AIDES
A LA REFLEXION

Le monde change, la sécurité industrielle aussi

Humain, numérique, nouvelles organisations : 10 points-clés à l'horizon 2040

Groupe scientifique d'analyse stratégique « Opérateur du futur »

Édition coordonnée par Caroline Kamaté

n° 2023-04

THÉMATIQUE

Opérateur du futur

Les Cahiers de la sécurité industrielle

FONCSI
Fondation pour une culture de sécurité industrielle

La Fondation pour une Culture de Sécurité Industrielle (Foncsi) est une Fondation de recherche reconnue d'utilité publique par décret en date du 18 avril 2005. Elle a pour ambitions de :

- contribuer à l'amélioration de la sécurité dans les entreprises industrielles de toutes tailles, de tous secteurs d'activité ;
- rechercher, pour une meilleure compréhension mutuelle et en vue de l'élaboration d'un compromis durable entre les entreprises à risques et la société civile, les conditions et la pratique d'un débat ouvert prenant en compte les différentes dimensions du risque ;
- favoriser l'acculturation de l'ensemble des acteurs de la société aux problèmes des risques et de la sécurité.

Pour atteindre ces objectifs, la Fondation favorise le rapprochement entre les chercheurs de toutes disciplines et les différents partenaires autour de la question de la sécurité industrielle : entreprises, collectivités, organisations syndicales, associations. Elle incite également à dépasser les clivages disciplinaires habituels et à favoriser, pour l'ensemble des questions, les croisements entre les sciences de l'ingénieur et les sciences humaines et sociales.

FONCSI
Fondation pour une culture de sécurité industrielle

Fondation pour une culture de sécurité industrielle
Fondation de recherche reconnue d'utilité publique

http://www.foncsi.org/

6 allée Émile Monso – CS 22760
31 077 Toulouse Cedex 4
France

Twitter : @LaFoncsi
Courriel : contact@foncsi.org

Ce document

Titre	Le monde change, la sécurité industrielle aussi
Sous-titre	Humain, numérique, nouvelles organisations : 10 points-clés à l'horizon 2040
Mots clés	Digitalisation, évolutions socio-démographiques, complexité, paradigmes de sécurité, gouvernance des risques
Date de publication	Mai 2023

Ce *Cahier de la sécurité industrielle* est issu des travaux du groupe scientifique d'analyse stratégique « Opérateur du futur - Génération des travailleurs à venir 2030-2040 » de la Foncsi. Ce groupe a rassemblé, autour d'un noyau de chercheurs académiques, des experts d'organisations mécènes de la Foncsi. Il s'est réuni à une quinzaine de reprises afin d'explorer les impacts à l'horizon 2040 sur la sécurité industrielle des évolutions du monde en cours et à venir. Ce *Cahier* présente une synthèse de ses réflexions.

À propos de la coordinatrice

Caroline Kamaté est titulaire d'un doctorat en biologie. Elle a une expérience postdoctorale en milieu universitaire (University Medical Center, Utrecht, Pays-Bas) et en industrie (Sanofi-Aventis, France). Son intérêt pour la communication scientifique l'a amenée à rejoindre la Foncsi en 2007 où elle est chargée de la gestion de programmes de recherche et de la diffusion de résultats.

Pour citer ce document

GSAS « Opérateur du futur » (2023). Le monde change, la sécurité industrielle aussi - Humain, numérique, nouvelles organisations : 10 points-clés à l'horizon 2040. Numéro 2023-04 de la collection les *Cahiers de la sécurité industrielle*, Fondation pour une culture de sécurité industrielle, Toulouse, France. DOI : 10.57071/240dpc

Gratuitement téléchargeable sur : www.foncsi.org

Avant-propos

Démographie, avancées technologiques, mondialisation, désagrégation industrielle, complexité et interdépendance des systèmes… À l'horizon 2030-40, les mégatendances évolutives qui traversent notre monde, nos sociétés et donc le monde des activités industrielles à risque, obligent à revisiter l'approche de la sécurité. Quels impacts ces évolutions pourraient-elles avoir sur les directions HSE et, au-delà, sur les organisations ? Comment penser les nouveaux modes de production, les nouvelles organisations et les nouveaux profils professionnels requis en intégrant les évolutions prévisibles de la technologie, des générations de salariés, des attentes de la société ? Pourquoi et comment l'industrie à risque doit-elle adapter sa vision et ses actions sécurité pour faire face aux challenges de demain ?

