en Europe des conséquences physiques bien plus importantes que la catastrophe de Fukushima (2011) ; les conséquences sociétales du dernier ont été bien plus importantes avec des pays comme l'Allemagne et la Suisse qui décident de sortir de l'énergie nucléaire.

Enfin, Weinberg (1975) et Leveson (2011) apportent un éclairage complémentaire en distinguant les besoins en approche sécurité en fonction d'une caractérisation des systèmes à risques sur deux échelles : le niveau d'aléa statistique et la complexité.

- Les systèmes appartenant à la catégorie complexité désorganisée se définissent par un haut niveau de variabilité mais présentent des schémas de comportement agrégés récurrents. Ils sont ainsi approchables par les lois statistiques. A titre d'exemple, prévoir le vote d'un unique individu est difficile, mais ceux d'une population représentative peuvent faire l'objet d'analyses statistiques valides.
- Les systèmes appartenant à la catégorie simplicité organisée peuvent être décomposés dans la mesure où les comportements de leurs composants sont suffisamment indépendants pour être analysés individuellement. L'absence d'interactions non linéaires et de phénomènes d'émergences de nouveaux états du système rend les approches analytiques classiques basées exclusivement sur la décomposition et le contrôle de performances adaptées.
- Enfin, la catégorie complexité organisée désigne des systèmes suffisamment organisés pour ne pas être approchés par les statistiques mais dont les composants sont fortement intriqués rendant les approches analytiques limitées.

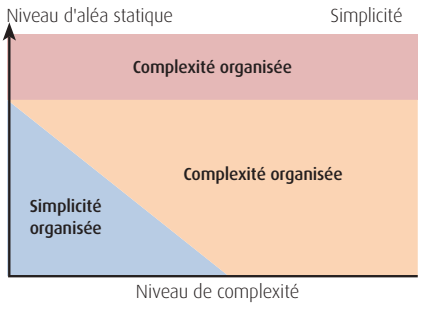


Figure 8 Définitions de la sécurité

Les systèmes sociotechniques auxquels nous nous intéressons dans ce travail peuvent être rattachés à cette catégorie. Nous avons régulièrement recours aux approches statistiques pour qualifier les probabilités d'événements, notamment les événements redoutés centraux (ERC).

Nous avons aussi recours à la discrétisation des comportements (approches de fiabilité humaine) et à la décomposition des systèmes quand ceux-ci sont déjà bien connus et suffisamment simples.

Enfin, la complexité organisée est aussi fortement présente comme cela a déjà été largement soulevé dans la littérature et déjà discuté plus en avant.

Par conséquent, nous parlerons dans ce qui suit de complémentarité entre ces visions de la sécurité et les modèles qui leur sont associés plutôt que de contradictions.

Fiche 4

De la définition de la sécurité à la définition des modèles de sécurité

De la définition aux modèles : La sécurité en actions

La sécurité ainsi définie de manière plurielle, les questions fondant la gestion des risques demeurent identiques : Comment prévenir l'occurrence d'accidents majeurs ? Quand ceux-ci ont quand même lieu, quelles sont les responsabilités ?

Répondre à ces questions nécessite de développer des modèles de sécurité expliquant ce que l'on pense être les mécanismes sous jacent à la production de la sécurité, et des accidents majeurs. La littérature scientifique regorge aujourd'hui de modèles de sécurité, appelés aussi modèles d'accidents ou modèles de causalité.

Hovden et al (2010) assignent à ces modèles les usages suivants :

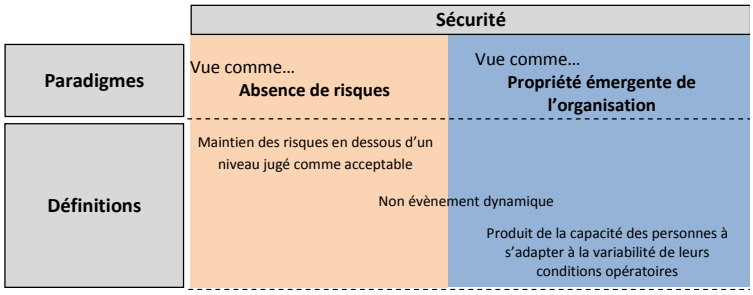


Figure 9 Définitions de la sécurité

- Création d'une **compréhension commune** des phénomènes accidentels à travers une simplification partagée des accidents réels ;
- Aider à **structurer les échanges** sur les questions des risques majeurs ;
- Offrir une **base méthodologique** permettant de dépasser les biais individuels lors des enquêtes post accidentelles ;
- Guider les investigations **post accidentelles** ;
- Offrir une **variété de points de vue** lors de ces enquêtes.

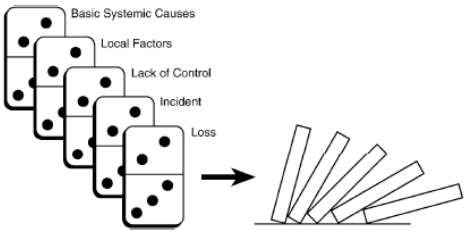
Dans le cadre du présent guide, nous nous focaliserons sur les usages en situation de prévention, où il s'agit d'accompagner les gestionnaires de la sécurité dans l'identification des aspects et mécanismes importants pour la préservation ou l'amélioration des niveaux de sécurité. En d'autres termes, il s'agit de savoir quoi mesurer quand on s'intéresse aux performances sécurité.

Hollnagel (2004) classifie[24] les modèles de sécurité selon les trois catégories suivantes :

Modèles « séquentiels »

C'est la première catégorie de modèles de sécurité à avoir été développée. L'accident est décomposé en séquences où s'enchainent des évènements liés par des relations cause-conséquence. Gérer la sécurité revient donc à identifier de manière exhaustive les séquences accidentelles possibles ainsi que les évènements (défaillances humaines ou techniques) qui y contribuent.

L'objet principal de ces modèles étant l'identification des défaillances et leur maitrise, ils entrent bien au service d'une définition de la sécurité axée sur la maitrise des risques. Un modèle emblématique de cette catégorie demeure celui des dominos d'Heinrich (1931).



A l'image des dominos qui chutent les uns après les autres, l'accident est ici vu comme une séquence linéaire commençant par un environnement inadapté générant des comportements dangereux qui finissent par déboucher sur des erreurs humaines et des accidents.

[24] La typologie adoptée ici répond aux besoins pédagogiques du présent document. Le lecteur peut enrichir sa compréhension des modèles de sécurité en se référant à d'autres typologies dans Lehto et Salvendy (1991) ou Le Coze (2013).

Fiche 4

De la définition de la sécurité à la définition des modèles de sécurité

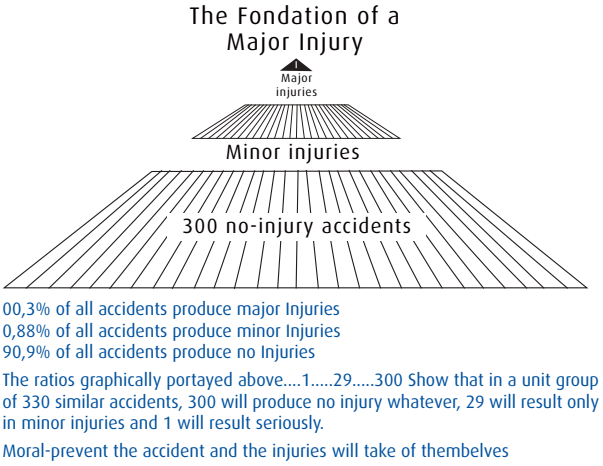


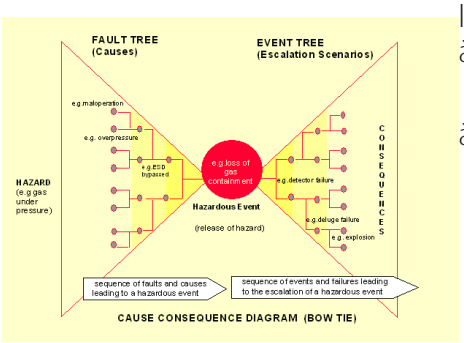
Figure 9. Pyramide statistique d'Heinrich

Heinrich propose de focaliser la prévention sur le dernier domino avant l'accident, c'est-à-dire les comportements dangereux ou l'erreur humaine. Il construit la légitimité de cette assertion sur la base de statistiques assurantielles précisant que 87% des accidents étaient dus à des erreurs humaines (Heinrich, 1950).

