AIDES
A LA REFLEXION

Exploitation des systèmes techniques à risques majeurs et culture de sécurité

Groupe d'échange « Culture de sécurité et sécurité des systèmes techniques »

Edition coordonnée par Dounia Tazi et Jean-Michel Pesteil

n° 2020-01

THÉMATIQUE

Culture de sécurité

Les Cahiers de la sécurité industrielle

ICSI
Institut pour une culture de sécurité industrielle

Seveso, Bhopal, Enschede, Fukushima… nous avons tous en mémoire des exemples d'accidents ou d'incidents qui ont fortement impacté l'environnement, meurtri des familles, mis en péril l'activité économique d'un territoire.

La complexité technique du sujet, les enjeux de sécurité, les impératifs de développement des territoires, induisent une nécessaire appropriation de la démarche par toutes les parties prenantes.

Les progrès en matière de sécurité industrielle doivent émerger de tous les acteurs pour lesquels il est essentiel d'acquérir et de développer une véritable culture de sécurité.

C'est la vocation de l'**Institut pour une culture de sécurité industrielle** (Icsi), association loi 1901 créée en 2003, née de l'initiative conjointe d'industriels, d'universitaires, de chercheurs et de collectivités territoriales qui œuvrent collectivement à :

- ▷ Améliorer la sécurité dans les entreprises par la prise en compte du risque industriel sous tous ses aspects : technique, organisationnel et humain,
- ▷ Favoriser un débat ouvert et citoyen entre les entreprises à risques et la société civile, par une meilleure « éducation » à la gestion du risque et à l'amélioration de la sécurité,
- ▷ Favoriser l'acculturation de l'ensemble des acteurs de la société aux problèmes des risques et de la sécurité.

Éditeur : **Institut pour une culture de sécurité industrielle**
Association de loi 1901

http://www.icsi-eu.org/

6 allée Emile Monso – BP 34038
31029 Toulouse Cedex 4
France

Téléphone : +33 (0) 532 093 770
Courriel : contact@icsi-eu.org

Ce document

Titre	Exploitation des systèmes techniques et culture de sécurité
Mots-clés	Culture de sécurité, sécurité des procédés, système technique, conscience partagée, risques majeurs
Date de publication	Février 2020

L'efficacité de la prévention des accidents majeurs et de la préparation à la gestion d'une éventuelle catastrophe passe par une conscience partagée des risques majeurs pour tous les acteurs de l'entité concernée, de la direction aux opérateurs de terrain, sans oublier les entreprises extérieures.

Le groupe d'échange propose trois axes de travail pour accéder à cette conscience partagée du risque :

- ▷ Placer les risques majeurs au cœur du pilotage des processus ;
- ▷ Favoriser l'appropriation des risques majeurs par les équipes opérationnelles ;
- ▷ Mettre en place des moments clés d'animation sur les risques majeurs.

Pour chacun de ces trois axes, des recommandations et des bonnes pratiques sont présentées, ainsi que des conseils pour leur adaptation à d'autres contextes.

À propos des coordinateurs

Dounia Tazi est docteur ingénieur chimiste dans les systèmes industriels. Elle s'est spécialisée depuis 2005 dans la prise en compte des facteurs humains et organisationnels et la culture de sécurité dans les grands groupes industriels internationaux et chez leurs sous-traitants. Elle prend en 2019 la direction des opérations de l'Icsi.

Jean-Michel Pesteil est bénévole à l'Icsi. Il est ancien directeur délégué du Centre nucléaire de production d'électricité (CNPE) de Golfech.

Pour citer ce document

Groupe d'échange de l'Icsi « Culture de sécurité et sécurité des systèmes techniques » (2020). *Exploitation des systèmes techniques à risques majeurs et culture de sécurité. Les Cahiers de la sécurité industrielle*, n°2020-01. Institut pour une culture de sécurité industrielle, Toulouse, France.

Gratuitement téléchargeable sur : http://www.icsi-eu.org/.

Avant-propos

Après plus de 10 ans d'existence et de travaux sur la sécurité industrielle, il était temps pour l'Icsi de prendre un peu de recul sur la prévention des accidents majeurs pour la population ou l'environnement, des catastrophes comme celle d'AZF qui a été à l'origine de la création de l'institut. Ce cahier est issu des travaux d'un groupe d'échange constitué d'industriels ou exploitants d'ouvrages ou de procédés à risque majeur, de chercheurs, de syndicalistes, d'experts des organismes publics concernés. Il s'agissait d'identifier et de caractériser des conditions de maîtrise du risque applicables à tout système technique à risque majeur, en phase d'exploitation. On ne s'intéresse pas ici à la conception des systèmes ni leur démantèlement.

Il est très rapidement apparu que l'efficacité de la prévention de l'accident majeur et de la préparation à la gestion d'une éventuelle catastrophe passait par une conscience partagée du risque majeur pour tous les acteurs de l'entité concernée, de la direction aux opérateurs de terrain et aux prestataires. Cette conscience doit être provoquée et entretenue car de nombreux facteurs conduisent les parties prenantes à oublier le risque : robustesse de la conception, rareté des évènements graves, préoccupations quotidiennes centrées sur la production ou la sécurité au poste de travail, etc.

Le groupe d'échange propose trois axes de travail pour accéder à cette conscience partagée du risque :

- ▹ Placer les risques majeurs au cœur du pilotage des processus ;
- ▹ L'appropriation des risques majeurs par les équipes opérationnelles ;
- ▹ Des moments clés d'animation sur les risques majeurs.

La conscience partagée du risque suppose la connaissance des lignes de défense et la conscience des responsabilités individuelles et collectives pour garantir leur efficacité, leur maintien dans la durée et leur amélioration si nécessaire.

Pour chacun de ces trois axes, quelques recommandations générales sont présentées ainsi que des pratiques développées avec succès dans des entreprises représentées dans le groupe d'échange, avec quelques conseils pour leur adaptation à d'autres contextes.

Remerciements

Ce *Cahier de la sécurité industrielle* est issu des travaux du groupe d'échange « Culture de sécurité et sécurité des systèmes techniques » de l'Icsi, qui s'est réuni entre 2017 et 2019.

L'Icsi tient à remercier les personnes suivantes, qui par leur participation aux débats, leurs témoignages et leur investissement dans la rédaction, ont contribué à la réalisation de ce document.

Les membres du groupe d'échange

ANTOINE Augustin	Engie
BAGLAND Clara	Ponticelli
BODIN Audrey	Terega
DOMONT Jeremy	Ajinomoto Eurolysine
GALERA Christian	SNCF
HELDT Bernard	Icsi
JOUBERT Marc-Xavier	Suez
LAGATIE Philippe	Expert
LAGRANGE Valérie	EDF
LAURENT André	Université de Lorraine
LECHAT Jean-François	Icsi
MILARDO Charles	Expert
MONFORT Bertrand	CGT
MONIER Christelle	Expert
MORISSE François	CFDT
NOËL Philippe	Total
NORMAND Annie	DGPR - Barpi
PERCHE Vincent	DGPR - Barpi
PLANEIX Michèle	Expert
PRATS Franck	Ineris
PROVOST Pascal	Syctom
SUDRET Pascal	Air Liquide
THELLIER Sylvie	IRSN
THOMAS Rémy	Expert
TOLEDO Nicolas	Icsi
TOUPIN Mathias	BASF
WAXIN Raphaël	Total

Les rédacteurs

Mireille Jauffret, secrétaire de rédaction
Bernard Seytre, journaliste scientifique

Les relecteurs scientifiques

François Daniellou, Icsi-Foncsi

Les instances de l'Icsi

COE : Conseil d'Orientation et d'Evaluation

Les coordinateurs de l'Icsi

Dounia Tazi et Jean-Michel Pesteil ont coordonné les différentes étapes de la discussion du groupe d'échange et de l'écriture du *Cahier*.

Sommaire

Introduction

Le besoin d'une approche globale de la maîtrise des risques majeurs

La nécessité d'un échange sur les éléments culturels liés à la maîtrise des risques majeurs lors de l'exploitation de systèmes techniques a été exprimée par plusieurs membres de l'Icsi, qu'ils soient industriels, donneurs d'ordre et sous-traitants, ou représentants d'organisations syndicales. On considère ici les systèmes techniques de fabrication, de transformation, de transport, les ouvrages et bâtiments qui sont susceptibles de générer des risques importants au-delà du personnel d'exploitation. À titre d'exemple : une explosion ou une rupture de confinement avec des victimes dans la population, la pollution massive d'une rivière détruisant la faune et la flore, le déraillement d'un train, ou encore l'effondrement d'un pont.

La maîtrise des risques des systèmes techniques correspond à un besoin vital des entreprises concernées par des risques d'accidents technologiques graves, c'est-à-dire des accidents qui auraient des conséquences inacceptables pour la population ou l'environnement. Les entreprises sous-traitantes sont également conscientes qu'elles ont un rôle important pour assurer la sécurité des systèmes techniques dans le cadre de leurs interventions (fonctionnement opérationnel ou maintenance). Or, elles sont souvent mal informées des risques d'accidents potentiellement graves, voire majeurs, liés aux systèmes sur lesquels elles interviennent et/ou ne font pas le lien avec leurs activités.

Ces dernières années, l'expertise sur ces questions s'est améliorée et approfondie. Les suites d'accidents technologiques graves ont permis d'en analyser et approfondir les causes, en particulier les facteurs humains et organisationnels, et l'expertise s'en est trouvée renforcée.

Les réglementations, plus exigeantes, ont contribué à progressivement complexifier les systèmes par le renforcement des lignes de défense. Les incidents sont plus rares et leur compréhension par les acteurs de terrain, plus délicate.

L'observation des grands accidents industriels montre des scénarios souvent très éloignés des études de danger théoriques. Le renforcement des exigences conduit souvent à la multiplication des règles et il devient d'autant plus difficile de gérer les situations imprévues.

Enfin, la sécurité industrielle progresse et les événements très graves sont heureusement très rares. Les opérateurs de terrain, qui constatent la multiplicité et l'apparente robustesse des lignes de défense et font le constat de l'absence d'événement majeur, peuvent considérer ces événements comme impossibles. On aboutit ainsi à une distanciation entre les opérateurs de terrain et la maîtrise de la sécurité des systèmes techniques. Si la pression de l'opinion publique pour renforcer la sécurité peut servir d'aiguillon, elle touche principalement la direction.

Toutes les industries se penchent depuis des années sur ces questions et les aspects techniques et les systèmes de management ont été, dans l'ensemble, très approfondis.

Divers organismes (CCPS, IOGP, AIChE, AIEA, WENRA, WANO et autres) proposent des analyses et recommandations d'ordre technique et organisationnel pour maîtriser la sécurité dans les grands secteurs industriels. En revanche, les analyses et recommandations transverses à l'ensemble des activités à risque majeur sont beaucoup plus rares. À noter une publication de l'OCDE (Process safety for directors), cependant difficilement exploitable par le terrain.

Pour développer cette réflexion, l'Icsi a décidé courant 2016 de mettre en place un groupe d'échange afin de dégager des principes et des pratiques applicables à tous les secteurs, pour garantir les lignes de défense contre l'accident majeur.

De manière plus globale, les travaux de l'Icsi entre 2016 et 2019 portent sur la prévention des accidents graves, mortels et technologiques majeurs. À cette occasion, de nombreuses ressources ont été développées. Vous en trouverez sur le site www.icsi-eu.org.

Le groupe d'échange

Le groupe d'échange « Culture de sécurité et sécurité des systèmes techniques » a été constitué avec des représentants des industriels de la chimie, de la pétrochimie, de l'énergie, du transport, des syndicats, d'instituts d'expertise et d'appui aux autorités de contrôle, de l'enseignement supérieur et de la recherche.

Le groupe s'est réuni une douzaine de fois. L'animation était assurée par l'Icsi avec la participation de plusieurs bénévoles, anciens cadres de l'industrie.

Dans le cadre fixé par le comité d'orientation et d'évaluation de l'Icsi (COE), le groupe s'est concentré dans un premier temps sur la sécurité des procédés industriels, puis l'exploitation de tout système technique : procédé industriel, moyens de transport, ouvrages d'art et BTP susceptibles de générer des risques majeurs pour la population ou l'environnement. L'ambition fixée est de fournir à toutes les parties prenantes, d'une part, un état des lieux des pratiques de maîtrise de la sécurité du système en exploitation et, d'autre part, des réflexions sur les méthodes à engager pour les améliorer.

Nous nous intéressons ici principalement à l'exploitation des systèmes, leur mise en service ou leur modification. On ne traitera pas de la conception initiale, même si on peut recommander d'intégrer dès la conception le point de vue de l'exploitant.

Très rapidement, les travaux du groupe se sont orientés vers la recherche des éléments de la culture de sécurité communs à toute activité à risques majeurs permettant de garantir la sécurité dans la durée. L'ambition était d'adopter la vision du terrain : comment faire pour que l'opérateur et l'équipe traitent avec la meilleure efficacité possible les actions nécessaires ou liées à la sécurité ?

Ce document n'aborde donc pas les questions techniques qui sont éminemment liées aux systèmes, ni les dispositions organisationnelles propres à chaque entreprise ou secteur d'activité. Nous aborderons seulement des processus organisationnels essentiels pour développer et entretenir des comportements individuels et collectifs adaptés aux enjeux.

Les réflexions qui suivent ne se focalisent pas sur les caractéristiques des systèmes techniques et des organisations concernés par les risques majeurs. Rappelons simplement ici quelques objectifs pour atteindre un bon niveau de sécurité :

- Une conception rigoureuse du système technique pour identifier et prévenir les risques majeurs pour le personnel, la population et l'environnement : identification des scénarios d'accidents, des lignes de défense et des exigences relatives aux systèmes et matériels de sécurité ;
- Une délimitation claire du domaine de fonctionnement en exploitation et un programme de surveillance et de maintenance qui permette de garantir la sécurité prévue lors de la conception ;
- Des consignes et modalités à mettre en œuvre en cas de fonctionnement dégradé ou d'incident, pour prévenir toute dérive et restaurer rapidement le niveau nominal de sécurité ;
- Des consignes et des modalités à mettre en œuvre en cas d'accident pour retrouver la maîtrise du système et limiter les conséquences pour l'environnement et la population ;
- Une définition claire des rôles et responsabilités dans les activités concernant la sécurité à tous les niveaux (préparation, mise en œuvre, retour d'expérience, contrôle et arbitrages) ;
- Une gestion des moyens et compétences (recrutement, formation) nécessaires en interne et en externe (sous-traitance).

La réflexion a été alimentée par trois types de présentations en séance de travail du groupe d'échange :

- Des témoignages de membres du groupe ou d'invités sur des pratiques de maîtrise du risque majeur ou des analyses ;
- Des études sur la sécurité des systèmes techniques (procédés industriels et moyens de transport principalement) ;

- Les comptes rendus des immersions d'un représentant de l'Icsi sur des sites industriels pour observer les pratiques et établir un échange avec les acteurs de terrain sur leurs problématiques de maîtrise du risque.

La priorité retenue : développer une conscience partagée du risque majeur

Le groupe d'échange a d'abord posé les constats généraux suivants sur le fonctionnement des organisations concernées :

- Le top management est principalement préoccupé par les indicateurs transverses de sécurité du personnel et de productivité, et insuffisamment par les indicateurs spécifiques à la sécurité des systèmes techniques. On note une focalisation assez fréquente de la hiérarchie sur le taux de fréquence des accidents du travail (Tf) qui est parfois le seul indicateur de pilotage pour la sécurité.
- Les équipes opérationnelles et les opérateurs sont principalement préoccupés par le bon fonctionnement des systèmes techniques à leur niveau et par les problèmes techniques quotidiens qui entravent ce fonctionnement.
- Les experts spécialistes de la sécurité des systèmes techniques sont préoccupés par la conformité réglementaire et la conception, mais sont assez éloignés de la réalité quotidienne du terrain. Les études amont sont souvent très techniques et parfois quasi confidentielles (scénario d'accident, conception des barrières), avec pour conséquence un déficit d'imaginaire en sécurité pour les autres acteurs.
- Le management local est généralement conscient des risques majeurs mais contraint par les problématiques d'exploitation courante du système technique et les injonctions du top management. Plus globalement, les arbitrages au quotidien n'intègrent pas suffisamment le risque majeur.
- Ne se produisant jamais ou rarement, l'accident majeur n'appartient pas à l'environnement quotidien des opérateurs, qui ont des difficultés à se représenter sa genèse et son arrivée dans le cadre des activités quotidiennes.
- Les opérateurs sont parfois les seuls à connaître les pratiques réelles.
- Les entreprises intervenantes souvent multisites ou multi-systèmes techniques, ne connaissent pas toujours bien le contexte local et les enjeux de sécurité du système.
- L'émergence du pilotage à distance des installations grâce à des salles de contrôles distantes et centralisées, ne risque-t-il pas de conduire à une moindre perception du risque majeur du fait de l'éloignement physique ?

On constate donc que les différents acteurs n'ont ni les mêmes priorités ni la même conscience du risque. Chacun gère ses préoccupations souvent très éloignées du risque majeur. Seuls certains experts sont focalisés sur ce sujet, mais surtout pour répondre aux « exigences administratives » et souvent sans prendre bien en compte les spécificités du terrain.