Anticiper « la sécurité du futur » est donc une priorité pour l'industrie en général, et pour tous les mécènes de la Foncsi. C'est pourquoi la Foncsi, en partenariat avec des organisations qui la soutiennent (Airbus, EDF, EPSF, IRSN, Eurovia, GRTgaz, SNCF et TotalEnergies) a lancé une analyse stratégique sur ce thème. Ce programme de recherche en temps limité mais aux objectifs ambitieux a donné lieu à un séminaire académique international en novembre 2020, une conférence de restitution devant les organisations partenaires de la Foncsi en juillet 2021, et un livre collectif publié en *open access* dans la collection « SpringerBriefs in Safety Management ».

Ce *Cahier*, en présentant une synthèse de l'ensemble des résultats en 10 points, vient clore cette analyse stratégique et paver la route aux futurs travaux de la Foncsi.

Toulouse, le 8 février 2023

Caroline Kamaté,
Fondation pour une culture de sécurité industrielle (Foncsi)

Remerciements

Le Groupe scientifique d'analyse stratégique (GSAS) remercie chaleureusement les experts français et internationaux qui ont participé au projet et ont signé un chapitre dans le livre, ainsi que les experts qui lui ont accordé une audition, ou bien ont participé à l'atelier prospectif « sécurité ferroviaire » :

Allspaw John	Adaptive Capacity Labs, USA
Antonsen Stian	Université norvégienne de sciences et technologies (NTNU), Norvège
Baram Michael	Université de Boston (BU), USA
Barcellini Flore	Conservatoire national des arts et métiers (CNAM), France
Charlet Vincent	Fabrique de l'industrie, France
Chevet Pierre-Franck	Institut français du pétrole-Energies nouvelles, France
Davenne François	Union internationale des chemins de fer (UIC), France
De Boisboissel Gérard	Académie militaire de Saint-Cyr, France
Dorbec Loïc	Association française des gestionnaires d'infrastructures ferroviaires indépendants (AGIFI), France
Enlart Sandra	Université Paris-Nanterre, Dsides, France
Leriche Yann	Getlink, France
Messulam Pierre	SNCF, France
Richier André	Commission Européenne
Giraud Pierre-Noël	Mines ParisTech, France
Hadzilacos Rigas	Forum économique mondial
Ollivier Daniel	Thera Conseil, France
Pison Gilles	Institut national d'études démographiques (INED), France
Riquet Dominique	Parlement Européen
Rodriguez Jean-Hugues	Airbus, France
Shorrock Steven	Eurocontrol, France
Tosé Akira	Université de Niigata, Japon
Weil Thierry	Mines ParisTech, France

Sommaire

Introduction

Contexte : Le futur du travail et de l'industrie au cœur des préoccupations

Il n'existe pas de science permettant de prédire le futur, même proche. Il importe donc de rester humble face aux incertitudes lorsque l'on engage une réflexion sur l'avenir. Certaines hypothèses raisonnables peuvent néanmoins être faites. Et le fait que le travail et l'industrie à risque devraient faire face à d'énormes défis d'ici 2030-40 en fait partie.

En effet, notre monde subit une mutation radicale, globale, et, à l'échelle de l'histoire des sociétés, à un rythme extrêmement rapide. Le changement climatique, le vieillissement de la population occidentale, la délocalisation de la chaîne de production de valeur, la mondialisation, la financiarisation, la fragmentation en réseaux interdépendants des organisations, la complexification, la numérisation massive, la fabrication et le trafic intenses de données transforment non seulement le travail, la production et les organisations, mais également les attitudes des individus et de la société à leur égard (Pariès, 2022).