Dans un second temps, il établit un lien statistique entre le nombre de comportements dangereux constatés et le nombre d'accidents graves donnant ainsi naissance à la première version de la pyramide statistique des accidents (***Figure 9***).

Plusieurs points sont à relever :

- Si les dimensions organisationnelles sont déjà considérées dans ce modèle, elles demeurent au second plan du fait de la vision linéaire de l'accident qui pousse à porter son attention sur le dernier élément précédant l'accident, savoir, l'erreur humaine.
- Les statistiques ayant servi à construire ces pyramides sont axées sur les risques au poste de travail et non pas sur les risques majeurs. Cela n'a pas empêché une utilisation massive de ce modèle pour le développement d'indicateurs de performance sécurité pour les risques majeurs.



D'autres modèles peuvent être classés dans cette catégorie. Les plus populaires d'entre eux demeurent probablement les arbres d'événements et de conséquences largement utilisés dans le cadre des analyses de risques pour identifier et décrire les scénarios d'accidents.

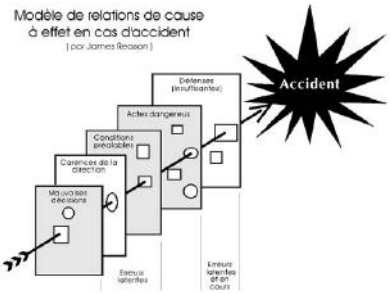
❒ Modèles « épidémiologiques »

A la différence des modèles purement séquentiels, les accidents sont vus ici comme la combinaison d'événements manifestes et visibles et de conditions latentes ou dormantes installées depuis longtemps dans l'organisation. Le mécanisme est semblable à celui d'une maladie causée par la concomitance d'un facteur pathogène et de conditions environnementales (conditions latentes telles que le stress, la fatigue...) affaiblissant les défenses immunitaires et permettant à la maladie de s'installer.

Turner (1976) a été un précurseur en soulignant que les accidents démontraient avant leur apparition une période d'incubation matérialisée par l'existence de symptômes latents qui ne se transforment en accident que si combinés avec des événements précis.

Fiche 4

De la définition de la sécurité à la définition des modèles de sécurité



Plus tard, Reason (1990) propose la métaphore de tranches de gruyères où les trous représentent les conditions latentes qui affaiblissent les barrières de sécurité mises en place dans le système. Le Swiss cheese model est ainsi devenu représentatif de cette catégorie de modèles et a été repris largement, aussi bien au niveau académique que professionnel, à des finalités d'enquête accident et de prévention des risques.

Un autre exemple de modèle dans cette catégorie est celui du Système de Gestion de la Sécurité (SGS). Basés sur une approche empirique recensant les facteurs susceptibles de contribuer à améliorer la sécurité (Hale, Heming, Carthey, & Kirwan, 1997), les SGS ambitionnent de définir et conceptualiser la liste des processus managériaux permettant à une organisation de détecter et traiter les défaillances latentes qui peuvent y séjourner *(Figure 3)*

De très nombreux modèles de SGS se trouvent aujourd'hui dans la littérature (Delatour, Laclemence, Calcei, & Mazri, 2014). Néanmoins, il serait prétentieux pour chacun de ces modèles de prétendre à l'identification de l'ensemble des conditions latentes dans la mesure où celles-ci ne font pas toujours l'objet de processus managériaux bien identifiés. A titre d'exemple, les attitudes individuelles vis-à-vis de la sécurité, la politique de sanction des erreurs individuelles[25] , le leadership ou encore les équilibres de pouvoir entre fonctions de production d'une part et sécurité d'autre part sont généralement peu ou pas considérés dans les SGS.

Les SGS sont aujourd'hui largement repris aussi bien par la réglementation (Directives Seveso II et III) que par les industriels qui en font le cadre organisationnel de référence s'agissant de la sécurité.

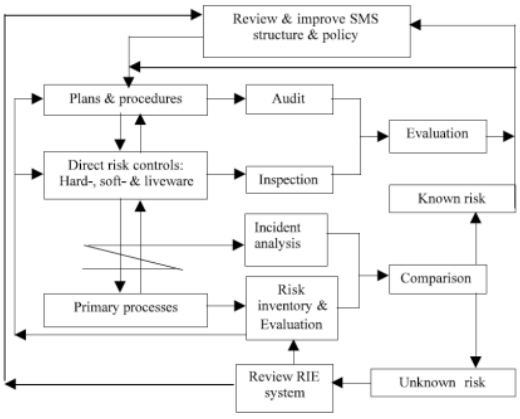


Figure 10 Modèle de Système de gestion de la Sécurité par Hale et al (2003)

Cette catégorie de modèles est à distinguer des modèles séquentiels sur les aspects suivants :

- La culpabilité de l'accident ne repose plus sur les épaules de l'opérateur qui effectue le dernier geste avant l'accident. C'est l'ensemble de l'organisation qui se doit de s'interroger sur sa capacité à créer et entretenir des conditions latentes favorables à un accident.

  Ainsi, Reason précise que les conditions latentes peuvent aussi bien provenir des comportements individuels que des choix stratégiques dont les conséquences impactent l'ensemble de l'organisation.

  A titre d'exemple, privilégier systématiquement la disponibilité de l'appareil de production au détriment des actes de maintenance sur les dispositifs de sécurité quand ceux-ci peuvent nécessiter un arrêt ou un ralentissement de la production est une condition latente.

[25] En tant que facteur influençant la remontée d'informations dans le cadre du retour d'expérience.

Fiche 4

De la définition de la sécurité à la définition des modèles de sécurité

- L''accident n'est plus une séquence linéaire d'événements, mais une combinaison complexe d'événements et de conditions environnementales latentes. La sécurité ne se résume donc plus à contrôler le comportement de l'homme pour en détecter les erreurs, il s'agit plutôt de comprendre et de gérer une multiplicité de conditions environnementales dans lesquelles les décisions et pratiques sont situées pour en détecter les déviations et les corriger. Là aussi, une évolution sémantique importante s'opère. On ne parle plus d'erreur qui désigne un écart par rapport à une norme ; mais de déviation de performance du fait de conditions opératoires.

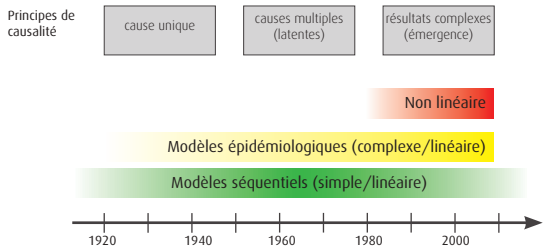


Figure 11 Typologie des modèles de sécurité selon Hollnagel (2004).

❒ Modèles « systémiques »

L'évolution des systèmes à risques vers plus de **complexité** et de **connectivité** a trouvé un large écho dans cette troisième catégorie de modèles où l'accent est mis sur la singularité et la complexité des mécanismes sous jacents à la performance sécurité.

Les premiers travaux sont ceux de Perrow (1984) qui voit les accidents comme une conséquence normale et inévitable de l'évolution des systèmes à risques vers plus de complexité rendant le nombre de combinaisons accidentelles illimité.

Ces systèmes ne peuvent donc plus être simplement étudiés par décomposition et analyse mais doivent plutôt être abordés dans une vision globalisante ou systémique. Un tel constat appelle les conclusions suivantes :

- L'impossibilité d'**identifier l'ensemble** des événements et conjonctions pouvant amener à l'occurrence d'un accident limite l'usage des normes et standards puisque ces derniers ne peuvent englober l'ensemble des possibilités.

  Plutôt que de concevoir des normes et traquer les erreurs et défaillances, le gestionnaire du risque est invité à reconnaître la variabilité naturelle des systèmes complexes à travers la valorisation des capacités d'adaptation à tous les niveaux.

- La sécurité ne peut se réduire à traquer et éliminer les combinaisons de défaillances et d'erreurs, elle est aussi une capacité à **promouvoir des comportements** adaptés et à identifier les adaptations nécessaires aux fluctuations naturelles du système.

- La sécurité est le résultat de la combinaison de multiples dynamiques qui traversent le système. Ces dynamiques peuvent être techniques, humaines et organisationnelles. Elles peuvent aussi se manifester à l'ensemble des niveaux de l'organisation et de son environnement, allant jusqu'au cadre législatif dans lequel les organisations opèrent (Rasmussen, 1997). Par conséquent, la sécurité est une **propriété émergente** du système à risques.