Il apparaît difficile de progresser significativement en matière de sécurité des systèmes techniques si on ne partage pas une même vision des enjeux et des moyens de maîtrise. Le groupe a conclu qu'il est nécessaire et prioritaire de construire une conscience partagée des risques majeurs par tous les acteurs, pour mener efficacement les actions conduisant à la maîtrise de ces risques.

Cet objectif de conscience partagée des risques est un premier pas vers la culture de sécurité intégrée qui conditionnera une bonne maîtrise des risques dans la durée. La *figure 1* représente les différents types de culture de sécurité. Si la culture fataliste est généralement dépassée, les cultures de sécurité des métiers (maintenance, exploitation de système ou conduite de procédé, logistique, ingénierie, etc.) et la culture managériale (injonction descendante) coexistent sans véritable synergie dans nombre d'entreprises. L'enjeu est bien de construire une culture intégrée, commune, qui s'appuie sur la conscience partagée des risques majeurs.

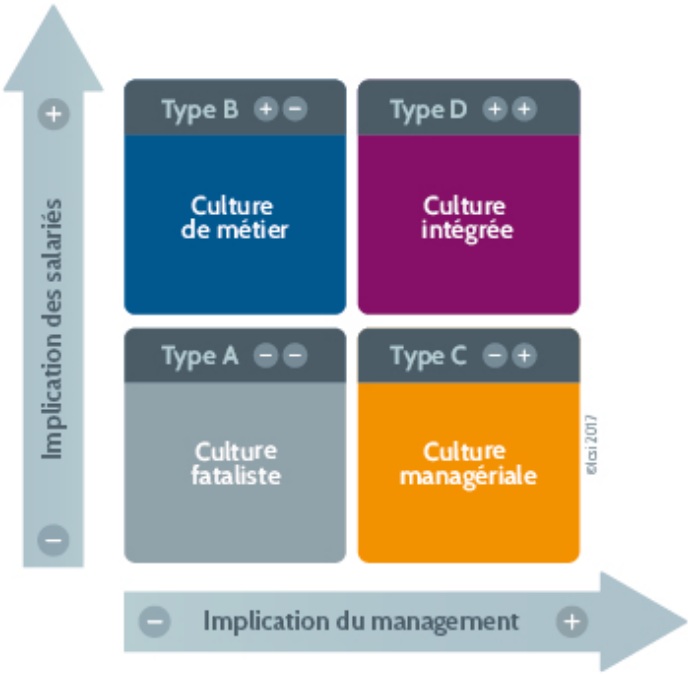


FIGURE 1 : *Différents types de culture de sécurité selon Marcel Simard*

La production du groupe d'échange

Le groupe d'échange s'est donné comme ambition de faire **un état de lieux des pratiques de maîtrise de la sécurité des systèmes techniques par l'équipe opérationnelle dans son environnement spécifique et des réflexions sur les méthodes à engager pour l'améliorer**. Il s'agissait de dégager des principes applicables à tous les secteurs d'activité, pour garantir les lignes de défense en place ou à définir contre l'accident majeur.

De quoi parle-t-on ?

La conscience partagée du risque majeur englobe la conscience du danger et la connaissance du rôle de chacun dans la gestion du risque. Par « **construire une conscience partagée des risques** », le groupe d'échange entend donc :

- ▷ Éviter la banalisation des risques majeurs ;
- ▷ Rendre visibles et prioriser les risques ;
- ▷ Rendre visibles les différentes composantes des barrières de défense, leur rôle et leur configuration courante ;
- ▷ Promouvoir une vision pluridisciplinaire, complémentaire et intégrée des risques majeurs aux différents métiers.

Par « **équipe opérationnelle** », le groupe d'échange entend : tout collectif de travail des phases d'exploitation, de maintenance et modification dont les réflexions, décisions et actions ont un effet direct ou indirect sur la sécurité des systèmes techniques.

Par « **environnement spécifique** », le groupe d'échange entend :

- ▷ L'environnement réglementaire ;
- ▷ Le contexte social ;
- ▷ Le secteur d'activité ;
- ▷ Le type d'organisation ;

- ▷ Les fonctions dans l'entreprise hors périmètre de la phase d'exploitation de maintenance ou de modification ;
- ▷ La configuration des lignes de défense actuelles.

Par **pratiques** le groupe d'échange entend :

- ▷ Les temps de réflexion individuels et collectifs ;
- ▷ Les décisions avec effet immédiat, différé, direct ou indirect ;
- ▷ Les actions intentionnelles ou non intentionnelles.

La *figure 2* représente la transformation qu'il faudrait opérer entre cette situation de vision éclatée, la plus courante aujourd'hui, et un modèle de prise en compte du risque majeur s'appuyant sur la conscience partagée du risque.

FIGURE 2 : *Pour une conscience partagée des risques majeurs*

Objet du document

Ce document fait partie d'un ensemble de supports issus des réunions du groupe d'échange « Culture de sécurité et sécurité des systèmes techniques ». Ces supports sont destinés à aider les entreprises à instaurer une conscience partagée des risques majeurs sur les sites d'exploitation et parmi tous les partenaires contribuant aux activités de leur structure.

Trois axes majeurs de réflexion ont été définis par le groupe d'échange pour développer cette conscience partagée :

- ▹ Les risques majeurs au cœur du pilotage et des processus ;
- ▹ L'appropriation des risques majeurs par l'équipe opérationnelle ;
- ▹ Les moments clés des animations sécurité.

Chacun de ces axes fait l'objet d'un support vidéo utilisable lors des animations sécurité en entreprise, que vous pourrez retrouver sur www.icsi-eu.org

Ce document n'est pas un guide méthodologique. Il vise seulement à donner quelques éclairages, quelques pistes de réflexion pour les entreprises concernées par le risque industriel majeur. Il s'intéresse principalement aux phases d'exploitation, de maintenance et de modification de systèmes techniques, quel que soit le secteur d'activité de l'entreprise, lorsqu'ils sont susceptibles de provoquer des accidents graves pour la population ou l'environnement.

Il ne s'intéresse pas aux risques liés aux postes de travail ni aux risques directement liés à la coactivité même si les situations à haut potentiel de gravité peuvent venir de chacun de ces segments, qui ont des zones de recouvrement

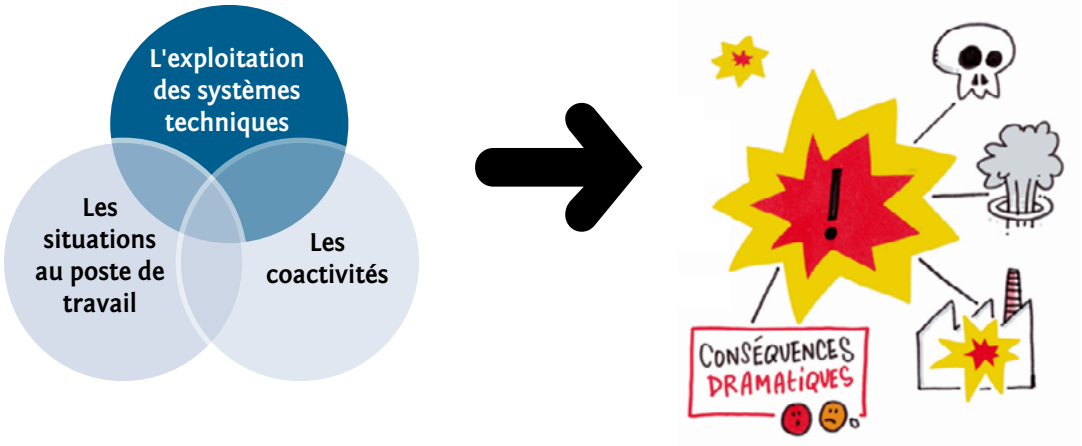


FIGURE 3 : *Ce document se focalise sur l'exploitation des systèmes techniques*

1

Placer les risques majeurs au cœur du pilotage des processus

1.1 Constats généraux

En l'absence d'un processus spécifique, la direction a tendance à se focaliser sur les objectifs corporate économiques, de production ou de respect réglementaire et normatif dont les conséquences sont les plus tangibles, plutôt que sur les impacts pour la sécurité des systèmes techniques, potentiellement plus difficiles à évaluer.

Il est difficile de mobiliser des ressources pour investir dans la sécurité car le retour sur investissement est mal évalué par les indicateurs de résultats classiques et quantitatifs. Les arbitrages relatifs à la sécurité des systèmes techniques nécessitent donc une approche spécifique qui ne prenne pas seulement en compte les données économiques ou des indicateurs généralistes de la sécurité au travail.

Les systèmes de management déclinés en processus peuvent avoir tendance à cloisonner les activités, chaque processus ayant ses objectifs d'optimisation et des indicateurs dédiés, sans mesurer ni prendre en compte les impacts sur les autres processus.

Les barrières de défense mises en place sont souvent la conséquence de la mise en conformité avec des réglementations, normes ou assurances. Elles sont rarement issues d'une réflexion sur une stratégie globale de prévention.

1.2 Faire vivre une stratégie de prévention des risques majeurs

Les risques « majeurs » correspondent à la combinaison d'événements qui peuvent conduire à des conséquences inacceptables pour la population et l'environnement, c'est-à-dire à des accidents « majeurs ».

Événement soudain et imprévu qui met en danger les salariés, les riverains d'un site et l'environnement, un accident majeur peut également compromettre la pérennité du site s'il entraîne un arrêt temporaire ou définitif de l'exploitation, voire même l'abandon d'activités industrielles similaires sur décision des pouvoirs publics.

FIGURE 4 : *Exemples de d'accidents majeurs*

1.2.1 Les barrières et leurs composantes

L'organisation doit définir et mettre en place un système de protection contre les risques majeurs basé sur des barrières destinées à éviter l'accident majeur ou limiter les conséquences potentielles d'un accident. Ce système comporte trois lignes de défense [1] :

- La prévention, pour empêcher l'exposition au danger ;
- La récupération, pour reprendre en main une situation à risque ;
- L'atténuation, pour limiter les conséquences de l'événement accidentel.

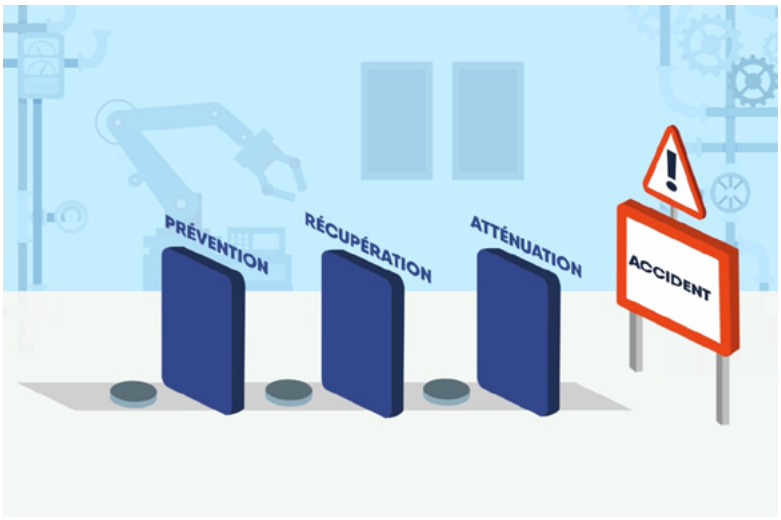


FIGURE 5 *: Les 3 types de lignes de défense : prévention, récupération, atténuation*

Ces trois lignes de défense sont autant de remparts qui protègent de l'accident. Elles sont constituées de barrières, elles-mêmes constituées de composantes :

- Techniques : l'ensemble des éléments matériels, dispositifs de sécurité ou système instrumenté de sécurité ;
- Organisationnelles : l'ensemble des processus et procédures qui permettent de gérer les situations courantes et exceptionnelles en situation d'urgence ;
- Humaines : l'ensemble des pratiques et comportements des membres de l'équipe opérationnelle qui permettent de gérer les situations risquées.

Ces trois composantes sont indissociables et doivent être conçues, évaluées et modifiées en cohérence.

1. Groupe d'échange de l'Icsi « Prévention des accidents graves et des accidents mortels » (2019). *Prévention des accidents graves et des accidents mortels. Les Cahiers de la sécurité industrielle*, n°2019-01. Institut pour une culture de sécurité industrielle, Toulouse, France. Gratuitement téléchargeable sur www.icsi-eu.org

FIGURE 6 : *Les composantes d'une ligne de défense*

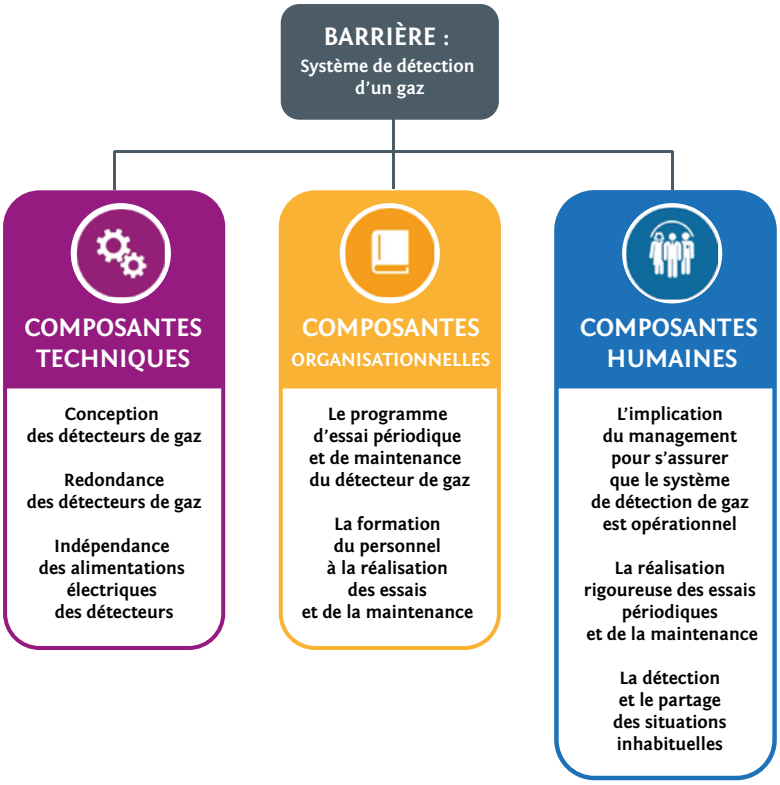


FIGURE 7 : *Exemple de composantes techniques, organisationnelles et humaines d'une barrière*

Techniques

- Appareils de détection avec alerte (par exemple, un détecteur de gaz) ;
- Mur de sécurité ;
- Enceinte de confinement ;
- Arrêt d'urgence ;
- Protections contre les surpressions ou la surchauffe ;
- Bassin de rétention ;
- Sprinklers, rideau d'eau ;
- Arrêts automatiques de sécurité ou automatismes de sécurité, interrompant l'évolution du procédé avant un accident si des conditions potentiellement dangereuses surviennent.

Organisationnelles

- Programme d'essai périodique des systèmes de sécurité ;
- Programme régulier d'entretien préventif des équipements, programme d'inspection (audits) sur le terrain des activités en cours, procédures d'exploitation détaillées ;
- Formation du personnel ;
- Procédures d'évacuation ;
- Plan d'urgence ;
- Programme d'exercices de sécurité ;
- Écoute des lanceurs d'alerte ;
- Ergonomie du poste de travail, organisation du travail.

Humaines

- Leadership du management ;
- Réalisation rigoureuse selon les consignes pour des tâches critiques ;
- Fiche réflexe ;
- Contrôle mutuel et vigilance partagée ;
- Autocontrôle ;
- Détection et partage de situations inhabituelles, etc.

FIGURE 8 : *Exemples non exhaustifs des différentes composantes de barrières.*

1.2.2 Faire vivre les lignes de défense

Mais au-delà de la conception et de l'exploitation des lignes de défense, des barrières et de leurs composantes, une des principales problématiques de la prévention du risque majeur est le maintien opérationnel et fonctionnel de celles-ci dans la durée.

Suivre, contrôler, maintenir et éventuellement modifier ou remplacer si besoin les composantes de chaque barrière est indispensable.

En d'autres termes, il faut faire vivre les 3 lignes de défense de sécurité même s'il n'est pas toujours facile d'avoir une information précise sur la configuration des barrières associées et de leurs composantes.

Enfin, les lignes de défense de sécurité ne sont pas définitives. Les modifications des systèmes techniques ou de leurs conditions d'exploitation, les analyses de risque (ou études de danger), l'expérience collective et la remontée d'information doivent permettre de les réinterroger et de les améliorer sans cesse.

Bonne pratique

Faire la photo de la maîtrise des risques majeurs

Des dispositions organisationnelles sont nécessaires pour une photographie aussi précise que possible de la maîtrise des risques majeurs : détection et traitement des écarts, suivi des indisponibilités et mesures compensatoires, traitement des tests périodiques, suivi des performances des matériels et systèmes, régularité des exercices et variations dans les scenarii, etc.