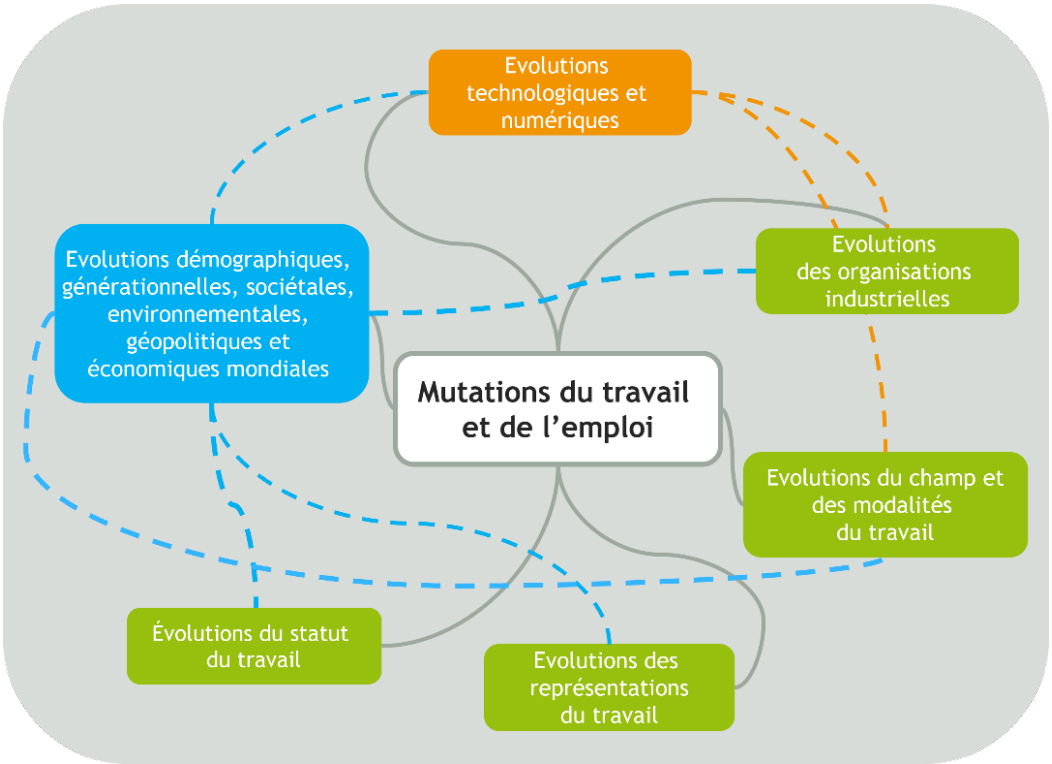

FIGURE 1 : Mégatendances impactant le travail et l'emploi, (très) inspiré de (Gaxie & Obadia, 2019)

Ces grands changements multidimensionnels, ces évolutions dénommées « mégatendances » sont interconnectées et s'influencent mutuellement. Cependant, par souci de simplification, nous distinguons 3 catégories :

1. Les évolutions technologiques ;
2. Les évolutions industrielles et socio-économiques ;
3. Les évolutions socio-démographiques, sociétales, environnementales, géopolitiques.

Étant donnés les enjeux pour l'industrie, l'économie et l'avenir des sociétés, les impacts sur le travail de ces forces de transformation globales sont au cœur des préoccupations de recherche, économiques et politiques de très haut niveau. Ils font l'objet de nombreuses études prospectives, plans nationaux et internationaux, rapports (Fig. 2).

FIGURE 2 : Le futur de l'industrie, un sujet brûlant, thème de nombreux think-tanks, plans et programmes

Qu'en est-il de la sécurité industrielle ?

Pour autant, bien que les impacts de l'automatisation/numérisation, du vieillissement, des changements socio-économiques et sociétaux sur la santé et la sécurité au travail soient largement étudiés[1], nous avons constaté que, de manière assez surprenante, les questions de risques technologiques et de sécurité industrielle n'étaient pas autant explorées par les études prospectives. Il existe peu de publications, de réunions, d'organisations qui discutent de l'influence des changements majeurs en cours et à venir sur la sécurité des activités industrielles à risque.

Pourtant, ces mégatendances, par les mutations profondes qu'elles entraînent en matière d'emplois, de compétences individuelles et collectives, d'organisation et de modalités du travail, de rapport au travail, d'attentes sociétales… questionnent des enjeux de sécurité qui ne doivent pas être négligés par les industries à risque.