- Les accidents ne peuvent plus être représentés par des séquences linéaires d'événements mais plutôt par des **réseaux** représentatifs de la variété des interactions façonnant la performance sécurité finale.

- La variabilité et l'adaptation étant les maîtres-mots de ces modèles, il est naturel d'y retrouver au cœur le besoin de **développer des outils** de suivi et d'évaluation de performances permettant aux boucles de pilotage d'opérer.

Ils ont dit...

« Rather than striving to control behavior by fighting deviations from a particular pre-planned path, the focus should be on the control of behavior by making the boundaries explicit and known and by giving opportunities to developing skills at boundaries »

(Rasmussen, 1997)

Fiche 4

De la définition de la sécurité à la définition des modèles de sécurité

Ci-dessous sont présentés quelques exemples de modèles systémiques.

① ACCIMAP

Proposée par Rasmussen (1997), cette approche de modélisation s'intéresse à déployer une **démarche verticale** permettant de comprendre l'**ensemble des décideurs**, ou autorités de contrôle, dont les activités et décisions se superposent et interagissent pour influer sur la performance sécurité finale. Les usages d'ACCIMAP varient en fonction des contextes.

Elle a aussi bien été utilisée pour le déploiement d'une démarche proactive de gestion des risques (Rasmussen & Svedung, 2000) que pour reconstituer, dans l'ensemble des niveaux de l'organisation, les facteurs ayant contribué à l'occurrence d'un accident.

Nous présentons ici ce modèle pour illustrer les différences de modélisation et de représentation du concept d'accident induites par ces approches comparativement aux modèles séquentiels et épidémiologiques décrits précédemment.

Cinq niveaux de décision susceptibles d'influer sur la performance sécurité sont distingués : le gouvernement, le régulateur ainsi que les niveaux stratégiques, tactiques et opérationnels de l'entreprise en charge de la gestion du risque.

La superposition de ces différents niveaux de contrôle, la description de leurs interactions et de la manière dont ils influent sur le déroulement des événements sont représentés dans des diagrammes dont nous présentons le format ainsi qu'un exemple en ***Figure 12***.

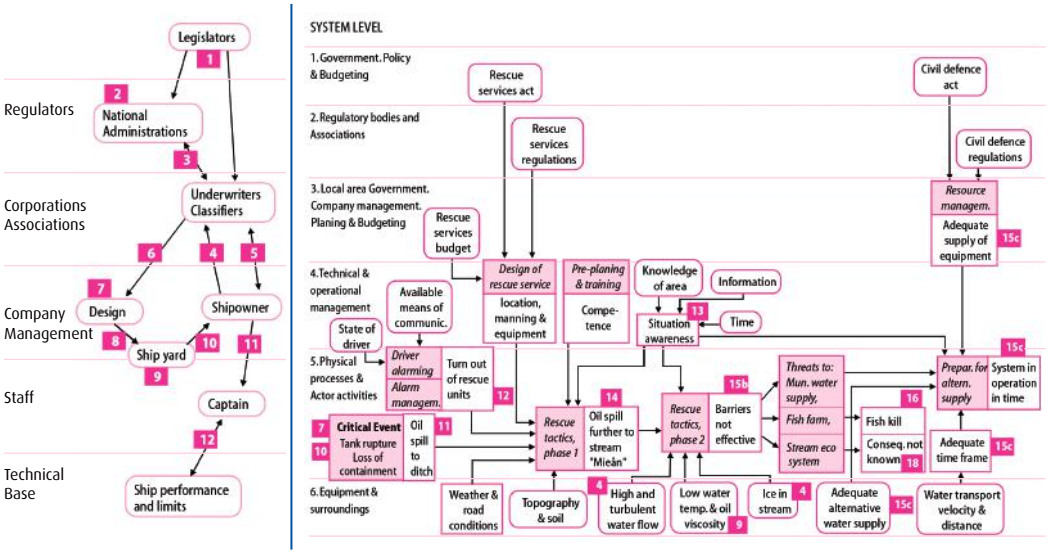


Figure 12 : Structure des diagrammes ACCIMAP à gauche et un exemple d'application à droite.

② HRO (High Reliability Organisations)

Certaines organisations démontrent une capacité à atteindre et maintenir des performances sécurité élevées malgré les caractères complexe et risqué de leurs activités. Le nucléaire ou le transport aérien sont des exemples souvent cités à ce niveau.

Le modèle des organisations hautement fiables vise à identifier et décrire les conditions permettant à ces organisations d'atteindre ces performances. La sécurité y est vue comme le résultat d'attitudes personnelles et de pratiques managériales permettant de produire de la sécurité. Identifier et décrire les impacts de ces attitudes et pratiques pour en proposer la généralisation sont les objectifs de ces modèles.

Avec la variété des études varient les descriptifs des pratiques et attitudes contribuant à produire de la sécurité.

Fiche 4

De la définition de la sécurité à la définition des modèles de sécurité

Nous décrivons ci-dessus un échantillon, nécessairement non exhaustif, des descriptions empiriques proposées par ce cadre théorique :

- La combinaison de modes décisionnels centralisés et décentralisés en fonction des situations. Ainsi, quand l'activité est routinière et bien connue, le cadre hiérarchique et centralisé est adopté. Dès que le niveau d'incertitudes est élevé ou quand l'activité est exceptionnelle, ce sont **les compétences et savoirs qui priment** sur les positionnements hiérarchiques.
- Le développement de compétences est un **processus continu** et au cœur des activités de l'ensemble du personnel.
- Une bonne culture de **déclaration** et de **traitement des incidents** et signaux d'alerte. Plus précisément, l'engagement individuel de l'ensemble du personnel à déclarer les événements est complété par une attitude managériale plus intéressée par la compréhension du caractère systémique des événements (conditions organisationnelles) que par la recherche de culpabilités individuelles.
- La communication des informations sur la sécurité est performante et bilatérale entre opérateurs et managers. A titre d'exemple, la transmission des consignes entre équipes ou la révision participative des procédures au regard de l'évolution des conditions opérationnelles sont des canaux d'information organisés et maintenus dans le temps.

Dans le cadre du présent travail, l'ensemble de ces aspects mis en lumière par les HRO peuvent directement constituer des objets de mesure approchables par des indicateurs de performance dédiés.

③ **FRAM** (Functional Resonance Accident Model)

Proposé par Hollnagel (2004), FRAM est une approche de modélisation d'accidents ne résultant pas de défaillance ou de mauvais fonctionnements particuliers, mais plutôt de combinaison de variabilités individuelles qui peuvent être en résonance et ainsi entrainer des conséquences disproportionnées aux évènements initiateurs.

Pour ce faire, FRAM se base dans un premier temps sur une modélisation individuelle des fonctions ou activités composant le système à travers les six paramètres suivantes : I (Input : ce que la fonction utilise ou transforme) ; O (Output : ce que la fonction produit) ; P (Pré-conditions nécessaires pour que la fonction remplisse sa mission) ; R (Ressources nécessaires à la fonction) ; T (Temps) et C (Contrôles et supervision de la fonction). Chacune des fonctions entrant dans la composition du système à risques est donc représentée par un hexagone tel qu'en ***Figure 13***

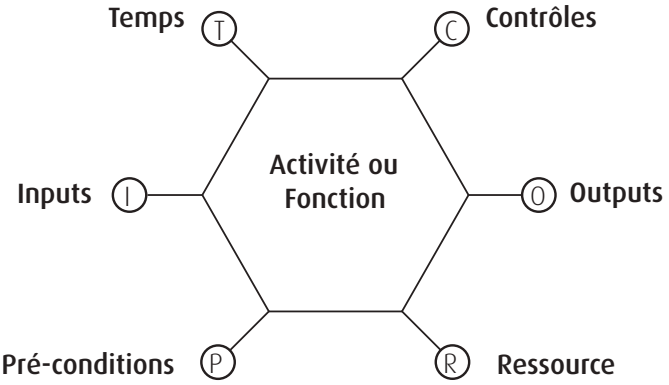


Figure 13 Modélisation des activités dans FRAM

Chacune des fonctions ainsi modélisée est dans un second temps explorée pour identifier les possibles facteurs contributifs à la variabilité de son fonctionnement dans le temps. Enfin, en liant ces activités entre elles en fonction de leurs

Fiche 4

De la définition de la sécurité à la définition des modèles de sécurité

dépendances, l'utilisateur est capable d'étudier les combinaisons de variabilité pouvant amener à l'occurrence d'un accident majeur.