Connaître avec précision l'état de maîtrise des risques et la fiabilité des lignes de défense n'est pas facile. Les lignes de défense peuvent évoluer tout en restant silencieuses dans le fonctionnement courant et les dispositions organisationnelles tendent également à s'éroder avec le temps.

Par exemple, certains systèmes de sécurité sont au repos en fonctionnement normal et doivent pouvoir répondre à une sollicitation en cas d'incident, et des dégradations peuvent intervenir sans être visibles. Certaines dispositions organisationnelles peuvent devenir plus ou moins obsolètes du fait de l'évolution des pratiques et des comportements.

1.3 Focaliser la ligne managériale et la direction sur la maîtrise des risques majeurs

1.3.1 La nécessité d'indicateurs spécifiques

Il est difficile de réaliser une évaluation précise et exhaustive du niveau de maîtrise de la sécurité des systèmes techniques. Il est donc nécessaire de disposer d'indicateurs proactifs et spécifiques.

Le choix, la définition d'indicateurs pertinents dans le temps et légitimes n'est pas chose aisée. Ceux-ci peuvent avoir des limites ou générer des déviances.

Le choix des indicateurs est une étape importante. Ils devront porter sur les dimensions techniques, humaines et organisationnelles de la sécurité. Leur suivi et leur analyse permettront d'identifier des axes d'amélioration. Ils doivent être pertinents, mesurables et atteignables, pour ne pas provoquer un phénomène de refus. Ils doivent être définis en fonction des pratiques de l'industriel et communiqués à l'ensemble du personnel. Ils seront évalués et modifiés si nécessaire.

Exploitation

- Nombre de sollicitations des fonctions de sécurité (ou atteinte des limites du domaine de fonctionnement en sécurité) ;
- Nombre de déclenchements intempestifs ;
- Nombre de pertes de confinement ;
- Nombre de départs de feu ;
- Durée d'indisponibilité d'équipements (ou fonctions) de sécurité ;
- Nombre de shuntage de dispositifs de sécurité ;
- Nombre de situations où un dispositif de sécurité nécessaire n'a pas été mis en place ;
- Nombre de récupérations de situations à haut potentiel de gravité ;

Maintenance

- Nombre ou pourcentage de procédures de test de sécurité non effectuées à la date prévue ;
- Nombre ou pourcentage de fonctions de sécurité trouvées inopérantes lors de tests ou de revues périodiques ;
- Taux de réalisation de la maintenance préventive critique ;
- Coût de la maintenance curative/corrective critique.

FIGURE 9 : *Exemples d'indicateurs spécifiques pour la prévention des risques majeurs*

Managers

- Qualité des visites de sécurité : portent-elles sur des risques majeurs, des lignes de défense de sécurité et leurs composantes techniques, organisationnelles et humaines ?
- Comment les objectifs annuels d'évaluation individuels et collectifs prennent-ils en compte la sécurité des systèmes techniques ?
- Comment les managers monitorent-ils les perturbateurs récurrents ou occasionnels graves ?
- Comment sont organisés la remontée et le partage des situations à haut potentiel de gravité ?
- Quel est le budget consacré à l'entretien et à l'amélioration de la sécurité ?
- Quel est l'état d'avancement des programmes de renforcement de la sécurité ?

Opérationnels

- Qualité des briefings, réunions de coordination, « causeries » de sécurité : portent-ils sur le partage des risques majeurs, des lignes de défense de sécurité et leurs composantes techniques, organisationnelles et humaines ?
- Qualité des remontées d'information : quel pourcentage de remontées d'information touche à des activités sensibles (tâches critiques, lignes de défense de sécurité, etc.) ?
- Suivi des contraintes dans l'activité : empêche-t-il la réalisation prévue ?
- Pratiques réelles et les procédures prescrites : des échanges sont-ils organisés sur le sujet ? Existe-t-il un écart entre les deux ?

FIGURE 10 : *À la recherche d'indicateurs spécifiques, les bonnes questions à se poser selon les acteurs*

Au-delà de leur suivi, il est préconisé de faire évoluer les indicateurs si nécessaire, d'analyser les pistes d'amélioration, de communiquer, susciter les remontées d'information et de commenter les résultats auprès des équipes pour les sensibiliser au risque majeur.

1.3.2 Repérer les événements à haut potentiel de gravité

Les accidents majeurs sont extrêmement rares et le retour d'expérience qui en découle est donc limité mais les incidents courants d'exploitation révèlent des fragilités qu'il faut savoir exploiter.

Certains incidents d'exploitation peuvent être qualifiés de presqu'accidents parce qu'une ou plusieurs composantes de barrières faciles à identifier ont permis d'éviter la catastrophe. Ils sont généralement analysés. Mais de nombreux événements d'exploitation susceptibles de passer inaperçus pourraient être les initiateurs d'accidents graves. Savoir repérer et exploiter ces événements dits à haut potentiel de gravité permet de consolider ou de réinterroger les barrières existantes.

Bonne pratique

Suivre les composantes des barrières résiduelles

Lors des analyses sécurité des systèmes techniques, un suivi des composantes de barrières résiduelles est effectué selon la démarche suivante :

- Détection d'événements sécurité : les événements sont recensés et leurs causes analysées. Les conséquences réelles et potentielles sont évaluées.
- Analyse de la gravité potentielle : un classement est effectué en fonction de la gravité potentielle de l'événement en l'absence de barrières de sécurité, de la probabilité que la gravité maximale soit atteinte et du nombre de personnes potentiellement exposées.
- Identification et caractérisation des composantes des barrières résiduelles disponibles : le nombre de composantes disponibles dans l'enchaînement entre l'événement détecté et l'événement maximal est analysé. Moins il reste de barrières effectives, plus l'événement est potentiellement grave.

Ces indicateurs permettent de définir des zones de risque à surveiller. Les résultats de ce type d'analyse doivent être présentés et expliqués dans l'entreprise afin de renforcer l'impact des retours d'expérience et de la remontée d'information. Ils fournissent également à la direction des indications sur les points à améliorer en matière de sécurité.

1.4 Processus-clés

1.4.1 Processus d'arbitrage et sécurité des systèmes techniques

Les arbitrages relatifs à la sécurité des systèmes techniques nécessitent une approche spécifique qui ne prenne pas seulement en compte les données économiques.

Les autorités de régulation et le public sont un garde-fou, tout comme la conviction des managers et du personnel qu'une entreprise performante économiquement est une entreprise qui maîtrise ses risques majeurs.

Néanmoins, la sécurité a un coût et il est légitime de s'interroger sur l'efficacité des investissements dans la sécurité. Certains industriels ont développé des approches coût-bénéfice utiles dans la relation avec les autorités de contrôle.

Bonne pratique

Mettre en place un processus d'arbitrage

La maîtrise des risques majeurs au-delà d'une injonction réglementaire doit être une démarche volontariste. Certaines organisations s'assurent que :

- Le processus d'arbitrage inclut systématiquement une analyse des impacts sur la sécurité des systèmes techniques à court, moyen et long terme ;
- Le nombre de fois où l'avis du service sécurité n'a pas été suivi est un indicateur du tableau de bord de la direction : la direction vérifie également qu'une analyse à froid de ces cas est systématiquement réalisée ;
- Un investissement et des ressources appropriées sont dédiés à la sécurité des systèmes techniques.

1.4.2 Analyse des risques a priori

Simulation avant mise en exploitation

Réaliser des simulations avant mise en exploitation

Bonne pratique

En plus des simulations techniques, des entreprises réalisent avant le premier démarrage des simulations organisationnelles intégrant notamment les opérateurs d'exploitation, de maintenance et d'intervention d'urgence. Ces simulations visent à s'assurer que l'organisation prévue permette le fonctionnement des installations en situation normale, dégradée et accidentelle.

Vérification avant mise en fonctionnement

Avant la mise en service du système technique il est indispensable de s'assurer que les lignes de défense prévues sont bien opérationnelles.

Une fois l'installation fonctionnelle, la ligne managériale est responsable de l'entretien des lignes de défense de sécurité et de l'actualisation de l'analyse des risques pour prendre en compte les changements.

De même, avant la remise en service d'un dispositif de sécurité, il est nécessaire de vérifier le respect des performances requises.

Vérifier avant la mise en fonctionnement

Bonne pratique

Certaines entreprises mettent en place des *pré-startup safety review* (PSSR) qui permettent de vérifier si le matériel est conforme aux procédures de management de la sécurité avant le démarrage ou le redémarrage d'une exploitation. La mise en route est reportée si l'un des points de contrôle met en lumière un risque. Une mise en conformité est alors effectuée, à la suite de laquelle une nouvelle enquête PSSR est organisée.

1.4.3 Analyse de risque avant intervention

De nombreuses activités en exploitation sont susceptibles de générer des évolutions non souhaitées du procédé : sortie du domaine de fonctionnement autorisé, altération des performances des dispositifs de sécurité ou indisponibilité de matériel important pour la sécurité.

Dans certains secteurs d'activité, l'analyse de risque préalable à une intervention de maintenance ou une manœuvre d'exploitation est systématique.

1.4.4 Coconstruire une culture juste et équitable[2]

La plupart des événements ont une composante humaine et les opérateurs concernés peuvent, individuellement ou collectivement, avoir tendance à éviter la remontée d'information pour se protéger d'une mise en cause éventuelle.

Certaines entreprises ont choisi de mettre en place les conditions nécessaires pour promouvoir la confiance, l'empathie et la coopération entre leurs membres. Chacun se sent libre, légitime et soutenu pour alerter, informer, analyser et réagir en toute transparence.

Parmi ces conditions, il est indispensable que les employés disposent de garanties comme le droit de se tromper, ou que la responsabilité des écarts aux règles ne soit pas systématiquement imputée aux employés. Les causes profondes de tels écarts doivent être systématiquement recherchées.

2. Groupe de travail de l'Icsi « Culture de sécurité » (2017). *La culture de sécurité : comprendre pour agir. Les Cahiers de la sécurité industrielle*, n°2017-01, Institut pour une culture de sécurité industrielle, Toulouse, France. Gratuitement téléchargeable sur www.icsi-eu.org

Bonne pratique

Co-construire une culture juste et équitable

Certaines entreprises s'assurent que la réaction du management est homogène et prévisible, pour assurer la confiance et la liberté de parole. Elles ont développé une politique acceptée et partagée de traitement managérial des événements non souhaitables. Le traitement des causes profondes des écarts a été privilégié par rapport au traitement purement individuel. La reconnaissance a été développée et les sanctions éventuelles sont aujourd'hui perçues comme justes et équitables. Ceci repose sur une politique et des pratiques managériales acceptées et partagées autour :

- D'une vision claire de ce qui doit être remonté, traité et partagé en priorité ;
- D'une politique de reconnaissance positive des signalements et des bonnes pratiques ;
- De la définition partagée d'une ligne rouge entre l'acceptable et l'inacceptable ;
- De la réaction appropriée et homogène de l'encadrement face aux écarts.

Mettre en place une culture juste est un processus au cours duquel les acteurs de l'organisation se mettent d'accord pour définir les comportements qui doivent être reconnus et valorisés, ou au contraire les comportements qui ne sont pas acceptables et qui seront donc sanctionnés.

Bonne pratique

Analyser les écarts

Dans cette organisation tout écart technique ou erreur humaine est analysé selon une approche en cinq étapes :

- Recueil des faits ;
- Caractérisation et analyse de l'écart (analyse des causes profondes) ;
- Évaluation : l'écart est-il acceptable ou non ? Quelle réponse juste et équitable ?
- Prendre des mesures adaptées : décisions à prendre pour que l'écart ne soit pas reproduit ;
- Retour à l'ensemble des acteurs : partager l'événement, les enseignements avec tous les opérateurs et revenir sur leur rôle, notamment pour leur montrer ce qu'ils ont évité ou ce à quoi ils ont contribué.

De bonnes pratiques en la matière auront tendance à mettre les salariés en confiance. À l'inverse, une sanction arbitraire ou un manque de reconnaissance inciteront à la défiance.

Le premier pas vers une culture juste et équitable consiste à reconnaître et à accepter le droit à l'erreur.

1.4.5 Développer une culture d'apprentissage qui utilise la remontée d'information, le REX, l'analyse d'événement et la formation

Détection des écarts et remontée des bonnes informations

Nombre d'organisations ont mis en place des systèmes de remontée d'information dont l'efficience pour la maîtrise des risques majeurs est aujourd'hui discutée. Ces systèmes sont souvent engorgés par des remontées disparates et dont la pertinence par rapport aux risques majeurs n'est pas évidente. Le traitement de toutes les remontées et le retour vers les personnes qui les ont détectées devient alors impossible et les salariés finissent par renoncer à remonter des anomalies, écarts ou situations inhabituelles.

Une piste est que les opérateurs soient formés à la détection et à la caractérisation des écarts et capables de repérer ceux qui concernent les composantes des barrières de défense relatives à l'accident majeur.

FIGURE 11 : *Échanger autour des événements à haut potentiel de gravité*

Les obstacles rencontrés à l'efficacité des remontées sont :

- ▷ Le manque de vision globale des dispositions de sécurité ;
- ▷ La crainte de sanction lorsque le salarié remonte des anomalies qui pourraient lui être imputées ;
- ▷ Les écarts qui se creusent parfois lentement entre les pratiques réelles et les modes d'action prescrits.

Exemple

Témoignage : remonter les situations à haut potentiel de gravité

« Après être passé par une phase quantitative où nous demandions à chaque personne de remonter deux situations dangereuses par mois, nous avons changé de focale. Ce qui nous intéresse le plus, ce sont les situations dangereuses à haut potentiel. Nous incitons nos salariés à remonter avant tout les situations qui peuvent mener à des accidents majeurs.

Par exemple, un dispositif technique de sécurité qui n'a pas fonctionné lors d'un test, un programme de maintenance préventive qui prend du retard, ou encore une tâche critique qui a été réalisée alors qu'une des personnes de l'équipe intervenante n'était pas en état de le faire. Et ça fonctionne. Ils y trouvent beaucoup plus de sens et nous nous engageons à leur faire un retour sur la prise en compte de cette remontée dans les délais les plus brefs. »

Les remontées d'information des opérateurs sont déterminantes pour une bonne maîtrise des risques. Le retour d'expérience doit s'inscrire dans le contexte de culture juste évoqué plus haut, afin de ne pas biaiser la phase de collecte d'informations. L'organisation doit encourager le signalement de toute anomalie, tout écart par rapport à un référentiel d'exigences et toute situation inhabituelle.

Leur analyse et leur traitement sont primordiaux pour le bon fonctionnement des lignes de défense de sécurité à tous les niveaux et le retour vers les opérateurs contribue à entretenir la vigilance et le signalement des écarts.

Bonne pratique

Traiter prioritairement les remontées en lien avec les risques majeurs

Les remontées d'information en lien avec les risques majeurs sont traitées prioritairement.

Les procédures sont adaptées selon les remontées d'information, afin de toujours être en phase avec le fonctionnement quotidien de l'entreprise. L'objectif recherché est que les procédures soient opérationnelles, efficaces sans entrer en contradiction, et compréhensibles par tous.

Exemple

Exemples d'indicateurs sur la remontée d'information

- Délai de traitement : délai moyen, minimum et maximum entre une remontée d'information et le retour vers celui qui l'a remontée ;
- Rapport entre le nombre de remontées spontanées et le nombre total de dysfonctionnements.

L'analyse des événements

L'analyse des événements est un formidable levier pour comprendre et apprendre sur la maîtrise des risques majeurs, à condition de se doter des moyens pour accéder aux causes profondes et traiter celles-ci.

Bonne pratique

Réduire les transgressions de procédures

« Il faut traiter ce qui conduit à une transgression plutôt que la transgression elle-même », telle est la conclusion d'une étude menée par un bureau d'analyse sur les causes profondes des transgressions de procédures.

On est souvent focalisé sur le geste final, or la sécurité est assurée par une succession et une synchronisation d'opérations et de composantes de barrières de défense. L'ensemble du système doit être questionné.

Pour réduire les transgressions de procédures, il est important de :

- Maintenir la cohérence d'ensemble du référentiel documentaire ;
- S'assurer de la pertinence intrinsèque des procédures ;
- Cadrer, légitimer et accompagner l'usage des procédures.

Bien sûr, la participation des équipes opérationnelles à la rédaction et la mise à jour des procédures est nécessaire pour qu'elles soient lisibles et compréhensibles, avec un bon niveau de guidage, et adaptées aux situations afin que l'opérateur leur fasse confiance. Mais la procédure ne fait pas tout. Il faut mettre en place des lignes de défense complémentaires pour des échanges apaisés entre la hiérarchie et les opérateurs.

La concertation doit être forte entre les deux parties pour respecter les procédures, travailler dans de bonnes conditions, pour le bon fonctionnement de l'entreprise. C'est une façon de viser l'atteinte concertée des objectifs multiples inhérents à l'exploitation des installations industrielles dans des conditions acceptables pour l'individu, l'équipe et l'entreprise.

Exemple

Exemples d'indicateurs sur la qualité du retour d'expérience

- Pourcentage d'événements à haut potentiel pour lesquels une analyse des causes profondes a été réalisée dans un délai de moins de trois mois ;
- Pourcentage de causes profondes identifiées dans les analyses qui ont été traitées dans un délai de 12 mois.