C'est pourquoi la Foncsi, partant des préoccupations soulevées par ses organisations mécènes (industries de transport et d'énergie, autorités de contrôle et autres organismes) a lancé en 2019, une analyse stratégique sur « Opérateur du futur - Génération des travailleurs à venir 2030-2040 »[2].

L'analyse stratégique « Opérateur du futur » en un clin d'œil

Cette analyse visait à générer une recherche de qualité dans un délai relativement court et à créer un continuum entre la recherche, l'innovation et l'industrie. Elle comprenait 3 étapes principales, décrites ci-dessous (Fig. 3) :

1. L'état de l'art : la première étape établit un panorama de la littérature, prépare un plan d'analyse, reformule le problème et identifie des experts internationaux qui contribuent à la thématique de l'analyse stratégique. La fin de cette première phase est marquée par la tenue d'un séminaire international académique de deux jours avec certains des experts identifiés par le GSAS.
2. L'appropriation et la confrontation avec les pratiques industrielles : cette phase permet d'analyser les contributions des experts, et confronte ce matériel avec les pratiques industrielles. Elle se termine par un séminaire d'une demi-journée entre partenaires industriels afin de tirer les enseignements de cette analyse, sur les concepts et les pratiques.

1. Marsot, et al., 2021 ; Aublet-Cuvelier, Hery, & Malenfer, 2022 ; INRS, 2016 ; ILO, 2019
2. Imparfaitement, mais plus commodément dénommée « Opérateur du futur ».

3. La valorisation et diffusion des résultats : un livre en *open access* publié chez Springer est prévu pour rendre compte des travaux présentés et des débats qui se sont tenus lors du séminaire académique. Dans le prolongement des travaux, l'analyse stratégique produit un rapport de synthèse dans la collection de la Foncsi intitulée les *Cahiers de la sécurité industrielle* et, possiblement, d'autres publications[3].

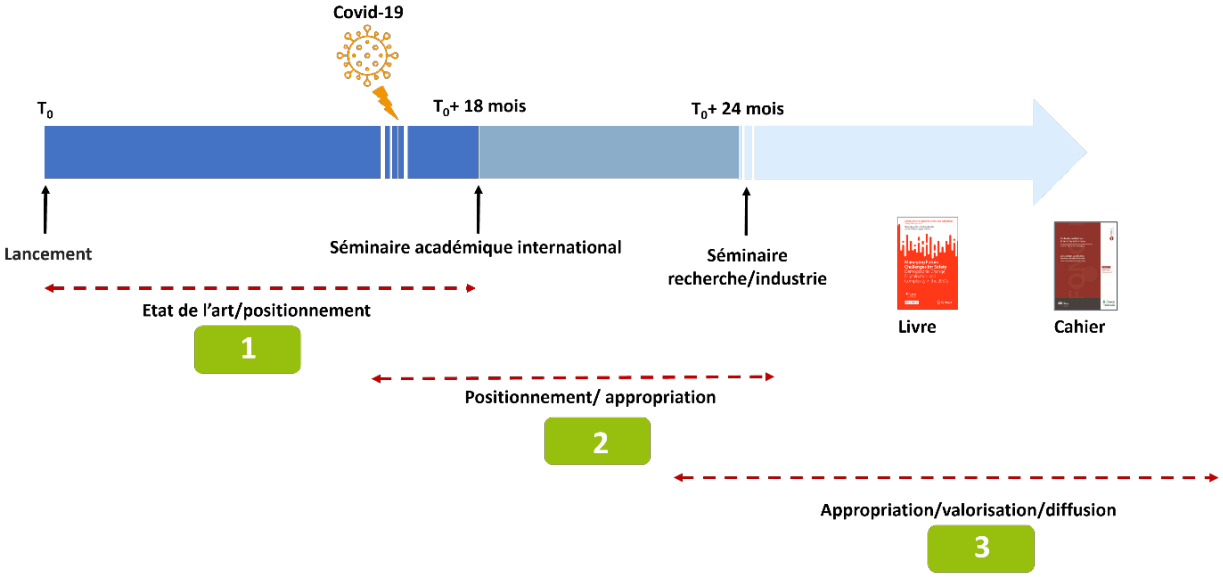

FIGURE 3 : Les différentes phases de l'analyse stratégique

Comme le montre le schéma, le calendrier de l'analyse n'a pas échappé aux impacts de la pandémie de Covid-19 qui a touché le monde à partir de 2020.