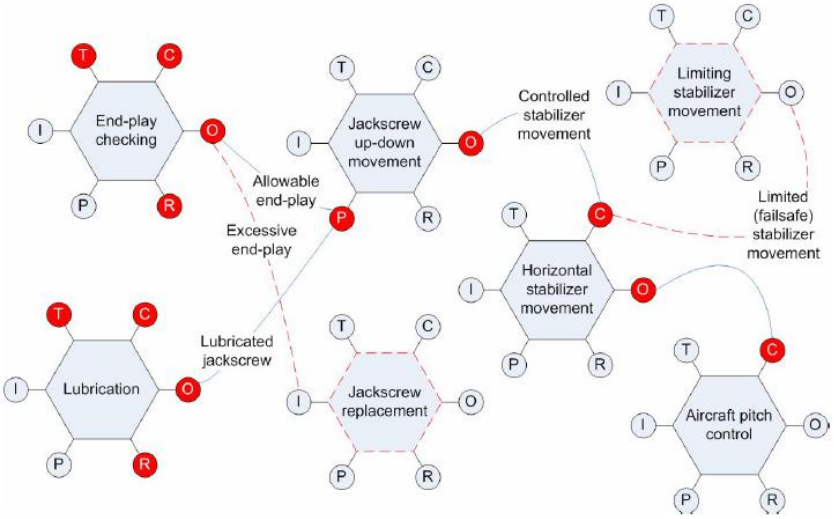


Figure 14 : Exemple des interactions entre fonctions composant un même système à risque. Les nœuds en rouge soulignant les variabilités pouvant aboutir à une séquence accidentelle (Woltjer & Hollnagel, 2007).

Ils ont dit...

« It is essential to create a corporate atmosphere or culture in which safety is understood to be and is accepted as, the number one priority »

Lord Cullen, 1990 après l'accident de Piper Alpha.

④ Culture sécurité

Dans la quête des modalités de production de la sécurité au sein des organisations, le développement d'une culture adaptée est une des pistes de travail explorées dans la littérature. Définie comme l'ensemble des règles non écrites qui gouvernent le comportement acceptable à l'intérieur et à l'extérieur de l'organisation (Mitrof, Pauchant, Finney, & Pearson, 1989), la culture est un concept transverse qui touche aussi bien les individus que les niveaux organisationnels impliqués dans la gestion des systèmes à risques. Cette vision holistique est donc particulièrement adaptée à l'ambition des modèles systémiques de sécurité.

La culture sécurité est donc **une dimension de la culture de l'entreprise** qui affecte les **attitudes** et **croyances** des membres de l'organisation en matière de performances sécurité (Cooper, 2000). Elle permet, là aussi, d'aller plus loin que la simple identification des défaillances et erreurs pour comprendre les contextes organisationnels et culturels dans lesquels les activités de l'organisation sont exercées. Elle ambitionne aussi d'agir sur ces facteurs pour en retirer une meilleure compréhension des faiblesses de l'organisation et identifier les axes d'amélioration.

A ce titre, une large variété de questionnaires, d'échelles et d'approches d'évaluations ont été développées, amenant parfois à s'interroger sur la maturité et la stabilité scientifique de ces approches (Guldenmund, 2000).

Nous pouvons néanmoins distinguer trois composantes majeures dont les interactions mutuelles sont considérées comme constitutives d'une culture sécurité (Cooper, 2000) :

- La **composante psychologique** s'intéresse à décrire les normes, valeurs et percep-tions individuelles qui président aux comportements des opérateurs dans leurs rapports quotidiens avec la sécurité. Cette composante est généralement décrite sous la dénomination de *climat de sécurité* (safety climate) et est essentiellement abordée à travers des questionnaires (Mearns, Whitaker, & Flin, 2003).
- La **composante situationnelle** désigne les effets des orientations et pratiques organisationnelles sur les activités quotidiennes. La politique sécurité, la définition des procédures ou le système de management mis en place sont des exemples des aspects évalués à ce niveau.

Fiche 4

De la définition de la sécurité à la définition des modèles de sécurité

- La **composante comportementale** étudie les comportements au quotidien au regard de la dimension sécurité à travers des observations ou des autoévaluations. Il s'agit ici en particulier de déceler les éventuels décalages entre les perceptions (composante psychologique) et la réalité des pratiques sur le terrain.

  Un élément important à ce niveau est de comprendre le caractère holistique de la culture sécurité qui ne peut être approchée par des évaluations distinctes de chacune de ces trois dimensions. C'est bien les dynamiques et interactions entre ces différents aspects qu'il s'agit de cerner lors des évaluations de performance sécurité.

⑤ ATHOS

Le modèle ATHOS (Analyse Technique, Humaine et Organisationnelle de la Sécurité) est le résultat d'une décennie de travaux en facteurs humains et organisationnels à l'INERIS. Ancré dans une démarche interdisciplinaire, ce modèle normatif vise à mettre en lumière un certain nombre de facteurs influant la sécurité à différents niveaux de l'organisation. Chacun de ces facteurs est représenté par une thématique que les managers sécurité sont invités à considérer aussi bien individuellement que dans le cadre des interactions qu'elle peut avoir avec les autres (***Figure 15***).

Au niveau micro, les gestionnaires de la sécurité sont invités à s'intéresser à l'état des barrières techniques et humaines ainsi qu'à leurs modalités d'implémentation qui se doivent de prendre en compte la variabilité quotidienne des opérations à risques. Le niveau méso s'intéresse à l'organisation et à ses caractéristiques à travers la capacité d'écoute des signaux faibles et de remise en cause, la compétence et l'influence du service sécurité sur les prises de décision ainsi que la prise en compte des changements techniques et organisationnels. Enfin, le niveau macro s'intéresse à l'environnement de l'organisation représenté notamment par la qualité des regards extérieur sur les pratiques sécurité de l'organisation ainsi que les modalités d'appréciation des ressources et contraintes au niveau stratégique.

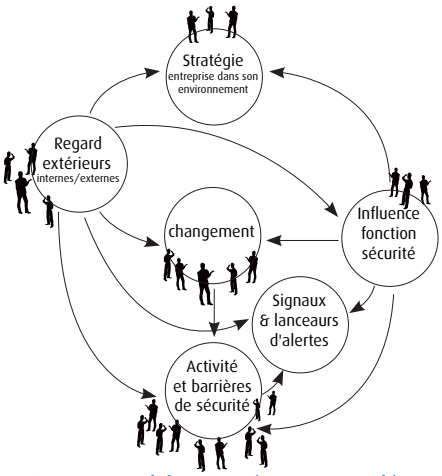


Figure 15 Modèle ATHOS (Le Coze, 2013b)

Ainsi le modèle peut se lire de la manière suivante :

Les adaptations stratégiques des dirigeants (1) de l'organisation dans son environnement (de marché, de régulation), l'environnement de l'organisation, etc, mènent à des changements organisationnels et technologiques (2), plus ou moins contraints, plus ou moins subis, plus ou moins concomitants, plus ou moins cumulés.

Ces changements peuvent avoir des conséquences positives ou négatives sur le fonctionnement des barrières techniques et humaines de sécurité (3) prévues en conception (analyse de risque). Les problèmes de mises en œuvre de ces barrières doivent se traduire notamment par une écoute attentive des signaux faibles ainsi qu'une capacité réflexive à la suite d'incidents/accidents (4).

Cette réflexivité repose au niveau organisationnel sur un service sécurité compétent et suffisamment influent (5), ainsi que sur, une organisation en mesure de mobiliser des regards extérieurs de qualité (6), pour comprendre et de tirer les enseignements, qui se traduisent concrètement dans les choix stratégiques et les pratiques.

Fiche 4

De la définition de la sécurité à la définition des modèles de sécurité

ATHOS se veut donc un modèle à essence systémique considérant la sécurité à travers un prisme à multiples niveaux organisationnels.

En ***Figure 16*** ci-dessous, nous nous proposons d'associer la représentation des paradigmes et définitions de la notion de sécurité aux différents modèles introduits ci-dessus.

Maintenant que les notions de performance et de sécurité ont été introduites, c'est la notion d'indicateurs que nous nous proposons d'explorer dans ce qui suit.