Le retour d'expérience

Le retour d'expérience est un processus clé de la sécurité des systèmes techniques et la base de son amélioration continue.

La mise en place des retours d'expérience suscite une attention commune à la maîtrise des systèmes techniques, à des fins pédagogiques. Mais le retour d'expérience pourrait être mal perçu et tout son potentiel ne serait pas valorisé si on se limitait à l'exploitation des échecs. Pour être complets, les retours d'expérience ne doivent pas présenter uniquement des incidents mais aussi des bonnes pratiques afin qu'elles puissent être analysées et développées sur tous les postes d'un site ou sur d'autres sites d'une même entreprise.

Il est également important d'analyser et de partager les situations à haut potentiel de gravité.

p. 49
Annexe 4

Organiser la formation : Quoi ? Pour qui ? Quels objectifs ? Quels contenus ? [3]

La formation est nécessaire à la maîtrise des risques majeurs que ce soit pour développer :

- ▷ Les compétences de conduite, de surveillance ou de maintenance des installations ;
- ▷ La connaissance des lignes de défense (barrières et leurs composantes) ;
- ▷ La compréhension du pourquoi des procédures.

Aujourd'hui, nombre d'organisations constatent que leur processus de formation n'est pas toujours relié à la sécurité du système technique. Les équipes opérationnelles reçoivent trop souvent, d'un côté, des formations techniques et, de l'autre, des formations en sécurité, sans que les liens ne soient établis. Or, l'objectif principal est qu'un bon professionnel soit un professionnel qui travaille en sécurité.

La compétence sécurité des systèmes techniques est un volet des compétences requises pour l'emploi, qui repose sur un maillage de connaissances diverses, d'expériences, de savoir-faire et de savoir-être. Ce besoin doit être analysé pour en déduire les actions de formation théorique, de mise en situation ou de compagnonnage adaptées au profil individuel et à l'emploi.

L'objet étant la prévention de situations hypothétiques, donc éloignées de l'activité quotidienne, les connaissances et le savoir-faire peuvent rapidement s'estomper. Aussi, il est indispensable de prévoir des actions de formation ou des exercices de simulation périodiques pour entretenir les compétences dans la durée.

Exemple

Exemple d'indicateurs sur la formation

- ▷ Pourcentage des formations techniques professionnalisantes dont la sécurité du système technique est partie intégrante ;
- ▷ Taux d'échec lors des contrôles de connaissances en formation ou lors des exercices de simulation.

1.4.6 L'importance des processus transverses : recrutement, achat et contrats

Ces processus ne sont généralement pas ou peu intuitivement reliés à la sécurité des systèmes techniques. Ils sont pourtant incontournables pour une bonne maîtrise des risques majeurs

Le processus de recrutement, souvent inclus dans les prérogatives des responsables ressources humaines, ou les processus achats, parfois sous la responsabilité d'une entité externe à l'unité opérationnelle, contribuent inévitablement à la sécurité des systèmes techniques. Les enjeux de sécurité doivent donc être pris en compte dans leur conception et leur pilotage.

Exemple

Exemples d'indicateurs sur le recrutement, les achats et les contrats

- ▷ Évaluation de l'appétence pour la sécurité, de l'attitude interrogative ou de la démarche rigoureuse et prudente lors des recrutements ou des entretiens individuels ;
- ▷ Prise en compte de la maintenabilité et des performances sécurité sur le long terme des équipements achetés ;
- ▷ Pourcentage de prestataires retenus alors qu'ils n'offraient pas les meilleures garanties de compétence en termes de sécurité des systèmes techniques.

3. Groupe scientifique d'analyse stratégique de la Foncsi (2018). *La sécurité, une affaire de professionnels? Intégrer la sécurité aux compétences professionnelles. Les Cahiers de la sécurité industrielle*, n°2018-02, Fondation pour une culture de sécurité industrielle, Toulouse, France. Gratuitement téléchargeable sur www.foncsi.org

1.4.7 Maîtrise des activités sous-traitées[4]

p. 51
Annexe 5

La ligne managériale ne doit pas négliger l'importance de la sécurité dans un contexte de sous-traitance. Au-delà des garanties de compétence technique, de connaissance du système technique et de ses risques et de savoir-faire, le partage d'informations est indispensable entre le donneur d'ordre, garant de la sécurité du système, et le sous-traitant, garant de la sécurité et de la qualité des opérations. Les deux parties doivent partager une même vision des risques majeurs, des lignes de défense de sécurité, des principaux éléments pouvant affaiblir ces lignes de défense et des mécanismes à mettre en place en cas d'incident sur l'exploitation.

Le donneur d'ordre doit conserver les moyens de contrôler la bonne réalisation des interventions et de s'assurer que les écarts éventuels soient correctement instruits. Et il doit bien sûr s'assurer de la mise en place des conditions pour que les sous-traitants interviennent en toute sécurité, pour tous les personnels comme pour la maîtrise du système.

1.4.8 Maîtrise des changements

Toute modification de l'organisation de l'exploitation ou d'un procédé doit être prise en compte, et les impacts identifiés. L'équipe managériale doit vérifier que les nouvelles conditions d'exploitation garantissent la sécurité, notamment que les différentes composantes des lignes de défense préexistantes, a priori non concernées par les évolutions ne sont pas involontairement affectées. Une analyse de risques, voire une nouvelle étude de dangers, doivent être envisagées, qu'il s'agisse d'une adaptation de procédure, d'un changement de matériel ou d'une évolution des équipes opérationnelles.

Analyser les impacts des changements sur la sécurité

Bonne pratique

Lors de tout changement, une analyse des impacts potentiels sur la sécurité est réalisée. Si l'impact potentiel du changement sur la sécurité est considéré comme conséquent, une analyse approfondie des impacts organisationnels et humains est alors réalisée par des spécialistes des facteurs humains et organisationnels.

1.5 Recommandations

Chaque décision, qu'elle ait un rapport direct ou non avec la sécurité des systèmes techniques, peut avoir une incidence sur les lignes de défense de sécurité. Afin de pérenniser la sécurité de l'exploitation d'un système, il est nécessaire de s'accorder sur la place de la sécurité dans les arbitrages et de replacer la maîtrise des risques majeurs au cœur du pilotage des processus.

Pour faire vivre le système de prévention des risques majeurs :

- Mettre en évidence les barrières de défense contre l'accident majeur, constituées de composantes techniques organisationnelles et humaines ;
- Évaluer (suivre, tester, réinterroger) et entretenir les barrières dans la durée.

Pour focaliser la ligne managériale et la direction sur la maîtrise des risques majeurs :

- Disposer d'indicateurs spécifiques à la sécurité du système technique à maîtriser, qui soient pertinents, partagés et légitimes et des objectifs associés ;
- Avoir un suivi spécifique de la surveillance et l'entretien des composantes des barrières techniques, organisationnelles ou humaines.

4. Groupe d'échange de l'Icsi « Prévention des accidents graves et des accidents mortels » (2019). *Prévention des accidents graves et des accidents mortels. Les Cahiers de la sécurité industrielle*, n°2019-01. Institut pour une culture de sécurité industrielle, Toulouse, France. Gratuitement téléchargeable sur www.icsi-eu.org

Groupe de travail de la Foncsi « Relations contractuelles équilibrées » (2018). *Partages des modèles de sécurité entre donneurs d'ordres et entreprises intervenante. Les Cahiers de la sécurité industrielle*, n°2018-05, Fondation pour une culture de sécurité industrielle, Toulouse, France. Gratuitement téléchargeable sur www.foncsi.org

Pour centrer le pilotage sur la maîtrise des risques majeurs ;

- Avoir, dans tous les domaines de gestion, des processus d'arbitrage intégrant systématiquement une analyse d'impact sur la sécurité des systèmes techniques à moyen et long terme ;
- Prendre en compte dans la définition et le pilotage des processus support (RH, achats, etc.) les enjeux de sécurité du système technique ;
- Développer une culture juste et équitable pour que les personnes se sentent libres, légitimes et soutenues pour alerter, informer, analyser les événements en toute transparence ;
- Développer une culture d'apprentissage qui utilise la remontée d'information, le retour d'expérience, l'analyse d'événement et la formation ;
- Exploiter au mieux tous les événements d'exploitation : signalement et traitement systématique, identification des événements à haut potentiel de gravité et vérification des lignes de défense résiduelles, analyse et traitement des causes profondes. Repérer les événements positifs pour pérenniser et étendre les bonnes pratiques ;
- Concevoir la formation dans sa globalité et garantir les compétences dans la durée.

Pour maîtriser l'impact des changements sur les lignes de défense sécurité des systèmes techniques, il faut analyser, gérer et accompagner les impacts des changements techniques et organisationnels, sans oublier de prendre en compte le risque de déstabilisation des barrières existantes. La digitalisation croissante, la dématérialisation et le pilotage à distance des installations sont à considérer avec la plus grande prudence pour s'assurer que les impacts de ces changements sont maîtrisés.

2

Identification et appropriation des risques majeurs par l'équipe opérationnelle

2.1 Constats généraux

On s'intéresse ici à des événements très rares que les équipes opérationnelles ne peuvent naturellement se représenter car ils sont très éloignés des situations quotidiennes ou même des incidents courants d'exploitation.

De plus, même si le danger est plus ou moins connu, l'accident majeur est souvent considéré non seulement comme improbable mais souvent comme impossible, car :

- Plus la robustesse de la conception inspire confiance plus il est difficile de s'attendre au pire et donc de s'y préparer ;
- Avec une fiabilité technique vérifiée dans le fonctionnement quotidien, la confiance dans l'outil se renforce et la vigilance s'estompe.

Paradoxalement, la capacité de réaction face à une dérive du procédé vers un accident majeur est plus difficile à entretenir pour les systèmes techniques les plus évolués :

- Plus un process, un équipement ou un ouvrage est fiabilisé et stabilisé, moins l'opérateur est confronté à la survenue de situations perturbées, et plus il aura de difficultés à réagir face à l'imprévu ;
- Plus le pilotage à distance et l'automatisation sont renforcés, plus l'opérateur va perdre la capacité de maîtriser le système (perte de capacité de détection de l'évolution des paramètres du système, diminution de la perception de la réalité de fonctionnement de procédés complexes) et plus le risque de perte d'expertise pour rattraper les situations perturbées est élevé.

2.2 Connaissance des risques majeurs, scénarios majeurs et lignes de défense de sécurité

La conscience partagée des risques majeurs et la connaissance des moyens de les prévenir sont un enjeu prépondérant de la maîtrise des risques.

Les opérateurs ont parfois du mal à situer leurs pratiques dans l'ensemble des dispositions garantissant la sécurité des systèmes techniques.

Pour assurer une sécurité collective, l'organisation doit mettre en place des dispositifs permettant aux opérateurs de connaître les principaux scénarios conduisant aux accidents majeurs et détectant les situations qui pourraient y conduire. Ils doivent pouvoir imaginer ce qu'il peut arriver de pire et combien de barrières de sécurité séparent un événement de l'accident majeur. Ils doivent également connaître leur rôle dans la sécurité des systèmes techniques.

Des organisations ont développé des modalités pour partager cette conscience des risques majeurs, en particulier :

- Des espaces où les accidents les plus graves de l'organisation ou du secteur d'activité sont partagés ;
- Le partage et l'enrichissement des scenarii majorants avec les équipes opérationnelles ;
- Les exercices et la formation aux scénarios d'accidents par la simulation.

2.2.1 L'importance des récits

Des visites d'usine ont constaté que l'accident majeur est trop éloigné de la réalité du terrain pour être une préoccupation naturelle des opérateurs. Les opérateurs interrogés sont concentrés sur le bon fonctionnement du système technique, sur les problèmes qui entravent ce fonctionnement et sur les actions pour régler ces problèmes techniques.

FIGURE 12 : *Quand le quotidien éloigne des risques majeurs*

Bonne pratique

Valoriser les récits et l'analyse collective d'événements

La loi du « mort-kilomètre », vous connaissez ? Elle évoque le fait que plus un événement est distant de nous, moins il éveille l'attention. Pour la conscience des risques importants, c'est pareil, alors il importe de faire parler « les anciens », ceux qui ont vécu des situations de catastrophe (réelle ou évitée), qui sauront raconter, avec leurs mots, mieux que des études. Cela permet de créer une mémoire de ce qui est arrivé, une proximité et donc une réalité.

Les personnes qui ont vécu des accidents graves les gardent en mémoire et ce sont surtout elles qui les partagent lorsqu'un espace y est dédié, ou spontanément lorsqu'un événement précurseur leur rappelle ce qu'elles ont vécu.

Aussi, il apparaît important de partager la chronologie et les enseignements des accidents majeurs survenus sur d'autres sites d'exploitation, partout dans le monde, sur des systèmes techniques similaires.

2.2.2 La connaissance des scénarios majorants, les composantes des lignes de défense associées et leurs fragilités

Les études de danger

Les études de danger sont trop souvent le « pré carré » de spécialistes dans la relation avec l'autorité de régulation du secteur.

Les scénarios majorants tels que décrits dans les études de danger sont évoqués, voire étudiés lors des formations mais globalement de façon descendante et théorique. Ils font rarement l'objet de discussions et d'échanges avec les équipes opérationnelles.

FIGURE 13 : *Souvent les études de danger, c'est ça*

Faire des équipes opérationnelles et prestataires un public destinataire, voire un acteur, des études de danger et analyses de risque

Bonne pratique

Montrez-leur que les études de danger ne sont pas qu'un lourd dossier réglementaire, donnez vie aux analyses ! Faites s'exprimer les personnes sur les situations à risque qu'elles ont rencontrées, demandez-leur leur avis sur l'état des barrières de défense, dialoguez sur les perturbateurs, les conséquences imaginées… Profitez de la revue périodique des HAZOPs pour faire participer les équipes opérationnelles et partager les scénarios d'accidents.

Pour vous aider, vous pouvez utiliser la technique de visualisation des scénarios d'accident à l'aide des « nœuds papillons ».

p. 43
Annexe 1

FIGURE 14 : *Faire vivre les études de danger pour sensibiliser les équipes opérationnelles*

Mettre en place des ateliers « culture & pratiques »

Bonne pratique

Réunissez des opérateurs et prestataires 2h par jour pendant 1 semaine et favorisez l'échange autour des situations dangereuses, des perturbateurs qui peuvent menacer les barrières dont ils se servent, de leurs idées pour améliorer le contrôle et le maintien de ces barrières. La clé du succès : à l'issue de la semaine, ils font des propositions concrètes d'aménagements, à mettre en place à leur niveau.

p. 45
Annexe 2

Les exercices/formations par simulation

Les exercices de simulation sont un bon outil pour se représenter les risques, nos gestes, décisions et leurs conséquences.

Simuler les phénomènes dangereux et leurs conséquences… en toute sécurité

Bonne pratique

Proposez des entraînements avec des exercices de simulation qui permettent la visualisation des conséquences d'un accident majeur. Par exemple : une explosion, une pollution massive ou le déraillement d'un train. Le débriefing, y compris émotionnel, est riche et favorise le développement d'une conscience des risques majeurs.

Les simulations les plus abouties intègrent les différentes phases d'activité y compris arrêt, redémarrage ou phase transitoire et situations incidentelles ou accidentelles. Ces simulations intègrent notamment les équipes de maintenance et de gestion technique ou administrative afin qu'elles soient imprégnées des risques et comprennent l'intérêt de mettre en œuvre les dispositifs de sécurisation et d'évacuation. Ces simulations prévoient des cas particuliers. Par exemple : un des opérateurs est malade et non remplacé, un ou plusieurs capteurs tombent en panne ou donnent des valeurs erronées, etc.

D'autres formes de simulation permettent de travailler sur les interactions/coopérations d'un collectif de travail. Le Crew Ressources Management (CRM), formation de groupe d'abord utilisée pour les équipages des avions, ainsi que les simulations grandeur réelle permettent les interactions avec les partenaires externes de la gestion de crise.

2.3 Assumer sa responsabilité et jouer son rôle en sécurité des systèmes techniques

Afin de garantir la sécurité des systèmes techniques, chaque personne doit être consciente qu'à son niveau, elle a une responsabilité et un impact possible sur la sécurité du système qu'elle exploite. Chacun doit situer sa responsabilité pour surveiller, entretenir, détecter les processus de fragilisation des composantes des barrières constituant les trois lignes de défense de sécurité et s'assurer que les barrières sont fonctionnelles.

Sur le terrain, la conscience partagée des risques majeurs se traduit par l'identification et le partage de bonnes pratiques, et une connaissance commune des installations et des activités sensibles pour la sécurité.

2.3.1 Être rigoureux dans la réalisation des tâches critiques

Connaître son rôle et ses responsabilités permet de maintenir les barrières de sécurité en place et fonctionnelles, surtout lors de la réalisation des tâches critiques, opérations susceptibles d'avoir un impact sur la sécurité du système technique. Les tâches critiques peuvent concerner tous types d'opérations : production, surveillance, nettoyage, maintenance, chargement ou transfert de matériel, traitement des déchets, etc. Elles constituent des points de fragilité si un incident se produit lors de leur réalisation. Être conscient de ce qui peut fragiliser la rigueur dans la réalisation des tâches critiques, permet de se poser la question de son impact sur la sécurité du système et de mettre en place des dispositions pour minimiser l'impact (alerte, récupération, etc.).