Le groupe scientifique d'analyse stratégique

Le projet a été mené par le groupe scientifique d'analyses stratégiques (GSAS) de la Foncsi. Ce dernier se compose d'un noyau permanent de chercheurs qui participent à l'ensemble des analyses stratégiques menées par la Foncsi :

- Corinne Bieder, Enac ;
- Hervé Laroche, ESCP Business School ;
- Jesús Villena López, Ergotec ;

ainsi que de la direction de la Foncsi :

- René Amalberti, directeur Foncsi ;
- Jean Pariès, directeur scientifique Foncsi/Icsi[4].

3. C'est le cas pour l'analyse « Opérateur du futur » puisque la synthèse d'un atelier ferroviaire a été publiée (Foncsi, 2021) et qu'un autre *Cahier de la sécurité industrielle* sera publié prochainement (Bieder, Bringing together humanity and technology in context, à paraître).
4. Institut pour une culture de sécurité industrielle, association avec laquelle la Foncsi entretient un lien historique : https://www.icsi-eu.org

À ce comité restreint, se sont adjoints des experts de l'industrie et d'autres organisations partenaires de la Foncsi largement reconnus dans le domaine de la sécurité et des risques :

- Florence Reuzeau, Airbus ;
- Raluca Ciobanu, EDF ;
- Laurent Cebulski & Bruno Dember, Autorité française de sécurité ferroviaire (EPSF) ;
- Franck Ollivier, Eurovia
- Nicolas Engler & Thierry Escaffre, GRTgaz ;
- Dounia Tazi, Icsi ;
- Alexandre Largier & Tania Navarro Rodriguez, Institut de radioprotection et de sûreté nucléaire (IRSN) ;
- Stella Duvenci-Langa & Cyril Cappi, SNCF ;
- Raphaël Waxin, TotalEnergies.

FIGURE 4 : Les mécènes qui ont participé à l'analyse stratégique

Les experts internationaux

Pour cette analyse stratégique, les perturbations liées à la crise de la Covid-19 ont empêché la tenue d'un séminaire académique résidentiel. Les sept experts internationaux identifiés et invités par le GSAS ont donc participé à un séminaire en distanciel au mois de novembre 2020, afin d'exposer leurs travaux au GSAS, de confronter leurs points de vue et de proposer des pistes d'amélioration :

- John Allspaw, Adaptive Capacity Labs, USA ;
- Stian Antonsen, Université norvégienne de sciences et technologies (NTNU), Norvège ;
- Michael Baram, Université de Boston (BU), USA ;
- Flore Barcellini, Cnam, France ;
- Gérard de Boisboissel, Académie militaire de Saint-Cyr, France ;
- Steven Shorrock, Eurocontrol, France ;
- Akira Tosé, Université de Niigata, Japon.

Ce Cahier de la sécurité industrielle

Objectifs

Au cours de l'analyse stratégique, le GSAS s'est focalisé sur les impacts potentiels des mégatendances susmentionnées sur trois dimensions essentielles de la sécurité :