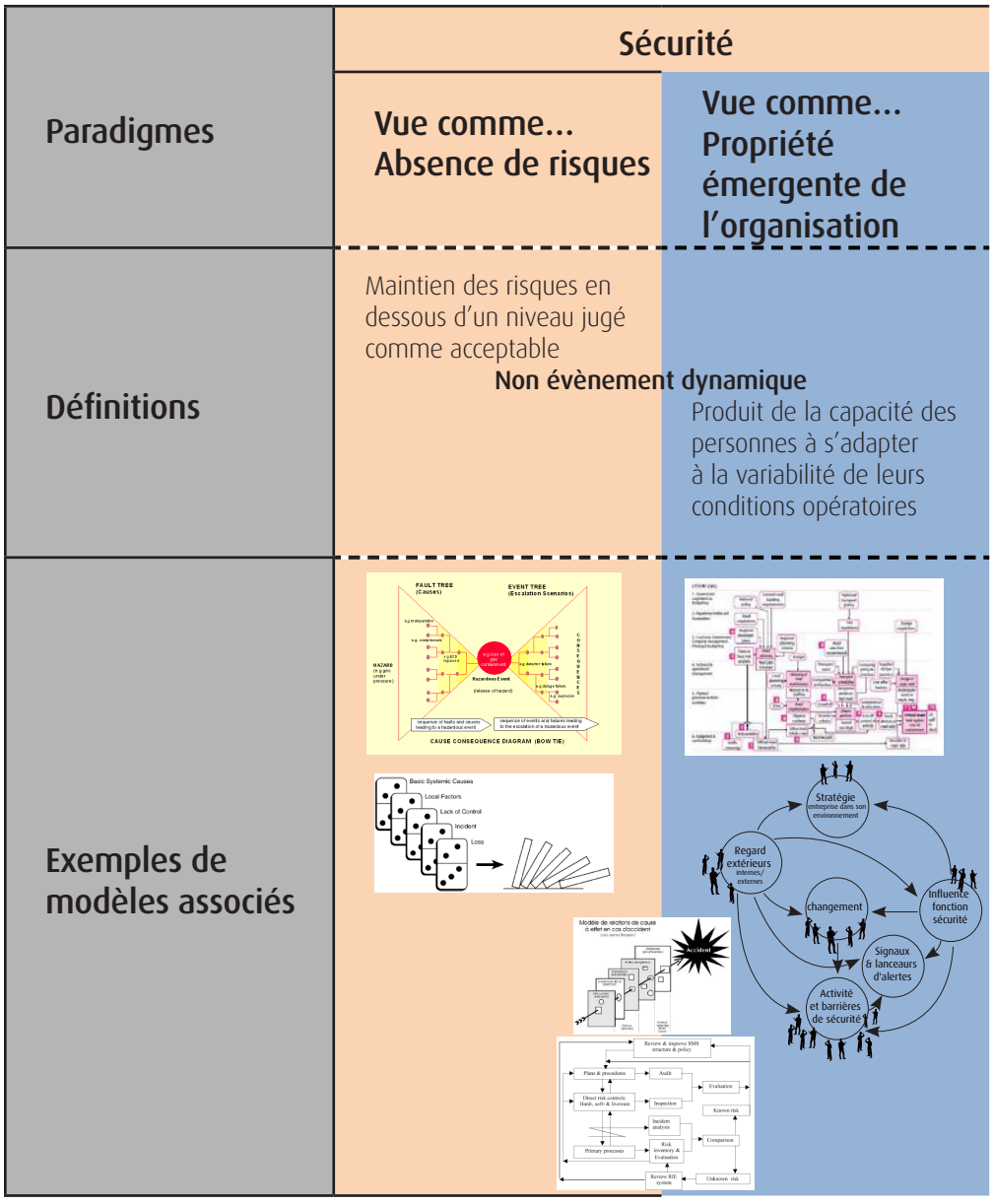


Figure 16 : Des définitions de la sécurité aux modèles

Bibliographie

Amalberti, R. (2012). *Piloter la sécurité.* Springer Verlag France.

Bird, F. E., & Germain. (1969). *Practical loss control leadership.* Intl loss control inst.

Cooper, M. D. (2000). *Towards a model of safety culture.* Safety science 36, 111-136.

Delatour, G., Laclemence, P., Calcei, D., & Mazri, C. (2014). *Systèmes de gestion*

de la sécurité. Quel espace critique pour la décision d'anticipation ? IMDR. Dijon.

EPSC. (1996). *Safety performance measurement.* IchemE.

Guldenmund, F. W. (2000). *The nature of safety culture : a review of theory and research.* Safety science (34), 215-257.

Hale, A. R., Heming, B. H., Carthey, J., & Kirwan, B. (1997). *Modelling of safety management systems.* Safety science 26(1), 121-140.

Heinrich, H. W. (1950). *Industrial accident prevention :* A scientific approach. 3rd edition. new York : McGraw Hill.

Hollnagel, E. (2006). *Achieving system safety by resilience engineering.* Conference on system safety. London.

Hollnagel, E. (2004). *Barriers and accident prevention.* Burlington : Ashgate.

Hopkins, A. (2008). *Failure to learn.* The BP Texas city refinery disaster. Sydney : CCH Australia.

Hovden, J., Albrechtsen, E., & Herrera, I. A. (2010). *Is there a need for new theories, models and approaches to occupational accident prevention.* Safety science (48), 950-956.

ICAO. (2006). Safety management manual.

le Coze, J. C. (2013). *New models for new times. An anti dualist move.* safety science (59), 200-218.

Le Coze, J. C. (2013b). *Outlines of a sensitising model for industrial safety assessment.* Safety science (51) , 187-201.

Lehto, M., & Salvendy, G. (1991). *Models of accident causation and their applications : Review and reappraisal.* Journal of engineering and technology management, 173-205.

Leveson, N. G. (2011). *Engineering a safer world. Systems thinking applied to safety.* London : The MIT Press.

Mearns, K., Whitaker, S. M., & Flin, R. (2003). *Safety climate, safety management practice and safety performance in management environments.* Safety science (41), 641-680.

Meyer, T., & Reniers, G. (2013). *Engineering risk management.* Berlin : De Gruyter.

Mitrof, I. I., Pauchant, T., Finney, M., & Pearson, C. (1989). *Do (some) organizations cause their own crises ? The cultural profile of crisis-prone vs crisis-prepared organizations.* Industrial crisis Quarterly (3), 269-283.
Perrow, C. (1984). *Normal accidents. New York :* Basic books.

Rasmussen, J. (1997). *Risk management in a dynamic society : A modelling problem.* Safety science 27 (2/3) , 183-213.

Rasmussen, J., & Svedung, S. (2000). *Proactive risk management in dynamic society. Karlstad:* Swedish rescue services agency.

Reason, J. (1990). *Human error.* Cambridge UNiversity Press.

Turner, B. (1976). *The organizational and Interorganizational development of*

disasters. Administrative science quarterly 21(3), 378-397.

Weick, K. E. (1987). *Organisational culture as a source of High reliability.* California Management Review (29), 112-127.

Weinberg, G. (1975). *An introduction to general systems thinking. New york :* John Wiley.

Woltjer, R., & Hollnagel, E. (2007). *The Alaska Airlines flight 261 accident : A systemic analysis of functional resonance.* Proceedings of the 2007 International symposium on aviation psychology, (pp. 763-768). Dayton.

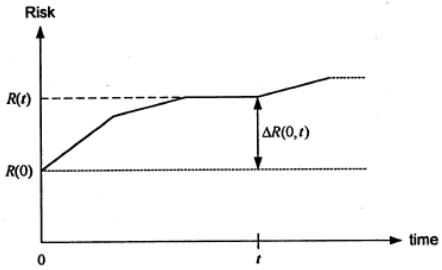
Fiche 5

Revue de littérature des méthodes d'identification d'indicateurs performance sécurité

Revue de littérature des méthodes d'identification d'indicateurs performance sécurité

Méthode 1 : Risk based indicators (Oien, Risk indicators as a tool for risk control , 2001)

Hypothèses de travail



- Le risque se définit comme un triplet (S_i, P_j, C_k) où S est l'ensemble des scénarios, P et C sont respectivement la probabilité et les niveaux de conséquences associées à chaque scénario.
- Le niveau de risque global d'un système se définit par le nombre de morts toutes les 10^8 heures de travail.
- Les indicateurs servent, dans ce contexte, à suivre l'évolution du niveau de risques entre deux analyses de risques (sur une durée t) sur la base de la métrique décrite ci-dessus. Cette démarche est donc bien basée sur un modèle où la sécurité est vue comme une absence de risques et appelle donc à la maitrise des évènements indésirables.
- La valeur finale du risque est fonction d'un certain nombre de facteurs d'influence (RIF : Risk Influence Factors). Est défini comme facteur d'influence tout paramètre du modèle en Figure 17 susceptible par son évolution d'influer sur la valeur finale du risque. A titre d'exemple, la modification de la probabilité de défaillance d'une mesure de maitrise des risques est un facteur d'influence puisqu'elle entre en compte dans le calcul du niveau final du risque.