Développer les pratiques de fiabilité humaine

p. 55 Annexe 6

Bonne pratique

Les tâches critiques sont clairement identifiées et connues des personnes qui en ont la charge ou qui peuvent avoir un impact sur leur déroulement. Les procédures écrites et les modalités pour les accomplir font l'objet d'une attention particulière et prennent en compte les remontées d'information des équipes opérationnelles pour être mises à jour. L'équipe opérationnelle dispose d'un temps de préparation et d'appropriation dédié aux tâches à réaliser. L'attitude interrogative, la démarche rigoureuse et prudente sont valorisées et des pratiques de fiabilité humaine sont développées.

Exemples de pratiques de fiabilité humaine :

- pré-job Briefing ;

- Minute d'arrêt ;
- Communication sécurisée ;
- Autocontrôle ;
- Débriefing ;
- Contrôle croisé.

2.3.2 Jouer son rôle en cas de situation accidentelle

Les situations d'urgence doivent être appréhendées comme telles sur le terrain pour rapidement mettre en place les réponses adaptées (plans d'urgence). Les situations ou critères déclenchant la mise en **œuvre** des plans d'urgence doivent être définis et communiqués aux équipes opérationnelles (types d'alarme, seuils d'alerte, conséquences potentielles, etc.). La notion d'urgence doit donc être « **étalonnée** » **et partagée par tous.**

De même, l'organisation doit mettre en place les conditions pour que la réaction attendue en cas d'événement majeur soit connue et partagée. Chaque acteur doit être préparé à tenir son rôle en situation d'urgence, rôle parfois sans rapport avec l'activité quotidienne. Des fiches réflexes peuvent se révéler nécessaires. L'entraînement reste indispensable pour développer les capacités de récupération des opérateurs dans des situations variées plus ou moins cadrées.

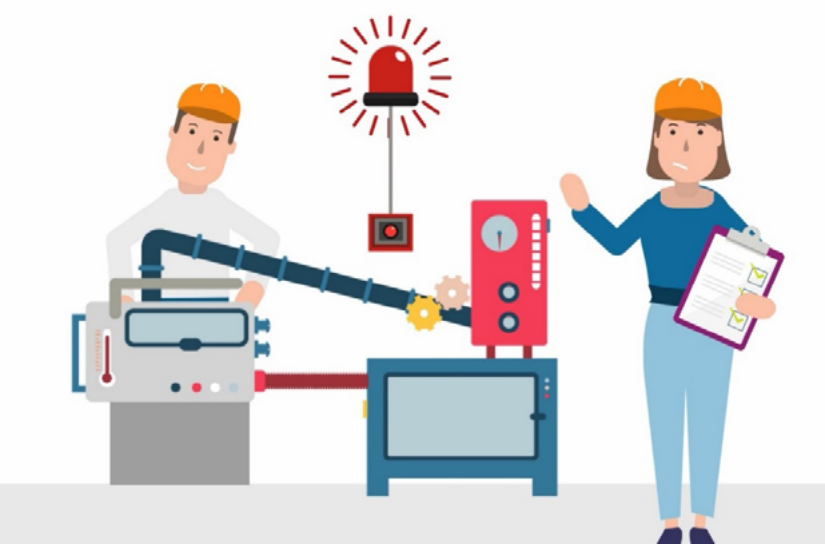


FIGURE 15 : *Réaliser des exercices de simulation permet de se préparer en cas de situation accidentelle*

Même pour les opérateurs qui n'ont pas de rôle déterminant dans la gestion accidentelle, les simulations à grande échelle sont l'occasion de rappeler et de s'entraîner sur les cinq points indispensables (pas plus) pour sécuriser son espace de travail et évacuer en toute sérénité.

2.3.3 Développer la vigilance partagée

Les programmes de vigilance partagée basés sur le devoir d'intervenir en cas de situation dangereuse se sont développés ces dernières années et d'abord au regard du risque d'accident corporel. Pourtant, ils peinent à s'ancrer dans les pratiques quotidiennes. Parmi les raisons invoquées : l'« **injonction** » **à intervenir**, alors que les personnes ne se sentent pas forcément légitimes à le faire ou ne savent pas quelle posture adopter.

La vigilance partagée a toute sa place dans la prévention du risque d'accident majeur. **À** la différence de l'accident du travail, les protagonistes partagent la même exposition au risque et la même responsabilité de prévention.

Bonne pratique

Favoriser la vigilance partagée

Dans le cadre de la Safety Academy, l'Icsi a développé un module e-learning dédié à la vigilance partagée et à une intervention réussie.

Parmi les points clés :

- Savoir identifier une situation potentiellement dangereuse ;
- Adopter une attitude de dialogue et d'écoute ;
- Aider le collègue à prendre conscience des risques et des conséquences potentielles ;
- Trouver ensemble la façon la mieux adaptée à un travail en sécurité ;
- Encourager et diffuser toutes bonnes pratiques de travail.

« Exercer une vigilance partagée demande de faire preuve d'un certain courage pour intervenir auprès des collègues. Plus cette pratique sera partagée et plus elle renforcera la culture sécurité de l'organisation. »

2.3.4 Participer à la rédaction et la mise à jour des procédures

Le temps où la rédaction des procédures était l'apanage des services méthodes et experts semble révolu. La participation des opérateurs de terrain permet de prévenir certaines difficultés de mise en œuvre et de renforcer leur responsabilisation.

Le fait que la sécurité dépende de chacun crée un climat d'échange entre les parties prenantes qui permet à tout membre de l'organisation, salarié ou prestataire, quel que soit le poste occupé, de faire évoluer les prescriptions et les pratiques afin d'assurer la sécurité des systèmes techniques. Les procédures doivent correspondre à la réalité du terrain et, dans la mesure du possible, intégrer des photos, des schémas de circuits et d'instrumentation, des logigrammes ou encore des schémas fonctionnels. Des procédures sous forme de vidéos peuvent être utilisées dans certaines situations.

Bonne pratique

Impliquer les équipes opérationnelles dans procédures relatives aux tâches critiques

Dans les organisations les plus matures les procédures des tâches critiques sont écrites ou mises à jour par les équipes opérationnelles, puis relues et validées par les experts techniques. C'est l'occasion d'un partage entre les services qui participent à la maîtrise des risques majeurs. Les procédures sont mieux adaptées aux situations réelles, enrichies par les retours d'expérience des autres entreprises et secteurs d'activités, et prennent en compte les dernières connaissances techniques. C'est l'occasion de développer la conscience partagée des risques majeurs.

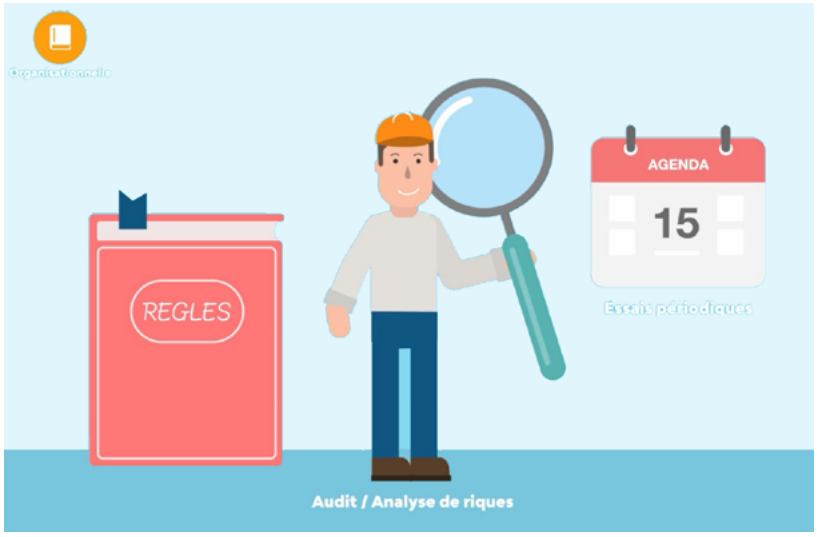


FIGURE 16 : *L'équipe opérationnelle un acteur essentiel pour que les règles soient pertinentes et adaptées aux situations rencontrées*

2.4 Partager cette conscience au sein de l'équipe opérationnelle et avec tous

L'identification et le partage des risques de toute nature par l'équipe opérationnelle n'est pas aussi naturelle qu'elle semble l'être. La première difficulté est une concentration sur les problématiques opérationnelles immédiates, le fonctionnement du quotidien. Une autre est celle d'accéder à une compréhension de la hiérarchie des risques et à une vision globale de la maîtrise des risques les plus importants.

2.4.1 Situer la place de son geste par rapport à la vie du système en exploitation

La conscience partagée des risques majeurs concerne non seulement les opérateurs, mais aussi les prestataires, les experts, les responsables de processus, les managers et les décideurs. En effet, le risque majeur doit être à l'esprit lors de toute nouvelle directive, modification de matériel, augmentation ou diminution des effectifs, décision de sous-traiter. Toute modification de l'organisation d'un site peut avoir une incidence sur la sécurité des opérations. Toute intervention, quelle qu'elle soit, peut être déterminante pour la sécurité des systèmes techniques.

Situer la place de son geste par rapport à la vie du système en exploitation et connaître son impact sur les gestes des autres opérateurs permet de créer un lien entre les séquences d'une même activité. Connaître au moins le rôle de son activité par rapport à celle qui précède et celle qui suit, contribue à construire cette conscience partagée des risques, apportant cohérence et compréhension entre les activités des uns et des autres dans la prévention des risques majeurs. Certaines entreprises insistent sur la nécessité de bien connaître les enjeux et de bien gérer les interfaces en amont et en aval de toute intervention : bien connaître le « geste d'avant » et le « geste d'après ».

Bonne pratique

Mettre en place des espaces de débats entre services

Certaines organisations ont mis en place des espaces de débat entre services pour favoriser les échanges sur les activités les plus sensibles en termes de sécurité. Cela permet à chacun de mieux comprendre l'activité des autres services et l'impact potentiel de sa propre activité sur celle des autres, et souvent de lever des incompréhensions et de partager les contraintes de chaque service.

Cette bonne pratique est détaillée dans l'annexe 3 « Mener une analyse de risques de type EPECT* » Elle permet d'améliorer la conscience partagée des situations risquées pour les patients et leur gestion et maîtrise.

**Espace de partage et d'exploration de la complexité du travail*

p. 47 Annexe 3

Cette continuité dans la gestion du risque doit être particulière observée en cas de sous-traitance afin de garantir la capacité de l'entreprise intervenante à assumer ses responsabilités.

Bonne pratique

Favoriser le partage d'informations entre donneur d'ordre et prestataires

Le partage d'informations est indispensable entre le donneur d'ordre, garant de la sécurité des installations, et le prestataire, garant de la sécurité des opérations. Les moments de partage sont organisés pour que les deux parties aient une vision commune des risques majeurs, des lignes de défense de sécurité, des principaux éléments pouvant affaiblir ces lignes de défense et des mécanismes à mettre en place en cas d'incident sur l'exploitation.

2.4.2 Donner toutes leurs chances aux barrières humaines

S'il existe de nombreux outils pour calculer la fiabilité des composantes techniques des barrières de sécurité, ce n'est pas le cas pour les composantes organisationnelles et humaines de sécurité.

La fiabilité humaine est variable et dépend de plusieurs paramètres parmi lesquels :

- La prise en compte des facteurs humains en conception ;
- La complexité de la situation ;
- Le niveau de formation ;
- Le rythme biologique ;

- L'état physique et psychique de la personne ;
- Le contexte propice à l'incident ou non ;
- La pression temporelle et la simultanéité des tâches ;
- La maîtrise de l'activité.

Il faut définir l'architecture de la sécurité des systèmes techniques sur le postulat que l'être humain fait inévitablement des erreurs. La capacité de détection d'une situation risquée et de rattrapage des erreurs par l'être humain est difficilement prise en compte dans l'analyse des risques. Elle est potentiellement importante, mais fragile.

Par ailleurs, la redondance ne fonctionne pas bien pour l'être humain : augmenter le nombre de personnes n'augmente pas mécaniquement la fiabilité du système. On renforce plutôt la sécurité par la complémentarité des positions de sécurité (prévention, surveillance, rattrapage des situations).

Les interactions entre les hommes qui contribuent au bon fonctionnement des lignes de défense de sécurité sont donc difficiles à prendre en compte dans le calcul de fiabilité d'un système.

Enfin, les facteurs temps et espace sont des éléments qui influencent fortement les composantes humaines des lignes de défense de sécurité (rythmes, pression temporelle, distance géographique, etc.).

Bonne pratique

Donner leurs chances aux barrières humaines

Pour que les opérateurs aient le plus de chances de détecter et d'identifier les situations à haut potentiel de gravité, il est important de :

- Partager une connaissance des risques et des barrières associées ;
- Proposer des formations et des entraînements individuels et collectifs aux situations susceptibles de se produire, dans le but d'enrichir le modèle mental ;
- S'assurer de la disponibilité d'informations pertinentes au bon moment ;
- Gérer la charge de travail afin d'éviter la simultanéité des tâches critiques.

2.5 Recommandations

Les améliorations successives de la sécurité des systèmes techniques ont paradoxalement rendu plus difficile la prégnance des risques majeurs dans la conscience de l'équipe opérationnelle, qui se concentre principalement sur le fonctionnement quotidien des installations et des dysfonctionnements les plus fréquents. Ceci peut être accentué dans le cas de pilotage à distance des installations. Il est alors incontournable de permettre l'identification et l'appropriation des risques majeurs par l'équipe opérationnelle, ainsi que d'ancrer la conviction que les barrières ne sont pas définitives. En effet, les barrières doivent être sans cesse réinterrogées et améliorées.

Pour développer la connaissance des risques majeurs, des scénarios majeurs et des lignes de défense sécurité, il est nécessaire de :

- Assurer par une formation adaptée une connaissance physique suffisante des installations ou situations à risques, des barrières, y compris pour les équipes qui n'assurent pas l'exploitation sur site mais doivent pouvoir matérialiser les risques et les parades.
- Favoriser l'imaginaire en sécurité de l'équipe opérationnelle grâce au témoignage de personnes qui ont vécu des accidents ou presqu'accidents graves, ou au partage autour d'accidents majeurs du secteur d'activité. Mener une réflexion sur les enseignements et les transpositions possibles pour mieux intégrer la sécurité dans les pratiques.
- Partager et enrichir les scénarios majeurs avec les équipes opérationnelles, en utilisant des documents simples présentant les études de danger relatives au système et les barrières des 3 lignes de défense de sécurité. En faire un outil au service des équipes opérationnelles.
- Mettre en place des ateliers de débat, que ce soit dans une même activité ou entre activités sur la base d'un incident, pour partager sur ce qui aurait pu arriver de pire et la gestion d'une situation complexe.

Pour responsabiliser et permettre à chacun de jouer son rôle en sécurité du système technique, il est recommandé de :

- Mettre en place des dispositifs de formation et de partage qui permettent de connaître le rôle de chacun (mon rôle et celui des autres) pour entretenir la sécurité du procédé et s'assurer que les lignes de défense techniques, organisationnelles et humaines soient fonctionnelles.
- Réaliser des exercices de simulation les plus réalistes possibles intégrant des imprévus (une personne malade non remplacée, erreurs d'un capteur, confusions de matériels, etc.) pour que l'ensemble des acteurs (exploitants, maintenance, administratifs, services externes, riverains, etc.) s'entraînent à réagir face à des situations incidentelles et accidentelles.
- Encourager la vigilance partagée entre acteurs pour détecter, stopper et sécuriser les situations à risques.
- Former à la détection des événements et situations inhabituelles qui pourraient avoir des conséquences sur la maîtrise des risques majeurs et favoriser la remontée de ces informations.

3

Les moments clés d'animation sur les risques majeurs

3.1 Constats généraux

Les préoccupations quotidiennes pour effectuer la production, être efficace et atteindre les objectifs sont souvent très éloignées des risques majeurs. Afin de limiter cet éloignement et remettre au cœur des préoccupations la maîtrise des risques majeurs, les managers intermédiaires et les animateurs ou responsables d'équipes opérationnelles jouent un rôle clé, que ce soit pour traiter l'information et organiser sa diffusion, ou pour créer et organiser des espaces de discussion.

Après la connaissance et l'appropriation des risques majeurs, la connaissance de son rôle dans la prévention ou la gestion du risque, thèmes traités au chapitre précédent, il s'agit ici d'entretenir un lien entre les problématiques d'exploitation au quotidien et la prévention de ces risques majeurs.

Des moments d'animation sécurité centrés sur les risques majeurs permettent de les maintenir au cœur des préoccupations de chacun, quelle que soit sa fonction dans l'entreprise. La prévention des risques majeurs se construit dans le quotidien et collectivement. Il faut pour cela à la fois savoir exploiter les occasions d'échange dans les processus d'exploitation et créer des moments spécifiques où la prise de recul sera privilégiée.