1. La nature des risques et les modèles de sécurité ;
2. La culture de sécurité ;
3. La gouvernance de la sécurité.

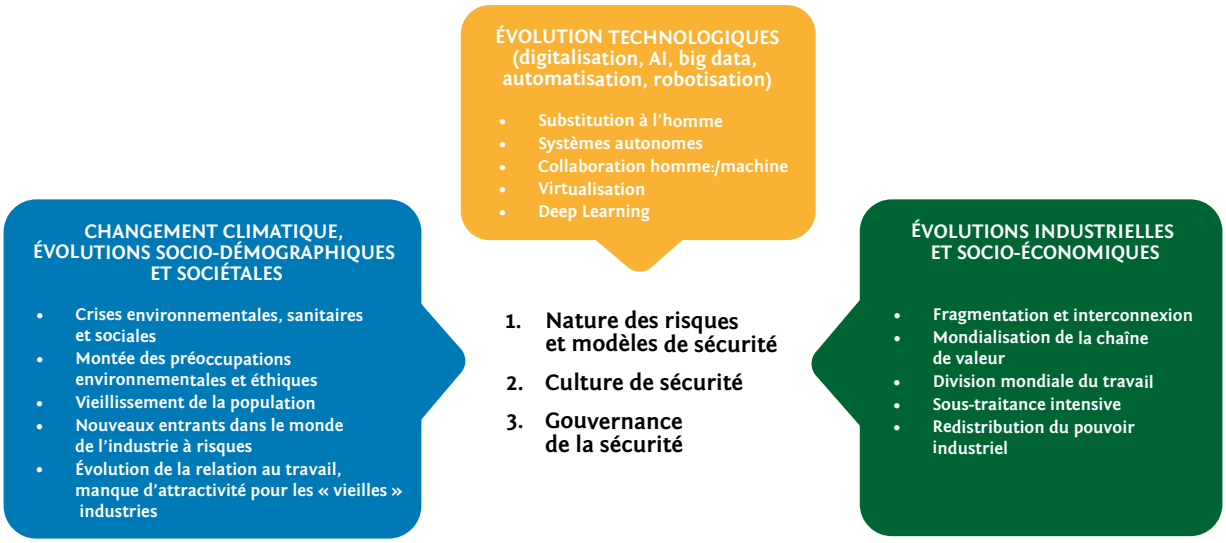

FIGURE 5 : Les mégatendances mondiales impactent des dimensions clés de la sécurité

Le GSAS a élaboré quelques questions de sécurité qui émergent lorsque l'industrie à haut risque est vue au prisme des mégatendances. Il s'est concentré sur les vulnérabilités qui pourraient apparaître ou se renforcer dans le futur, les menaces potentielles sur la(les) culture(s) de sécurité et a osé quelques conjectures sur les évolutions possibles de la gouvernance de la sécurité. Ce sont là quelques problèmes majeurs qui, du point de vue du groupe, devraient être abordés par les décideurs du monde des activités à risque pour faire face à un avenir complexe, instable et incertain.

Structure

Le *Cahier* est structuré en 2 parties qui couvrent au total 10 points clés :

- Partie I : 7 **défis « sécurité »** induits par les évolutions du monde ;
- Partie II : **3 pistes** pour appréhender la sécurité industrielle à l'horizon 2030-40.

Pour aller plus loin

Lectures

Nous renvoyons le lecteur intéressé à la section bibliographie en fin de document, et notamment aux autres productions de l'analyse stratégique sur « La contribution du travail humain à la sécurité dans les industries à risques à l'horizon 2040 » :

- le livre publié en *open access* chez Springer en octobre 2022 (en anglais) ;
- la synthèse de l'atelier ferroviaire publiée en mai 2021, gratuitement téléchargeable sur le site de la Foncsi ;
- un deuxième *Cahier de la sécurité industrielle* rédigé dans le cadre de cette analyse stratégique, axé sur l'humain et la technologie (Bieder, à paraître).

Travaux futurs

Certaines questions soulevées par cette analyse stratégique feront l'objet d'études plus poussées dans le cadre du programme 2023-2027 de la Foncsi (programme « Foncsi 4 »). Sont notamment inscrites à l'agenda Foncsi 4 les analyses stratégiques suivantes :

- Les pratiques de sécurité à l'ère de la transition numérique ;
- Compétences et carrières à l'horizon 2040 ;
- Gouvernance de la sécurité dans un périmètre élargi à la soutenabilité et la responsabilité sociale ;
- Améliorer l'intégration des risques industriels dans le reporting ESG.