Déroulé de la méthode

1. Dans le cadre d'un QRA[26] , le niveau de risque final exprimé en nombre de morts par 10^8 heures de travail est évalué en agrégeant l'ensemble des probabilités des scénarios considérés. De ce fait, tous les paramètres entrant dans le calcul des probabilités de chaque scénario se trouvent mathématiquement reliés à la valeur finale du risque. Ces paramètres sont les RIFs du système.

   Vinnem (2003) définit trois types de facteurs d'influence (RIF) :

   - Facteurs d'influence *opérationnels* relatifs aux activités humaines quotidiennes susceptibles d'avoir un impact sur la sécurité du système.
   - Facteurs d'influences *organisationnels* ou managériaux définis par les orientations organisationnelles mises en place pour gérer la sécurité.
   - Facteurs d'influence *réglementaires* relatifs aux cadres réglementaires mis en place et les mesures de contrôle associées.

2. Dans cette liste de RIFs, seuls ceux dont les performances peuvent évoluer, et notamment se dégrader dans le temps, sont considérés. A titre d'exemple, les performances des mesures passives de maitrise des risques (double enveloppe d'une sphère, cuve de rétention...) sont considérées comme suffisamment stables dans le temps pour éviter de recourir à des indicateurs de performance.
3. Une analyse de sensibilité est pratiquée sur chaque RIF pour évaluer l'impact de sa dégradation potentielle sur le niveau final du risque. Les facteurs d'influence sont ainsi classifiés en fonction de leur capacité à détériorer le niveau final du risque.

[26] Quantitative Risk Assessment.

Fiche 5

Revue de littérature des méthodes d'identification d'indicateurs performance sécurité

❹ Les RIFs les plus impactant sont retenus comme devant être suivis dans le temps. Oien (2001) suggère de retenir dans l'ordre ceux qui ont le plus d'impact et ceux dont l'impact sur le niveau de risque est supérieur à un facteur prédéterminé par le gestionnaire de risques.

❺ Un brainstorming est effectué pour identifier des indicateurs candidats associés à chaque RIF. Il est précisé que le choix d'un ou de plusieurs indicateurs par RIF demeure un arbitrage propre à chaque situation.

Méthode 2 : Dual Assurance Approach (HSE, 2006)

Hypothèses de travail

❒ Cette méthode s'appuie sur le modèle de sécurité proposé par de Reason (1990). Pour rappel, les accidents sont ici vus comme une combinaison de **conditions actives** (défaillances techniques ou humaines) et de **conditions latentes** ou dormantes de nature organisationnelle.

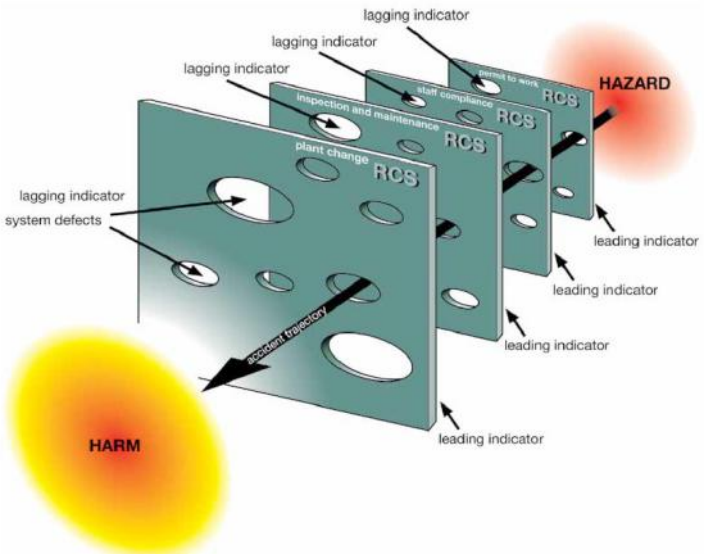


Figure 17 Les RCS dans le modèle de Reason (HSE, 2006).

❒ Il n'est pas nécessaire de mesurer les performances de l'ensemble des éléments du système à risques. De la même manière qu'un contrôle de santé chez un humain se concentre sur certains paramètres vitaux, il s'agit ici de focaliser le suivi de performances sur certains paramètres jugés symptomatiques de l'état de santé de l'organisation s'agissant de la sécurité.

Les paramètres symptomatiques de l'état de l'organisation ne doivent pas se limiter aux défaillances techniques ou aux erreurs humaines. Ils doivent remonter au fonctionnement même de l'organisation susceptible d'altérer les performances techniques et humaines.

❒ Six **leviers de contrôle** des systèmes à risques (Risk Control Systems, RCS) sont identifiés comme nécessitant un suivi dans le temps. Ces leviers sont :

- La *gestion des modifications* ;
- L'*inspection* et la *maintenance* des installations ;
- La gestion de la *compétence du personnel* au regard des questions relatives à la sécurité ;
- Modalités de *définition* et de *réactualisation* des procédures opérationnelles ;
- Gestion des situations d'*urgence* ;
- Modalités d'attribution des *permis de travaux* sur le site à risques.

Fiche 5

Revue de littérature des méthodes d'identification d'indicateurs performance sécurité

Déroulé de la méthode

Basée sur le modèle de sécurité de Reason, l'approche HSE définit les RCS comme autant de barrières empêchant la séquence accidentelle d'arriver à terme. Elle propose de suivre les performances de chaque RCS (qui constituent donc les objets de mesure) en combinant les deux types d'indicateurs que sont leading (proactifs) et lagging (résultats). Pour chaque RCS, il est proposé de combiner ces deux modes d'évaluation pour obtenir non seulement une représentation de la performance, mais comprendre aussi les dynamiques générant une bonne ou une mauvaise performance.

Ci-dessous quelques éléments d'interprétation de ces dynamiques :

- Dans les cas où les indicateurs proactifs et indicateurs de résultats indiquent simultanément des bonnes (ou des mauvaises performances), le constat est clair et ne nécessite pas plus d'approfondissement.
- Dans le cas où les indicateurs de résultat indiquent des performances satisfaisantes alors que les indicateurs de fonctionnement pointent l'inverse, cela implique que le RCS est en cours de détérioration même si les conséquences ne se sont pas encore fait ressentir sur le système.
- Si les indicateurs de résultats sont mauvais alors que ceux de fonctionnement sont bons, cela peut impliquer que des modifications introduites récemment n'ont pas encore produits de résultats visibles ou qu'une des deux catégories d'indicateurs n'est simplement pas bonne!

Méthode 3 : TRIPOD-DELTA (Hudson, Reason, Wagenaar, bentley, Primrose, & Visser, 1994)

Hypothèses de travail

- Similairement à la méthode précédente, la démarche TRIPOD-DELTA s'appuie sur le modèle de sécurité de Reason (1990). Elle se distingue néanmoins par les leviers identifiés pour exercer un contrôle sur le système. Ainsi, ce ne sont plus les 6 RCS retenus dans la démarche précédente mais Onze modes généraux de défaillances (General Failure types) qui sont considérés.
- Les GFTs font ici office d'objets dont les performances doivent être suivies dans le temps. Les 11 GFT en question sont les suivants :
  - **Matériel (Hardware) :** Qualité et disponibilité des équipements et outillages. Ce premier type questionne les politiques d'achat et de gestion des stocks de l'organisation au regard des impératifs sécurité.
  - **Design :** Traite des défaillances dans le design des installations ou des composants générant des conditions favorables à l'erreur humaine ou à la défaillance technique. A titre d'exemple, le caractère opaque des modalités et conditions d'utilisation des systèmes ou le caractère difficilement interprétable des informations renvoyées par le dispositif peuvent entrainer des accidents.
  - **Elaboration des procédures :** Appréciation du caractère clair, adapté et réactualisé des procédures opérationnelles.
  - **Gestion de la maintenance :** Place et qualité de la maintenance du système à risques.
  - **Conditions opérationnelles** favorables à l'erreur : Il s'agit d'évaluer comment les conditions de travail quotidiennes peuvent favoriser les comportements à risques ou les erreurs humaines.
  - **Incompatibilité des objectifs :** Quand les objectifs sécurité entrent en conflit avec d'autres objectifs, qu'ils soient personnels ou organisationnels.