3.2 Traiter l'information et organiser sa diffusion

3.2.1 Sélectionner et diffuser l'information sur les événements importants

Une veille sur les événements importants internes et externes est nécessaire afin d'extraire les éléments significatifs qui ont une résonance pour les exploitants du système et qui peuvent :

- ▷ Contribuer à la sensibilisation au risque majeur et aux attitudes de prévention ;
- ▷ Préparer la gestion des situations d'urgence ;
- ▷ Suggérer des améliorations techniques ou organisationnelles.

Bonne pratique

Ritualiser le récit d'accidents majeurs

Il s'agit en premier lieu de susciter une prise de conscience : ça n'arrive pas qu'aux autres !

Certaines entreprises qui ont vécu des accidents traumatisants ont ritualisé le récit et le partage d'accidents majeurs. Certains secteurs d'activités (nucléaire, pétrochimie, transport) exploitent les grands événements du secteur pour la formation du personnel.

FIGURE 17 : *Ça n'arrive pas qu'aux autres*

Les principaux enseignements de ces événements ainsi que les messages de prévention émanant de la direction doivent être largement diffusés par des supports d'information adaptés aux destinataires (affichages, revues internes, outils informatiques), en exploitant les temps d'animation sécurité.

Partager les REX positifs et négatifs

Bonne pratique

Des *Flashs sécurité* de l'unité de production sont émis régulièrement par les équipes opérationnelles en lien avec le service sécurité. Ils relatent des REX positifs et négatifs et sont partagés et discutés lors des réunions mensuelles.

3.2.2 Rendre accessible l'information sur la gestion des risques majeurs

Il est important de disposer d'un système d'information ouvert, pour permettre à chacun de comprendre, en fonction de son niveau d'expertise, le risque auquel lui-même, son entourage et le public sont potentiellement exposés.

Les indicateurs de performance ou de suivi de la gestion des risques majeurs doivent être largement diffusés et discutés dans les équipes.

Les déclarations d'événement et les comptes rendus d'analyse ne doivent pas être réservés à un public de spécialistes. Tout le personnel doit pouvoir y accéder et les moins avertis doivent pouvoir bénéficier d'explications complémentaires.

3.3 Créer et organiser des espaces de discussion

La sécurité doit être une préoccupation du management et ceci doit être visible pour le personnel. Les réunions périodiques de direction, de service ou d'équipe doivent aborder systématiquement la sécurité du système technique. Lors des visites de terrain, les managers doivent réserver un moment pour évoquer la sécurité du système, les risques majeurs et les mesures de prévention à la main des personnes rencontrées.

Au niveau opérationnel, il existe une multitude d'occasions pour repositionner la prévention des risques majeurs au cœur des discussions. Parmi elles, quatre moments clés d'animation sécurité constituent des espaces de discussion incontournables :

- La réunion de coordination, la veille d'opérations dans un secteur ;
- Le briefing sécurité, le jour d'une opération et juste avant qu'elle ne soit lancée ;
- La remontée et le traitement d'un événement à haut potentiel de gravité, si un tel événement est détecté ;
- La causerie de sécurité, pour mettre en débat des sujets de sécurité.

Ces quatre moments d'animation sécurité encadrent les opérations avant, pendant et potentiellement après leur mise en œuvre et ont pour but de garantir la sécurité des personnes et du site d'exploitation. C'est pourquoi il est indispensable d'en faire des moments privilégiés pour développer la conscience partagée du lien entre l'activité quotidienne et les risques majeurs.

3.3.1 La réunion de coordination

La réunion de coordination prépare collectivement les acteurs concernés par les opérations dans un secteur donné. Généralement organisée la veille de l'opération, elle suppose que tous les acteurs soient représentés, y compris les sous-traitants.

Ce temps de sécurité devrait s'articuler autour de quatre axes clés :

- La visualisation collective des opérations qui auront lieu le lendemain sur le secteur et des principaux risques associés, en particulier ceux liés à la coactivité ;
- Le partage des retours d'expérience des collègues à propos d'opérations similaires afin d'identifier les étapes critiques ;
- Le contrôle de l'attitude et de l'attention de chaque participant à la réunion pour vérifier la compréhension des enjeux ;
- La synchronisation des opérations du lendemain et les moyens de communication pour la vérifier.

Bonne pratique

Impliquer toutes les équipes intervenantes dans la réunion de coordination

Toutes les équipes qui interviendront le lendemain sont représentées lors de la réunion de coordination afin de transmettre les informations lors du briefing.

- Le plan de prévention et ses analyses réalisés préalablement, sont validés et actualisés.
- Le contexte général du site d'exploitation est partagé. Par exemple : les opérations étrangères au contexte dans lequel on intervient mais qui pourraient le modifier.

3.3.2 Le briefing sécurité

Le briefing sécurité, qui se situe le jour même, avant le début d'une opération, reprend les points de vigilance soulevés lors de la réunion de coordination pour les actualiser en fonction des conditions réelles du jour. Le but est que les personnes qui interviennent dans l'opération aient pleinement conscience des risques associés, des événements redoutés, des coactivités identifiées la veille, ainsi que des mesures de prévention à appliquer.

Le briefing sécurité est l'occasion de décrire l'opération à l'équipe opérationnelle, en rappelant toutes ses étapes.

Le briefing devrait :

- Prévoir le pire scénario d'un événement et ses conséquences ;
- Rappeler les expériences passées et s'en servir pour adapter la pratique ;
- Faire l'inventaire du matériel nécessaire à l'intervention pour vérifier sa disponibilité et son état ;
- S'assurer que tous les opérateurs aient compris leur rôle et soient aptes à le remplir.

Bonne pratique

Le briefing sécurité

Pour un briefing réussi :

- Il existe un climat d'échange entre tous les intervenants ;
- Les décisions du briefing sécurité doivent prendre en compte les conditions particulières des jours précédents, de la nuit précédente et du jour même de l'opération ;
- Le responsable de l'opération doit s'assurer que les autorisations et habilitations nécessaires à l'intervention ont été obtenues ;
- Les échanges sont fondés sur le compte rendu de la réunion de coordination, notamment sur les questions de coactivité ;
- Il y a un rappel des risques les plus importants et des dispositifs de sécurité disponibles sur la zone d'intervention ;
- Il y a un partage autour du rôle attendu de chacun pendant l'opération, en cas de situation imprévue ou accidentelle.

3.3.3 Partager la compréhension et les enseignements d'un événement à haut potentiel de gravité

Les bonnes réactions lors d'un événement à haut potentiel de gravité sont cruciales pour limiter les risques. Aux chapitres précédents, nous avons vu qu'il est essentiel de savoir le détecter, faire remonter l'information et analyser la situation pour en tirer des enseignements afin que cet événement ne se reproduise pas.

La remontée et le traitement d'un événement à haut potentiel de gravité sont une opportunité pour partager les enjeux et les enseignements. Face à une situation de ce type, le partage au sein de l'équipe d'intervention et avec les autres équipes potentiellement concernées doit être favorisé. Par exemple :

- Échanger avec toutes les personnes concernées par l'événement, après avoir pris des mesures d'urgence pour limiter les risques ;
- Partager la compréhension des conséquences potentielles ;
- Analyser la situation pour en identifier les causes ;
- Établir de nouvelles modalités de réalisation à partir de l'analyse de la situation ;
- S'assurer que les personnes ont pris conscience de l'importance de cet événement et qu'elles adapteront leurs pratiques.

Bonne pratique

Détecter et identifier les évènements à haut potentiel de gravité

La détection des événements et l'identification de ceux qui ont un haut potentiel de gravité doivent devenir un réflexe des équipes opérationnelles.

- La diffusion de la survenue des événements doit se faire auprès de tous, y compris au sein d'autres unités de l'entreprise, car un événement similaire peut se produire ailleurs ou sur le même site.
- Le suivi des actions correctrices doit être accessible : les décisions doivent être appliquées et leur efficacité doit être mesurable.

3.3.4 La causerie de sécurité

La causerie de sécurité est un moment privilégié de mise en discussion et de débat sur les questions de sécurité au sein des équipes. Organisée selon une fréquence définie, par exemple une fois par semaine ou par mois, elle peut être de durée limitée (généralement une quinzaine de minutes), mais est l'occasion d'échanger sur l'actualité sécurité du moment. C'est particulièrement vrai lorsqu'un incident arrive ou lorsqu'une bonne pratique est remontée et que des décisions sont prises. Tenir les équipes informées des avancées est essentiel.

Une causerie sécurité devrait :

- Solliciter toute l'équipe afin que chacun puisse se prononcer sur le sujet ;
- Valoriser la remontée d'information et remercier les opérateurs qui ont identifié les événements ou partagé une bonne pratique ;
- Faire le point sur les conséquences éventuelles de l'événement ou l'intérêt de la bonne pratique ;
- Faire le point sur les actions en cours et leur état au regard des enseignements tirés du traitement des événements récents ;
- Faire le point sur des évolutions éventuelles des exigences, de l'organisation ;
- Permettre de débattre des options éventuelles d'amélioration de la sécurité et d'ébaucher les meilleures solutions.

Bonne pratique

Pour une causerie réussie

Pour réussir une causerie sécurité, il est recommandé de favoriser l'animation par les opérateurs en mode participatif, et d'utiliser des supports d'animations pour donner un impact aux discours (ex. vidéos courtes, jeux de rôle, etc.).

3.4 Recommandations

Pour l'information générale du personnel :

- Prévoir un système de veille pour élaborer un fichier dynamique des événements importants, avec une synthèse de l'enchaînement des faits, la mise en exergue des lignes de défense, les similitudes avec le système technique de l'entité et les points de vigilance à faire ressortir.
- Prévoir des supports d'information réactifs pour partager ces analyses.
- Diffuser des indicateurs de performance sur la sécurité et avoir un système d'information ouvert qui permette à chacun de comprendre le risque majeur et d'apprécier le niveau de maîtrise du risque.

Pour des moments de partage sur la gestion du risque majeur :

- Pour le management, prévoir lors des réunions ou des rencontres sur le terrain, un temps pour évoquer la sécurité du système.
- Intégrer la sécurité dans les temps de coordination opérationnelle (réunion de coordination, briefing) pour rappeler les enjeux et les rôles, les risques et les mesures prises.
- Utiliser la détection et le traitement d'événements à haut potentiel de gravité pour partager les observations, les analyser et activer la prise de conscience des équipes.
- Dans le programme d'activité des équipes, prévoir un temps d'échange « à froid » sur la sécurité du système (hebdomadaire ou mensuel).
- Lorsque les équipes sont dispersées, que le travail à distance est développé ou qu'un pilotage à distance des installations est en place, il est particulièrement important de prévoir des modalités d'animations, des occasions d'échanges qui permettent un partage des modes de représentations et d'actions cohérents pour une meilleure maîtrise des risques majeurs.

Conclusion

La principale conclusion du groupe de travail est que la clé de la maîtrise des risques majeurs est la conscience partagée de ce type de risques par toutes les parties prenantes de la sécurité des systèmes techniques de l'industrie ou des services concernés.

Cette prise de conscience est compliquée par le fait qu'étant rares voire hypothétiques, les accidents majeurs n'apparaissent pas comme une menace réelle. Peu de personnes en ont connu, ce qui induit l'idée que ces accidents n'arrivent qu'aux autres. Pour placer la conscience des risques majeurs au cœur des préoccupations et développer une vigilance partagée, il faut convaincre que chacun est « l'autre » de quelqu'un.

Toutes les parties prenantes doivent savoir et comprendre qu'à leur niveau elles ont une responsabilité et un impact possible sur la sécurité des systèmes techniques. La responsabilité de chacun doit être identifiée dans le maintien des composantes des lignes de défense et leur fonctionnement. L'opérateur, notamment, n'est pas le seul garant de la sécurité, mais l'un des maillons d'une chaîne qui relie les prestataires, les experts, les responsables de processus, les managers et les décideurs, pour prévenir et maîtriser les risques majeurs.

Les animations sécurité sont des moments privilégiés pour maintenir la maîtrise des risques au cœur de l'activité quotidienne. Ils initient une réflexion collective autour des questions de sécurité et instaurent un climat propice au partage d'informations ainsi qu'au développement de processus clés pour la sécurité de l'exploitation.

Fort de ces constats et s'appuyant sur les axes de réflexion définis, nous vous proposons une liste non exhaustive de recommandations permettant le développement et le maintien d'une conscience partagée du risque majeur.

Les risques majeurs au cœur du pilotage des processus :

- ▷ Mettre en évidence le système de prévention des risques majeurs avec ses trois lignes de défense prévention, récupération et atténuation, chacune constituée de barrières, elles-mêmes formées de composantes techniques organisationnelles et humaines. Évaluer et entretenir ces barrières.
- ▷ Focaliser la ligne managériale et la direction sur la maîtrise des risques majeurs en ayant des indicateurs spécifiques à la sécurité du système technique.
- ▷ Centrer le pilotage sur la maîtrise des risques majeurs en :
  - Ayant, dans tous les domaines de gestion, des processus d'arbitrage qui intègrent systématiquement une analyse d'impact sur la sécurité du système technique à moyen et long terme.
  - Développant une culture juste et équitable pour que les personnes se sentent libres, légitimes et soutenues pour alerter, informer, analyser les événements en toute transparence.
  - Développant une culture d'apprentissage qui utilise la remontée d'information, le retour d'expérience, l'analyse d'événement et la formation et en ayant un processus de formation global qui garantisse les compétences dans la durée.
  - Exploitant au mieux tous les événements à haut potentiel de gravité et en repérant les événements positifs pour pérenniser et étendre les bonnes pratiques.
- ▷ Évaluer l'impact des changements techniques et socio-organisationnels sur les barrières de sécurité des systèmes techniques pour prévenir tout risque de dégradation.

Appropriation des risques majeurs par l'équipe opérationnelle :

- ▷ Développer la connaissance des risques majeurs, scénarios majeurs et lignes de défense sécurité en :
  - Développant l'imaginaire sécurité de l'équipe opérationnelle, grâce aux récits de personnes ayant vécu des accidents graves ou au partage d'accidents majeurs du secteur d'activité.
  - Créant des ateliers de débat dans une même activité ou entre activités sur les situations ou événements à haut potentiel de gravité.
- ▷ Responsabiliser et permettre à chacun de jouer son rôle dans la maîtrise de la sécurité des systèmes techniques en :
  - Mettant en place des dispositifs de formation et de partage qui permettent de connaître le rôle de chacun dans le fonctionnement et l'entretien des lignes de défense.
  - Réalisant des exercices de simulation de situations incidentelles et accidentelles les plus réalistes possibles pour s'entraîner à réagir face à l'imprévu.
  - Encourageant la vigilance partagée entre acteurs pour détecter, stopper et sécuriser les situations à risque.
  - Favorisant la détection et la remontée des événements et situations inhabituelles qui pourraient avoir des conséquences graves et révèlent des défaillances dans la maîtrise des risques majeurs.

Des moments clés d'animation sécurité pour entretenir la conscience et la maîtrise du risque :

▷ Disposer de vecteurs d'information pour sensibiliser au risque l'ensemble du personnel, diffuser des enseignements et favoriser le questionnement :

- Des supports d'information réactifs pour les événements internes et externes s'appuyant sur un système de veille sur les événements importants ;
- Un système d'information ouvert, facile d'accès qui permette à chacun de comprendre le risque auquel lui-même, son entourage, le public est potentiellement exposé et le niveau de maîtrise de ce risque (REX des événements, indicateurs).

▷ Prévoir des moments de partage sur la gestion du risque majeur en ayant :

- Un management qui évoque la sécurité du procédé dans ses réunions ou rencontres sur le terrain, en intégrant la sécurité dans les temps de coordination opérationnelle.
- Des temps d'échange « à froid » sur la sécurité du procédé.

Quelques pistes de réflexion complémentaires

Au-delà de ces recommandations, le groupe d'échange a abordé des thèmes de réflexion qui pourraient être repris dans chaque entreprise concernée pour faire progresser cette conscience partagée du risque et le niveau de maîtrise, chaque entité pouvant adapter la réponse à son contexte :

▷ Complexité de la documentation pour les acteurs de terrain ;

▷ Cloisonnement des activités, des rôles et missions, souvent renforcé par le niveau d'exigence, la spécialisation ;

▷ Communication entre donneurs d'ordre et sous-traitants ;

▷ Complexité des systèmes techniques et difficulté d'appréhension du fonctionnement d'ensemble ;

▷ Impact de l'éloignement physique des installations par rapport au poste de contrôle et de pilotage des installations dans le cadre du développement du pilotage à distance ;

▷ Sentiment de sécurité créé par la fiabilité croissante des systèmes, assurance induite par la digitalisation, les techniques de réalité virtuelle ou la perte de vigilance et de capacité de réaction engendrée par l'évolution des systèmes automatiques. Quel serait le bon équilibre entre niveau d'automatisation et de fiabilité technique, aides informatiques et intervention humaine ?

▷ Rapport coût/bénéfice des investissements dans la sécurité : jusqu'où investir dans la sécurité des systèmes techniques alors que le retour sur investissement est difficile à chiffrer ? Quel coût en termes d'image de l'entreprise ? Quel impact sur les personnes et l'environnement ?