Fiche 5

Revue de littérature des méthodes d'identification d'indicateurs performance sécurité

- **Faiblesse de la communication :** Quand la communication des informations à risques est absente ou défaillante. Nous pouvons citer comme exemple ici le cas des mauvaises transmissions de consignes entre équipes de travail successives.
- **Organisation :** Sont plus particulièrement considérés ici les modalités organisationnelles permettant de dissiper les responsabilités et éviter de traiter les problèmes même quand ceux-ci sont identifiés.
- **Engagement :** Célérité et volonté de l'organisation de s'attaquer aux problèmes dès que ceux-ci sont posés.
- **Formation :** qualité, disponibilité et réactualisation des formations, prise en compte des retours sur formations...
- **Défenses :** regroupe les défaillances relatives à la gestion des situations d'urgence et de retour à la normale.

Déroulé de la méthode

Comme spécifié précédemment, Tripod-DELTA identifie un ensemble de modes généraux de défaillance (GFT) qui constituent les objets dont elle souhaite mesurer l'évolution des performances.

Pour chacun des GFTs, une base de données d'indicateurs est constituée. Ces indicateurs sont nombreux mais volontairement simples (réponse oui/non) et faciles à comprendre. Un outil informatique sélectionne régulièrement un échantillon des bases de données de chaque GFT pour constituer un questionnaire soumis aux salariés.

Un profil global de l'organisation se dessine ainsi sur la base des performances remontées sur chaque GFT par les check-lists ainsi constituées. Ces dernières diffèrent d'un cycle à un autre puisque le logiciel s'assure de varier les indicateurs remontés à chaque cycle.

Nous notons ici deux types d'équilibres entre les contraintes de couverture et de coût pour l'organisation évoquées précédemment. L'approche HSE se concentre sur un ensemble relativement réduit d'indicateurs alors que la méthode Tripod-DELTA mise sur une large couverture à travers un grand nombre d'indicateurs mais dont l'utilisation est simplifiée tout en suivant un principe de renouvellement régulier.

Méthode 4 : REWI (Resilience Early Warning Indicators ; Oien, Massaiu, & Tinmannsvik, 2012)

La démarche place la notion de résilience au centre de son modèle sécurité. Ainsi, ce sont les capacités techniques et organisationnelles à prévenir les perturbations et à retrouver un état d'équilibre qui sont valorisées dans le cadre de cette démarche

- Hollnagel (2006) définit la **résilience** comme la capacité intrinsèque d'une organisation ou d'un système à ajuster son fonctionnement avant, pendant ou après qu'elle ait subit des perturbations, de manière à assurer la continuité de ses opérations. Plus simplement, la résilience peut être vue comme la capacité d'une organisation à gérer ce qu'elle n'avait pas prévu.

  Placée au centre d'un modèle de sécurité, la résilience désigne un **ensemble de capacités organisationnelles** qui vont au-delà des aspects classiquement traités quand il s'agit de gérer des risques que l'on a auparavant bien identifiés et caractérisés. Par conséquent, l'objet de la mesure de performances dans ce contexte est bien l'ensemble de ces capacités organisationnelles et leur maintien dans le temps.

Fiche 5

Revue de littérature des méthodes d'identification d'indicateurs performance sécurité

- La démarche REWI s'appuie sur une **décomposition arborescente** du concept de résilience conformément aux travaux de Storseth et al (2009). Plus précisément, cette décomposition permet d'identifier des facteurs contributifs au succès (Contributing Success factors, CSF) qui constituent donc autant d'objet à suivre dans le temps (***Figure 18***).

  Ces facteurs de succès doivent être considérés aussi bien individuellement pour en comprendre les implications quotidiennes que holistiquement pour en analyser les interactions et complémentarités.

  Ainsi, la notion de résilience est d'abord scindée en trois propriétés : La **conscience du risque**, la mise en place de **capacités de réponse** adaptées et la disponibilité d'un **appui à la prise de décision** quand les situations ne peuvent être totalement abordées par des procédures préétablies.

  Chacune de ces trois propriétés sont à leur tout décomposées comme suit :

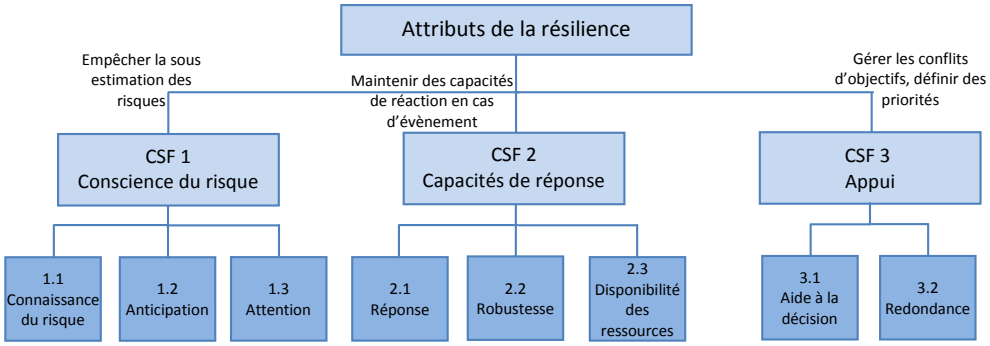


Figure 18 Capacités organisationnelles nécessaires à la construction de la résilience

- La **connaissance du risque** traduit les connaissances, compétences et expériences mises en pratique pour reconnaitre l'existence d'un risque et en décrire les propriétés (probabilité, intensité…).
- L'**anticipation** et l'**attention** traduisent les capacités de l'organisation à mettre en place l'écoute des signaux faibles et du retour d'expérience pour déceler les limites de ses connaissances et anticiper les évolutions du système.
- Les **capacités de réponse** sont décomposées en qualité de réponse (savoir quoi faire), capacité de faire face au stress en préparant l'organisation à différentes possibilités (robustesse) et enfin, la disponibilité des ressources pour mener à bien ces réponses.
- L'appui se base sur la disponibilité et la redondance des capacités d'aide à la décision.

Enfin, chacun des 8 CSF est à son tour décomposé en capacités considérées comme un niveau de maillage suffisant pour permettre la mise en place d'indicateurs dédiés.

Fiche 5

Revue de littérature des méthodes d'identification d'indicateurs performance sécurité

A titre d'exemple, nous ne présenterons dans ce qui suit la réflexion menée sur le CSF 1.1 à savoir « la connaissance du risque ».

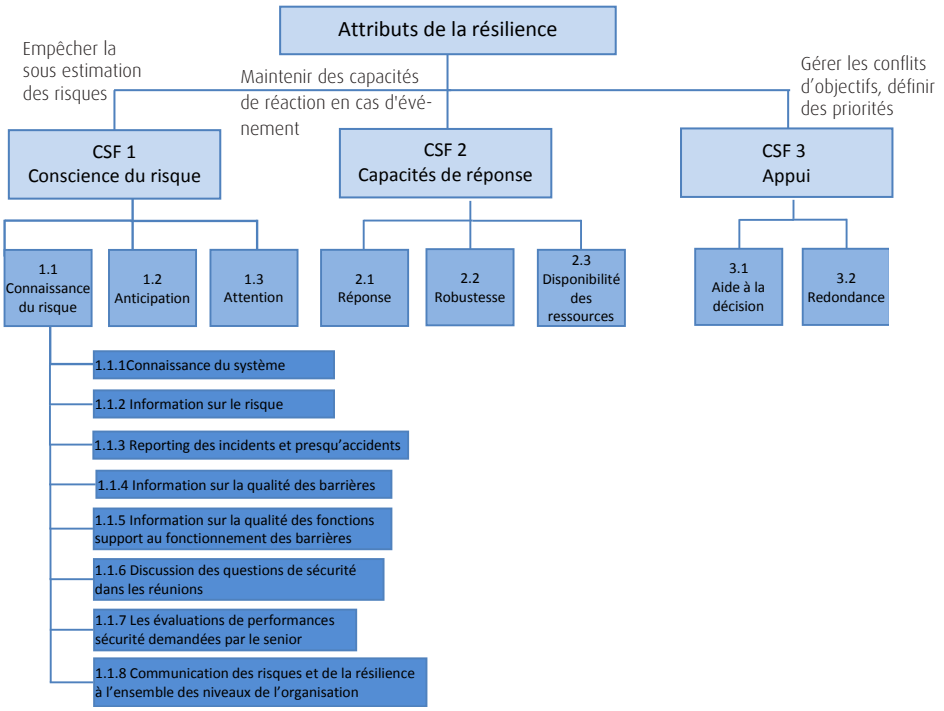


Figure 19 Liste des capacités associées au CSF « connaissance du risque ».