Annexes

Bonnes pratiques

A1

Bonne pratique n°1
Visualisation des scénarios d'accident à l'aide du « nœud papillon »

Secteurs ou cette bonne pratique a été mise en œuvre : principalement dans les industries de systèmes techniques.

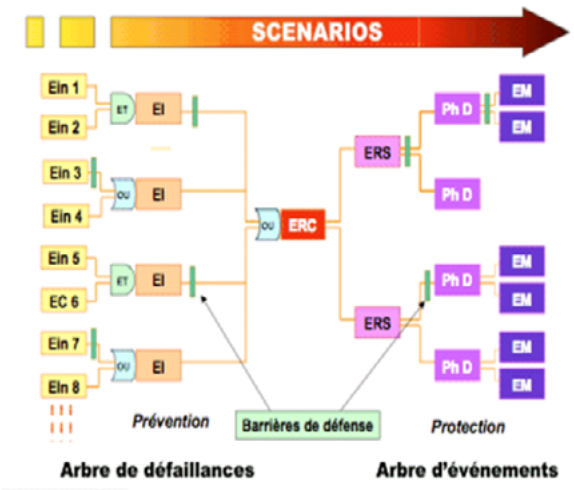
Objectifs recherchés

- ▷ Partager avec les équipes opérationnelles les scénarios d'accidents et les barrières associées ;
- ▷ Initier les équipes opérationnelles à l'identification des fragilités des barrières sur la base de leurs connaissances terrain ;
- ▷ Rappeler le rôle de chacun dans l'entretien des barrières ;
- ▷ Permettre une visualisation globale du système de prévention des accidents majeurs.

Description

Il s'agit d'un outil de visualisation concrète des scénarios d'accident. Visuel et synthétique, le « nœud papillon » est compréhensible à tous les niveaux de l'entreprise et peut servir d'outil de communication.

Cette représentation a le mérite de contenir beaucoup d'informations sous une forme très synthétique, d'autoriser simultanément une vue d'ensemble et des focus sur des branches particulières, de permettre des calculs de probabilités ou de dégager l'architecture. Chaque chemin conduit d'une défaillance à l'apparition de dommages au niveau des cibles désigne un scénario d'accident particulier pour un même événement redouté central.



Ein : Événement indésirable (défaillance sortant du cadre d'exploitation défini)

EC : Événement courant (événement admis survenant de manière récurrente)

EI : Événement initiateur (cause directe d'une perte de confinement)

ERC : Événement redouté central (perte de confinement sur un équipement dangereux)

ERS : Événement redouté secondaire (conséquence directe de l'ERC)

Ph D : Phénomène dangereux (phénomène accidentel pouvant engendrer des dommages majeurs)

EM : Effets majeurs (dommages occasionnés au niveau des cibles ou des enjeux

FIGURE 18 : *Exemple d'analyse d'un évènement à l'aide du « nœud papillon »*

La partie gauche du nœud papillon identifie les causes de l'événement central redouté (arbre des défaillances). La partie droite du nœud papillon s'attache à déterminer les conséquences de cet événement redouté (arbre d'événements).

Sur le schéma, les barrières de défense sont représentées sous la forme de barres verticales, symbolisant le fait qu'elles s'opposent au développement d'un scénario d'accident. Sur les branches de cette représentation, on peut placer des barrières :

- Sur la partie gauche : des barrières de prévention de la survenue de l'événement central ;
- Sur la partie droite : des barrières de protection/mitigation qui peuvent en limiter les conséquences.

Pour être retenue et apparaître dans le « nœud papillon », une barrière de défense doit :

- Assurer une certaine efficacité (pourcentage d'accomplissement d'une fonction de sécurité) ;
- Fonctionner selon un temps de réponse adapté ;
- Atteindre un niveau de confiance cible (facteur de réduction de risque).

La performance de ces barrières se dégrade dans le temps. Le maintien de leurs performances doit être assuré par de la maintenance et une inspection adaptée, avec des tests périodiques de fonctionnement.

Le nœud papillon permet de visualiser l'importance de certaines barrières de défense et, par conséquent, la nécessité impérative de réaliser la maintenance et les tests requis.

Points de vigilance et recommandations :

Il s'agit d'un outil relativement lourd à mettre en œuvre, son utilisation est souvent réservée à des événements critiques pour lesquels un niveau élevé de démonstration de la maîtrise des risques est indispensable. Il est généralement construit à partir d'une analyse des risques comme l'Analyse préliminaire des risques (APR). Autant sa construction est longue, autant son utilisation à des fins pédagogiques est aisée.

L'intégralité des causes possibles des accidents susceptibles de se produire est listée, puis quantifiée. Par cette quantification, on gagne une excellente visibilité sur les importances relatives des sources de risque, ce qui permet notamment de savoir où réduire ce risque pour que l'impact soit maximal. Le nœud papillon offre une vision globale des scénarios d'accident en mettant en exergue leurs causes, les liens logiques entre celles-ci et les barrières de sécurité. La modélisation graphique des séquences accidentelles proposée par cet outil en fait un support puissant et adapté pour la formation et la sensibilisation des équipes opérationnelles.

A2

Bonne pratique n°2
Ateliers culture et pratiques de sécurité

Secteur d'activité où cette bonne pratique a été mise en œuvre

Chimie, pétrochimie, pétrole… mais applicable dans toutes les industries ou activités de process à risques.

Objectifs recherchés

- ▷ Mettre les mêmes réalités terrain derrière les situations de travail à haut potentiel de gravité ainsi que les enchaînements associés (qu'est ce qui se passe si) ;
- ▷ Renforcer l'implication des équipes opérationnelles dans l'appropriation des pratiques de sécurité.

Description :

Ces ateliers regroupent des techniciens et des opérateurs en associant, a priori, des activités complémentaires (production, maintenance, logistique, ingénierie, etc.). Les groupes sont formés en tenant compte des situations de travail à forts enjeux de sécurité. Les ateliers durent une semaine avec une séance de travail quotidienne de 2 heures et réunissent une douzaine de participants

Déroulement :

- ▷ Jour 1 : Libération de la parole, expression des plaintes : échanger.
- ▷ Jour 2 : Partage et constat de l'état des lieux sur la base des situations à risque identifiées : se mettre d'accord sur les situations à fort enjeu de sécurité.
- ▷ Jour 3 : Élaboration commune et formalisation des propositions : négocier et hiérarchiser collectivement les propositions.
- ▷ Jour 4 : Validation et reformulation des propositions pour la présentation en réunion de synthèse : argumenter pour convaincre sur ces propositions.
- ▷ Jour 5 : Réunion des groupes et des représentants de la direction pour prendre acte des propositions présentées par chaque groupe et échanger de façon transversale.

Des prérequis :

Ces ateliers nécessitent un animateur extérieur (qui n'est pas juge et partie), garant de la démarche, qui connaît le site (visite détaillée notamment des équipements et process à risques majeurs) et qui a mené une analyse documentaire sur l'état d'identification des risques majeurs et des accidents.

Le rôle de l'animateur :

- ▷ Ne pas laisser le groupe entrer dans la revendication et expliquer clairement aux participants la règle du jeu et les livrables à produire, dans un temps très court ;
- ▷ Gérer le temps, réguler les débats et recadrer les « négociations » et « reformulations » nécessaires entre participants ;

- Mettre au propre chaque jour les supports qui permettent aux participants d'avancer sans souci logistique (c'est aussi une forme de reconnaissance) ;
- Aider les participants à préparer la restitution au Codir.

La direction s'engage à écouter et à prendre en compte les propositions des techniciens et opérateurs. Pour autant, tout n'est pas forcément recevable et compatible avec les priorités de la politique de sécurité et il convient d'analyser et d'arbitrer ces propositions avant d'informer le personnel de la suite qui sera donnée.

Indicateurs ou modalités d'appréciation

- La prise de parole par les personnels opérationnels de terrain ;
- Leur prise de conscience de la nécessité de se mettre d'accord collectivement, de reformuler leurs contributions, de les argumenter et de les illustrer par des exemples concrets, des situations connues, des difficultés récurrentes :
- Leur volonté d'être écouté et de participer, mais aussi leur acceptation que les solutions ne sont pas toujours aussi simples qu'on le croit à mettre en œuvre et que certaines problématiques (arbitrages, prises de décisions) induisent des changements importants de comportement à tous les niveaux.

Points de vigilance et recommandations

- Lutter contre ses propres a priori car on a déjà une lisibilité large des problèmes à traiter ;
- Accepter, le premier jour, que les discussions soient brouillonnes car elles permettent de libérer la parole et de faire participer tout le monde ;
- Mettre en avant la force du collectif et guider le travail, mais sans manipuler ;
- En parallèle, préparer les membres du Codir à dépasser les apparences (« mais tout ça on le sait déjà »), à ne pas se sentir personnellement mis en cause dans leur fonction (« comme si on n'avait rien fait »), à mesurer les écarts entre le travail prescrit et le travail réel (« tout le monde le sait mais pour autant on n'intervient pas »).

Cette démarche permet aussi de faire le lien avec quatre problématiques de la culture de sécurité :

FIGURE 19 : *Les 4 problématiques de la culture de sécurité*

A3

Bonne pratique n°3[5]
Mener une analyse de risques type EPECT*

*Espace de partage et d'exploration de la complexité du travail

Secteur d'activité où la bonne pratique a été mise en œuvre : radiothérapie (médical)

Objectif recherché

Cette méthode permet aux unités de radiothérapie de faire des liens entre une situation de travail complexe pour l'équipe médicale et une situation risquée pour les patients. L'identification et l'analyse de situations de travail risquées pour le patient permet d'améliorer la conscience partagée des risques. La méthode EPECT permet également de discuter des différentes dimensions organisationnelles du travail que les méthodes industrielles classiques ont du mal à questionner pour des systèmes sociotechniques complexes.

Description

La méthode EPECT nécessite :

- L'organisation d'un espace de discussion – en dehors du soin – d'environ deux heures tous les trois mois ;
- L'animation par un facilitateur et au moins deux représentants par métier pour favoriser les débats intra et inter-métiers.

Cette méthode sera illustrée par un exemple simple mais la maîtrise progressive de la méthode EPECT permet au fur et à mesure d'analyser des situations de travail plus complexes.

Cette méthode comporte quatre étapes.

Étape 1 : décrire une situation de travail complexe réelle ou imaginée (environ 30 minutes)

Il s'agit pour les participants d'élaborer un scénario à partir d'éléments de désorganisation du travail quotidien (tensions, changements, inerties, contraintes, contradictions).

Exemple

L'interne prend en charge un patient en soins palliatifs alors qu'il n'est pas encadré par un senior (radiothérapeute indisponible), qu'il est insuffisamment formé (début d'internat) et qu'il dispose d'un dossier patient incomplet.

Étape 2 : étudier la performance de l'équipe médicale (environ 30 minutes)

Les participants discutent des quatre modes de réussite (plutôt que des modes de défaillance) pour résoudre le scénario établi à l'étape n°1 :

1. La redéfinition des règles, des procédures, des actions de sécurisation ;
2. Les actions facilitantes (raccourcis, entraides) ;

5. Thellier, S. (2017). *Approche ergonomique de l'analyse des risques en radiothérapie : de l'analyse des modes de défaillances à la mise en discussion des modes de réussite.* Thèse de doctorat en ergonomie. Conservatoire National des Arts et Métiers, Paris, soutenue le 12 décembre 2017, 294 p.

3. Les régulations individuelles (récupérations, adaptations, ajustements) ;
4. Les régulations collectives (auto-organisation de l'équipe).

Exemple de modes de réussite

Exemple

L'interne prend en charge un patient en soins palliatifs. L'équipe cherche à récupérer des informations manquantes sur ce patient. Faute de disponibilité du radiothérapeute senior, l'interne est aidé par un autre interne et/ou un manipulateur lors de la préparation du traitement et/ou lors de son administration.

Étape 3 : identifier les situations risquées pour les patients (environ 30 minutes)

Il s'agit d'étudier comment un mode de réussite, identifié à l'étape 2, participe à la survenue d'une situation risquée pour le patient. Il existe deux types de fragilisation des modes de réussite : une fragilité interne (méconnaissance, absence de définition, de partage du mode de réussite) et une fragilité externe (éléments de contexte ou de la situation de travail qui rendent invalide un mode de réussite considéré comme valide, c'est-à-dire sécurisé). Pour définir le domaine de validité d'un mode de réussite, les participants devront analyser son domaine d'utilisation, son domaine d'exclusion et les conditions d'utilisation du mode de réussite.

Exemple de mode de réussite risqué

Exemple

L'interne prend en charge le patient en soins palliatifs en l'absence d'informations indispensables ou d'encadrement. S'il est encadré, il l'est par un manipulateur ou un interne peu expérimenté.

Étape 4 : sécuriser le processus de soin (environ 30 minutes)

Trois axes de sécurisation seront discutés :

1. Recenser les situations sécurisées (Go) et les situations risquées (No Go) ;
2. Définir des mesures techniques, humaines et organisationnelles ;
3. Si les mesures définies sont inapplicables, continuer la réflexion sous un angle différent, dans d'autres espaces (groupes de travail, commissions d'établissement, séminaire, etc.) et à d'autres niveaux de l'organisation.

Actions à définir pour ce mode de réussite sécurisé

Exemple

L'interne prend en charge un patient en soins palliatifs alors que :

▷ L'équipe a récupéré les informations indispensables ;

▷ Le radiothérapeute senior est disponible à des étapes clés ;

▷ Et/ou que le manipulateur est expérimenté ;

▷ Et/ou que l'interne est suffisamment formé et expérimenté pour qu'ils puissent l'aider, le former, l'encadrer, détecter ses erreurs, etc.

A4

Bonne pratique n°4
La formation interne

Secteur d'activité où la bonne pratique a été mise en œuvre : site pétrochimique.

Objectifs recherchés :

- Faire prendre conscience à chaque membre de l'équipe opérationnelle de son rôle et de sa responsabilité dans la sécurité des unités ;
- Adopter un langage commun et parvenir à une meilleure compréhension/perception de la sécurité des systèmes techniques par les équipes opérationnelles.

Description :

La direction a créé un service inspection instrumentation pour suivre et gérer les barrières de sécurité instrumentées et a chargé cette équipe de mettre en place une sensibilisation de l'ensemble des équipes concernée par la sécurité des systèmes techniques.

Une nouvelle norme internationale sur la sécurité fonctionnelle a servi de base pour élaborer les formations nécessaires. Elle s'articule autour de trois axes :

- Le rôle et la responsabilité de chaque acteur ;
- La compétence des acteurs dans leur domaine d'action ;
- La planification de toutes les tâches à effectuer.

La première action a été de sensibiliser le personnel d'exploitation par l'organisation de ¼ d'heure sécurité, réunissant de 50 à 100 personnes. Le rôle et la responsabilité de l'exploitant ont été développés en prenant des exemples concrets de bonnes pratiques et de mauvaises habitudes. Une feuille de présence attestait du suivi de cette sensibilisation.

Deux modules de formation ont ensuite été développés, un pour les ingénieurs et un pour les techniciens. La formation se terminait par un examen de validation des acquis. Une liste du personnel qualifié a été mise en réseau et distribuée à la direction du site. Elle a servi de base aux audits de terrain sur la vérification des compétences.

Cette formation a permis à chacun de mieux comprendre les tâches des autres et a remis en cause des procédures importantes comme la gestion du changement et les descriptions de fonctions du personnel.

Indicateurs ou modalités d'appréciation

L'indicateur le plus approprié est le pourcentage de personnes formées sur le nombre de personnes concernées. Le second est le nombre de personnes non formées trouvées en action lors d'audits.

A5

Bonne pratique n°5
Sous-traitance et maîtrise partagée des risques

Secteur d'activité où la bonne pratique a été mise en œuvre : industries de systèmes techniques.

Objectif recherché

La déclinaison de ces bonnes pratiques permettra au donneur d'ordre et aux sous-traitants de travailler plus sereinement. Elles contribuent au développement de la culture de sécurité à travers une conscience mieux partagée, avec des mesures et pratiques pour une meilleure maîtrise des risques majeurs.

Contexte

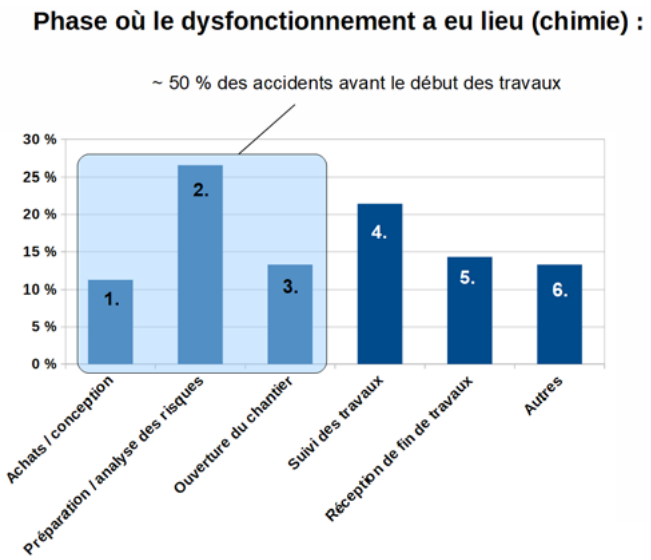


FIGURE 20 : *Dans le secteur de la chimie par exemple, 50 % des dysfonctionnements ont lieu avant le début des travaux*

Description : Les bonnes pratiques pour une maîtrise partagée des risques en cas de sous-traitance

1. Achats de prestations

- ▷ Lister les contraintes d'intervention (en temps, en zone, en limitation d'outils, ergonomie, etc.) ;
- ▷ Détailler les exigences (qualité des matériaux, conditions de fonctionnement) dans un cahier des charges ;
- ▷ Faire valider par les services techniques le choix des équipements retenus ;
- ▷ Prendre des prestataires qualifiés pour la gestion des risques de l'intervention ;
- ▷ Faire participer les services utilisateurs (opérateurs, maintenance, etc.) ;

- ▷ Préciser les qualifications nécessaires (ATEX, électrique) ;
- ▷ Détailler les risques présents dans la zone ;
- ▷ Anticiper la coactivité ;
- ▷ Intégrer le contrôle de la prestation sous-traitée ;
- ▷ Exiger le plan de contrôle des pièces achetées par le sous-traitant ;
- ▷ Fixer contractuellement un taux d'encadrement des prestataires.

2. Préparation du chantier

- ▷ Lister les risques de chacun : exploitant et sous-traitant ;
- ▷ Réaliser une analyse de risques commune ;
- ▷ Intégrer les risques liés à la coactivité (interne et externe) ;
- ▷ Clarifier les rôles et responsabilités de chaque acteur : qui fournit quoi en termes de sécurité ? Qui fait quoi en termes de contrôle ?
- ▷ Intégrer une check-list des contrôles à effectuer ;
- ▷ Vérifier l'adéquation des qualifications du personnel amené à intervenir ;
- ▷ Visiter les zones d'intervention avec un représentant du sous-traitant (zones de travaux, zones de stockage) afin de visualiser les risques, les contraintes, la signalétique ;
- ▷ Préparer le phasage en intégrant les points d'arrêt et les points de contrôle (ou points d'alerte) ;
- ▷ Tracer cela dans le plan de prévention.

3. Ouverture du chantier

Cela doit constituer un point d'arrêt obligatoire où le donneur d'ordre vient s'assurer que :

- ▷ Les conditions réelles d'intervention sont en phase avec ce qui avait été prévu, notamment la réalité des consignations ;
- ▷ Il n'y a pas de risque supplémentaire par rapport aux risques identifiés lors de la préparation ;
- ▷ Il n'y a pas de coactivité imprévue (suite par exemple à des décalages de planning) ;
- ▷ L'ensemble des moyens de prévention prévus soient effectifs, qu'ils soient de la responsabilité de l'exploitant ou du sous-traitant (par exemple : consignation, lignage, mise à la terre, outils antidéflagrants, etc.) ;
- ▷ Les conditions réelles permettent de démarrer les travaux en sécurité comme le contrôle ATEX avant démarrage ou le contrôle d'atmosphère ;
- ▷ Le personnel du sous-traitant en place connaît bien les risques et les consignes à respecter ;
- ▷ Il possède les qualifications nécessaires ;
- ▷ Le sous-traitant connaît bien les points d'alerte et les points d'arrêts de son chantier ;
- ▷ On va travailler au bon endroit (ex : erreur de tuyau) ;
- ▷ Le représentant de l'exploitant présent lors de la préparation de chantier est présent ;
- ▷ Le personnel a été formé aux risques spécifiques du site.

L'exploitant doit prévoir d'adapter sa surveillance à la qualité de l'équipe du sous-traitant : intérimaires, personnes habituées au site, risques importants au moindre écart, etc. Et surtout en cas de **travaux en urgence** !

4. Suivi du chantier

- ▷ Pendant les travaux, veiller au respect effectif par le sous-traitant des procédures, mesures de sécurité et plans de contrôle ;
- ▷ Faire preuve d'une vigilance particulière lors de travaux par point chaud ou si zone ATEX ;

- ▷ Levée rapide des points d'arrêt ;
- ▷ Adapter sa surveillance selon les constats effectués ;
- ▷ Ne pas se reposer sur le « papier » (le plan de prévention papier n'évite pas les accidents, c'est son respect qui le permet).

Nota : l'exploitant doit se doter des compétences nécessaires pour être en mesure de contrôler le travail du sous-traitant (ex : soudures).

5. Fin des travaux et suite

- ▷ Accorder du temps au contrôle final une fois le chantier terminé ;
- ▷ Mettre en place une visite de réception après toute intervention et une check-list des points à vérifier avant remise en service (le cas échéant) ;
- ▷ Vérifier l'absence de matériel sur place après la fin des travaux ;
- ▷ Vérifier l'absence de points chauds résiduels par caméra thermique ;
- ▷ Vérifier le lignage ;
- ▷ Organiser un débriefing avec le ou les sous-traitants sur les conditions de l'intervention.

A6

Bonne pratique n°6 Développer des pratiques de fiabilité humaine

Secteur d'activité où cette bonne pratique a été mise en œuvre : industrie nucléaire, adaptable à d'autres secteurs d'activité.

Objectif recherché

Les pratiques de fiabilité humaine visent à assurer la meilleure conformité possible et éviter les erreurs lors d'interventions à fort enjeu de sécurité ou risque élevé. Elles permettent de protéger l'intervenant et de sécuriser l'intervention. Elles maintiennent l'anticipation et la synchronisation dans l'action.

Description

Les pratiques de fiabilisation humaine font partie des règles de l'art d'un opérateur.

Plusieurs pratiques de fiabilité sont proposées. Certaines sont utilisables dans tous secteurs d'activité et situations, d'autres en présence d'enjeux spécifiques où lors de tâches critiques qui peuvent avoir des conséquences irréversibles.

Pratiques utilisables dans tous secteurs d'activité et de situations :

- Pré-job briefing ;
- Minute d'arrêt ;
- Débriefing.

Pratiques de fiabilité à mettre en place lors d'enjeux spécifiques où lors de tâches critiques qui peuvent avoir des conséquences irréversibles :

- Communication sécurisée ;
- Contrôle croisé.

Le pré-job briefing

Si l'analyse de risque sert à préparer l'intervention, le pré-job briefing prépare l'équipe intervenante et vérifie que les conditions réelles de l'intervention sont conformes à la préparation, identifie les perturbateurs et les parades nécessaires.

Le pré-job briefing est un échange verbal court (environ 5 minutes) réalisé au plus près de l'intervention préparer l'action en toute sécurité.

Lors du pré-job briefing toute l'équipe intervenante doit être présente ainsi qu'une personne tierce connaissant l'activité.

L'analyse de risque et la description détaillée de l'intervention doivent avoir été étudiées par l'équipe intervenante avant le pré-job briefing.

L'équipe intervenante doit aborder les cinq points clés du pré-job briefing :

1. Les résultats attendus ;
2. Les risques incluant les scénarios du « pire » ;
3. Les situations propices aux erreurs ;
4. Les parades et scénarios alternatifs ;
5. Le retour d'expérience sur l'activité à mener.

Les rôles et responsabilités de chacun sont établis.

Le pré-job briefing laisse une large part d'expression aux intervenants, qui doivent connaître les risques et les parades de leur activité. Ce sont eux qui doivent les citer.

La minute d'arrêt

Elle a pour objectif d'évaluer la situation de travail sur le terrain juste avant de commencer l'intervention, après son interruption ou lors d'un événement inattendu pour ne pas se laisser embarquer trop rapidement dans l'action.

Mise en œuvre :

- ▷ Avant de commencer, l'intervenant s'arrête et s'interroge sur l'environnement de travail (conditions d'accès, sécurité, etc.) ;
- ▷ Il désigne et nomme ce qui concerne son activité (numéro de tranche, de voie, le matériel, documents à utiliser).

Si l'intervention est interrompue, avant de reprendre l'activité :

- ▷ Il repère le point d'interruption de son activité ;
- ▷ Au retour il désigne et nomme ce qui concerne son activité (numéro de tranche, de voie, le matériel, ligne de la procédure, etc.).

Si l'intervention ne se déroule pas comme prévu :

- ▷ Il s'arrête ;
- ▷ Il analyse la situation et élabore un mode de reprise de l'intervention ;
- ▷ Il fait valider son analyse par un responsable ou référent technique ;
- ▷ Il reprend l'intervention lorsque les conditions de reprise sont partagées.

Le débriefing

Il permet de tirer profit du vécu de l'intervention et de favoriser les suivantes.

Mise en œuvre :

- ▷ Réunir tous les intervenants juste après l'intervention avec le management direct ;
- ▷ Identifier les difficultés rencontrées, les écarts et situations piégeuses ;
- ▷ Identifier les améliorations possibles, organiser leur large partage.

Communication sécurisée

La communication sécurisée garantit que la transmission d'une information est comprise et renforce la mémorisation de l'intervenant.

Mise en œuvre :

- ▷ L'émetteur formule un message clair, complet et concis et évite les termes ambigus du type « va vérifier la pompe » ;
- ▷ L'émetteur précise le nom du récepteur s'il y a plus de deux personnes dans l'échange ;
- ▷ Si un matériel est cité, l'émetteur donne son repère fonctionnel complet, y compris le numéro de la tranche ;

- ▷ Le récepteur répète à l'identique le message de l'émetteur pour confirmation ;
- ▷ L'émetteur valide après retour d'information par « c'est correct ».

Le contrôle croisé

Il permet d'assurer la conformité à la procédure pour une étape critique irréversible.
Sa mise en œuvre associe un intervenant et un « valideur » :

- ▷ L'intervenant expose au valideur l'action qui va être réalisée et les conditions préalables requises ;
- ▷ Le valideur vérifie la cohérence entre l'intention énoncée et les conditions réelles ;
- ▷ Le valideur valide l'action ;
- ▷ L'intervenant la réalise ;
- ▷ Le valideur confirme que l'action a été réalisée conformément à ce qui a été énoncé.

A7

Bonne pratique n°7
Prendre en compte les composantes organisationnelles des lignes de défense

Secteur d'activité où cette bonne pratique a été mise en œuvre : Tous secteurs. Ces bonnes pratiques sont issues de l'analyse des accidents enregistrés dans la base Aria[6].

Objectif recherché :

La mise en place d'une organisation robuste et bienveillante permet à l'exploitant :

- ▷ D'identifier les situations à risque et les signaux précurseurs ;
- ▷ D'anticiper et de préparer les opérateurs aux situations dégradées ;
- ▷ De ne laisser aucune place à l'improvisation.

Les composantes organisationnelles permettent de garantir la fiabilité des composantes techniques et humaines des lignes de défense.

Description :

Ci-dessous sont listées les grandes familles des composantes organisationnelles des lignes de défense organisationnelles.

Gestion des risques :

Identification des risques :

Avoir une démarche d'évaluation exhaustive des risques conformes aux bonnes pratiques de la profession et à la réglementation en vigueur et périodiquement mise à jour.

Choix des équipements et systèmes techniques :

Le choix des techniques, matériels, fonctionnalités, équipements et systèmes techniques doit être conforme aux bonnes pratiques de la profession ou à la réglementation en vigueur. Il doit être réalisé en lien avec les conditions de fonctionnement normales et dégradées de l'équipement et du procédé et selon les conclusions de l'identification des risques.

6. La base de données ARIA (Analyse, Recherche et Information sur les Accidents) répertorie les incidents, accidents ou presque accidents qui ont porté, ou auraient pu porter atteinte à la santé ou la sécurité publiques ou à l'environnement : https://www.aria.developpement-durable.gouv.fr/

Culture de sécurité :

Une faible culture de sécurité se traduit par des violations routinières des procédures de sécurité à tous les niveaux, une priorité donnée à la productivité et aux économies sur la sécurité, un faible engagement de la hiérarchie (qui ne montre pas l'exemple), l'absence de moyens pour la sécurité, la méconnaissance des risques, le manque d'actualisation des procédures, etc.

Retour d'expérience (REX) :

L'organisation permet de connaître, analyser et tirer les leçons des incidents et accidents, et de diffuser ces enseignements en interne et en externe.

Organisation des contrôles :

L'organisation assure le contrôle périodique et suffisant de la conformité, du bon fonctionnement et de l'intégrité des équipements/systèmes techniques/barrières du site. Elle garantit également la traçabilité de ces contrôles et l'application effective des actions correctives identifiées.

Communication :

Communication :

Transmission efficace de consignes et d'informations nécessaires à la production normale et à la sécurité du site. Cette circulation d'information doit se faire dans les deux sens hiérarchiques et en transversal (par exemple entre service maintenance et conduite).

Prise en compte des lanceurs d'alerte :

L'exploitant doit mettre en place une organisation qui permette de remonter des signaux précurseurs, notamment par des lanceurs d'alerte du terrain. L'exploitant doit écouter ces messages avec bienveillance.

Conditions de travail :

Formation et qualification des personnels par une organisation comprenant :

- L'identification du socle minimal de compétences pour chaque poste de travail ;
- Au besoin un système d'évaluation, d'habilitation et de mise à jour périodique des connaissances sur des postes clés, incluant le volet sécurité ;
- L'intégration des salariés extérieurs dans le processus.

Organisation du travail et encadrement :

Les tâches doivent être clairement définies et réparties.

Les ressources doivent être adaptées à la charge de travail réelle (cas des congés maladie, vacances, etc.) et à la complexité de la tâche. Le suivi et le contrôle hiérarchique des opérations doit être planifié, y compris celles confiées à des prestataires.

Environnement psychosocial de travail :

Conditions psychologiques et sociologiques de travail affectant les capacités physiques/cognitives/mentales de l'opérateur : manque de motivation, déresponsabilisation, stress, pression productive, objectifs incompatibles, mauvaise ambiance de travail, rivalité et agression verbale, culture d'entreprise favorisant la prise de risque, mauvaise compréhension du fonctionnement de l'organisation.

Procédures et consignes :

L'organisation doit intégrer une structure dont le rôle est l'identification des actions/phases nécessitant des procédures, consignes ou modes opératoires.

Les consignes doivent être rédigées en concertation avec les personnes qui devront les appliquer.

L'organisation doit prévoir leur mise à jour en fonction des évolutions des systèmes techniques et équipements. Ces documents doivent être clairs, facilement accessibles, compréhensibles par le personnel qui devra les appliquer, et prendre en compte la plupart des situations prévisibles des équipements et systèmes techniques (fonctionnement courant, mise en sécurité, marche dégradée, arrêt, etc.).

Environnement physique de travail :

L'organisation doit prévoir le maintien de l'ordre, de la propreté de l'unité ou des différents espaces de vie et de travail du site. Elle doit intégrer les conditions concrètes de travail affectant les capacités physiques/cognitives/intellectuelles des agents : bruit, lumière, température, qualité de l'air, etc.

Ergonomie :

L'organisation doit adapter les équipements (matériels et logiciels) et postes de travail à leur usage par les opérateurs, c'est-à-dire veiller à ce qu'ils soient compatibles avec les capacités physiques et cognitives des agents. Ce travail comprend l'ergonomie du poste de conduite (hiérarchisation des alarmes, indicateur de fausses alarmes, etc.) et des ateliers.

Intégrer ces critères lors de l'analyse des risques garantit que l'organisation prenne en compte tous les facteurs initiateurs d'un événement, afin d'apporter des réponses concrètes.

Abréviations et lexique

Dans la mesure du possible, la terminologie utilisée est celle du lexique illustré de la sécurité[7] mis en place par l'Icsi sur son blog[8] dédié à la prévention des accidents les plus graves. Cette terminologie est commune à tous les groupes d'échange, ou à défaut celle des référentiels officiels s'ils sont suffisamment explicites pour le public visé par le groupe.

Le lexique complète l'abécédaire de l'Icsi pour quelques termes qui méritent une définition particulière, soit parce que leur signification dans le langage courant est ambiguë ou imprécise, soit parce qu'ils sont absents des textes officiels, ou que leur définition n'est pas adaptée au public visé.

CCPS : Center for Chemical Process Safety

IOCP : International association Oil & Gaz Producers

AIChE : American Institute of Chemical Engineers

AIEA : Agence Internationale de l'Energie Atomique

Wenra : Western European Nuclear Regulators Association

Wano : World Association of Nuclear Operators

7. Icsi (2019). Lexique illustré de la sécurité : https://leblog.icsi-eu.org/2019/01/31/lexique-illustre-du-chemin-de-laccident/
8. Blog de l'Icsi « Porter le regard sur l'essentiel : prévenir les accidents graves, mortels et technologiques majeurs » : https://leblog.icsi-eu.org/

Reproduction de ce document

Vous pouvez télécharger le document (et d'autres versions des *Cahiers de la sécurité industrielle*) au format PDF depuis le site web de l'Icsi, www.icsi-eu.org.

Éditeur : **Institut pour une culture de sécurité industrielle**
Association de loi 1901

http://www.icsi-eu.org/

6 allée Emile Monso – BP 34038
31029 Toulouse Cedex 4
France

Téléphone : +33 (0) 532 093 770
Courriel : contact@icsi-eu.org

ISSN 2100-3874

6 allée Émile Monso ZAC
du Palays - BP 34038
31029 Toulouse cedex 4

www.icsi-eu.org