Déroulé de la méthode

L'exploration des capacités présentées précédemment est organisée selon les étapes présentées en ***Figure 20*** ci-dessous.

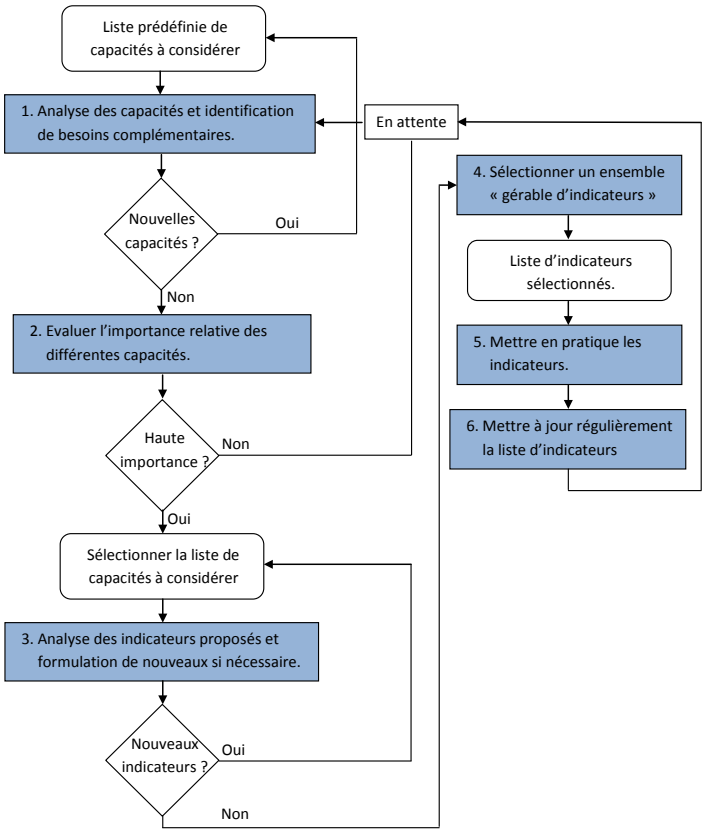


Figure 20 Schéma de la démarche REWI (Oien, Massaiu, & Tinmannsvik, 2012).

Fiche 5

Revue de littérature des méthodes d'identification d'indicateurs performance sécurité

Bibliographie

Hollnagel, E. (2006). *Achieving system safety by resilience engineering.* COnference on system safety. London.

HSE. (2006). *Developping process safety indicators.* A step by step guide for chemical and major hazard industries. HSE Books.

Hudson, P. T., Reason, J., Wagenaar, W. A., bentley, P. D., Primrose, M., & Visser, J. (1994). *Tripod-Delta: proactive approach to enhanced safety*. Journal of Petroleum technology 46(1), 58-62.

Oien, K. (2001). *Risk indicators as a tool for risk control.* Reliability engineering and system safety 74 (2), 129-145.

Oien, K. Massaiu, S., & Tinmannsvik, R. K. (2012). *Guidelines for implementing* the REWI method.

Reason, J. (1990). *Human error.* Cambridge UNiversity Press.

Reason, J. (1997). *managing the risks of organisational accidents.* Burlington: Ashgate.

Storseth, F. Tnimannsvik, R. K, & Oien, K. (2009). *Building safety by resilient organisation- A case specific approach.* European Safety and Reliability Association Annual Conference. Prague.

Vinnem, J. E. (2003). *Operational safety of FPSO shutter tank collision risk summary report.* NTNU, Norway : Research report 113.

Fiche 6

Modalités de calcul de l'indicateur PSI conformément aux recommandations du CCPS (2007)

Fiche 6 : Modalités de calcul de l'indicateur PSI conformément aux recommandations du CCPS (2007)

Description et objectifs

Cet indicateur comptabilise le nombre et la gravité des pertes de confinement associées à des risques majeurs. Il permet ainsi de juger de la capacité du système à maintenir une intégrité mécanique satisfaisante.

Afin de s'assurer que seules les pertes de confinement associées à des risques majeurs sont considérées, les conditions suivantes s'appliquent :

- La perte de confinement doit avoir lieu sur des équipements et activités susceptibles de générer des accidents majeurs. Plus précisément, il s'agit d'équipements/ateliers de production, distribution (tuyauterie ou canalisation sous le contrôle du gestionnaire), stockage et toute installation auxiliaire (génération de vapeur...).
- La perte de confinement doit entrainer des dommages dépassant à minima l'un des seuils suivants :
- Atteinte d'un salarié ou sous traitant nécessitant un arrêt de travail ou d'un tiers autre (personne hors site).
- La quantité de produit relâchée doit dépasser en une période limitée à 1 heure [27] un seuil qui varie en fonction de sa dangerosité.
- Incendies ou explosions dont les conséquences dépassent une valeur monétaire de 25000 $.
- Déclenchement d'un POI ou d'un PPI.

Modalités de calcul

Le tableau 1 ci-dessous indique un système de scoring associé à chaque incident en fonction des niveaux des différents critères suivants :

- Blessures et atteinte à la vie humaine.
- Dommages économiques dus aux incendies/explosions.
- Relâchement de substances toxiques.
- Impact sur l'environnement et riverains du site.

[27] **Si l'atteinte de la quantité minimale s'effectue sur des périodes dépassant l'heure, l'incident est considéré comme chronique et non accidentel.**

Fiche 6

Modalités de calcul de l'indicateur PSI conformément aux recommandations du CCPS (2007)

Severity Level (Note 4)	Safety/Human Health (Note 5	Fire or Explosion (Including overpressure)	Potential Chemical Impact (Note 3)	Community/Environment Impact (Note 5)
NA	Does not meet or exceed Level 4 threshold	Does not meet or exceed Level 4 threshold	Does not meet or exceed Level 4 threshold	Does not meet or exceed Level 4 threshold
4 (1 point used in severity rate calculations for each of the attributes chich apply to the incident)	Injury requiring tratment beyond first aid to employee or contractors (or equivalent, Note 1) associated with a process safety incident (In USA, incidents meeting the definitions of an OSHA recordable injury	Resulting in $25,000 to $100,000 of direct cost	Chemical released withim secondary containment or contrained withim the unitsee Not 2A	Short-term remediation to adress acute environnement impact. Nor long term cost or company oversight. Examples would include spill cleamp, soil and veetation removal.
3 (3 points used in severity rate calculations for each of the attributes which apply to the incident)	Lost time injury to employee or contractors associated with a proces safety event	Resulting in $100,000 to IMM of direct cost.	Chemical release outside of containment but retrained on company property OR flammable release without potential for vapor cloud explosives - see Note 2B	Minor off-site impact with precautionary shelter-in-place OR Environmental remediation required with cost less than $1MM. No other regulatory oversight required OR Local media coverage
2 (9 points used in severity rate calculations for each of the attributes which apply to the incident)	On-site fatality - employee or contractors associated with a process safety event ; multiple lost time injuries or one or more serious offsite injuries associated with a process safety event.	Resulting in $1MM to $10MM of direct cost.	chemical release with potential for injury off site or flammable release resulting in a vapor cloud entering explosion site (congrested/ confined area) with potential dor damage or casualties if ignited - see Not 2C	Shelter-in-place or community evacuation OR environmental remediation required and cost in between $1MM - $2;5MM. state government investigation an oversight of process. OR Regional media coverage or brief national media coverage.
1 (27 points in severity rate calculations for each of the attributes which apply to the incident)	Off-site fatality or multiple on-site fatalities associated a process safety event.	Resulting in direct cost >$10MM.	Chemical release with potential for significant on-site or off-site injuries or fatalities see Note 2D	National media coverage over multiple days. OR Environmental remediation required and cost in excess of $2,5MM. Federal government investigation an oversight of process. OR other significant community impact.

Tableau 7 Calcul du niveau de sévérité associé aux incidents dans le cadre de l'indicateur PSI

maîtriser le risque
pour un développement durable

Rédaction : Chabane MAZRI, INERIS - Direction des risques accidentels
INERIS - Parc Alata, BP2, 60550 VERNEUIL EN HALATTE - www.ineris.fr

Mise en forme pédagogique, conception graphique et mise en page :
Olivier PERON et Charlotte BRUNET, INERIS, Parc Alata, BP2, 60550 VERNEUIL EN HALATTE