Première partie

7 défis sécurité induits par les évolutions du monde

1

La complexité, l'incertitude et l'instabilité croissantes du monde impacteront la sécurité

Il semble raisonnable de conjecturer que la poursuite de l'accélération technologique, avec l'augmentation continue de la puissance de calcul, l'afflux des données, la perspective d'avoir systématiquement des jumeaux numériques, permet d'envisager une capacité d'anticipation encore plus grande qui augmente la fiabilité et la sécurité dans le domaine de fonctionnement connu des systèmes. Ainsi, les évolutions technologiques que nous connaissons s'accompagnent de gains significatifs en fiabilité et sécurité industrielle ce qui, d'ailleurs, est l'un de leurs objectifs. Néanmoins, il importe de considérer également les effets de bord.

Tout d'abord, le stockage et le trafic massifs de données dans un monde plus ouvert et largement connecté (avec notamment des capteurs, des capacités de transmission, des algorithmes qui sont parfois accessibles à tous), exposent les industries à haut risque, comme toute autre industrie, aux cybermenaces. On peut aisément imaginer les sévères conséquences d'une cyberattaque affectant la sécurité dans les secteurs d'importance vitale de l'énergie ou des transports, par exemple. À un autre niveau, lorsque les capacités (par exemple des algorithmes ou des satellites de communication) d'un autre pays sont utilisées pour exploiter un système à haut risque, les conditions géopolitiques peuvent avoir un impact direct sur le fonctionnement du système.

Ensuite, les nouvelles technologies ne pourront pas « faire tout, tout de suite ». Par exemple, dans les organisations à haut risque, le champ d'application de l'intelligence artificielle (IA) est encore limité, notamment pour des raisons critiques de sécurité[5] (Antonsen, 2022 ; Bieder & Villena-Lopez, 2022). Il est donc plus probable qu'à l'avenir, des technologies anciennes et avancées coexistent, et cette cohabitation pose des questions de sécurité.

Enfin, l'amélioration technologique substantielle associée à d'autres tendances évolutives telles que l'essor de l'IA, de plus en plus d'interconnexions et de réseaux, plus d'interactions entre les différentes parties prenantes (entreprises, régulateurs, pouvoirs publics, ONG, médias, citoyens, etc.) se fait au prix d'une complexité systémique, juridique et réglementaire accrue, ainsi que d'une redistribution des rôles et des responsabilités qui génèrent d'autres vulnérabilités et incertitudes. Une conséquence très importante de la complexification systémique est que des systèmes qui seront de plus en plus sûrs dans des conditions normales, c'est-à-dire dans leur domaine connu de fonctionnement, auront un comportement de plus en plus difficile à prévoir dans des conditions exceptionnelles. Ceci pourrait conduire à des catastrophes. En effet, bien que les propriétés respectives des composantes d'un système complexe soient généralement bien connues, ce ne sont pas ces propriétés individuelles, mais les *interactions et interdépendances* entre ces mêmes composantes qui déterminent majoritairement le comportement du système complexe global. Par exemple, le seul fait d'introduire une redondance (par exemple, deux pompes au lieu d'une) fait que la fiabilité individuelle du composant (la pompe) devient un contributeur de second ordre à la fiabilité globale, le facteur dominant étant les modes communs de défaillance. Et ces interactions induisent, hors du fonctionnement nominal mais aussi *dans le cadre* de leur fonctionnement nominal, des comportements « émergents » inattendus, imprévisibles, et non linéaires (effet papillon, cascade, avalanche, résonance, etc.) dont certains peuvent s'avérer catastrophiques. Le futur pourrait donc voir une plus grande vraisemblance d'occurrence d'« accidents normaux », au sens de (Perrow, 1999), c'est-à-dire d'accidents non pas liés à un comportement défaillant, mais à un comportement « normal » et imprévu du système. Ainsi, de nouvelles vulnérabilités émergeront, alors que les exigences sociales de sécurité seront probablement accrues.

5. Absence de confiance, pas de preuve d'innocuité sur les systèmes critiques.

Défi #1 : La complexité, l'incertitude et l'instabilité croissantes du monde impacteront la sécurité

Point clé

Capacité de calcul croissante, données massives :

- Plus de fiabilité et de sécurité dans le domaine connu de fonctionnement des systèmes ;
- Systèmes plus ouverts, plus interconnectés, cohabitation anciennes/nouvelles technologies, complexité accrue… ;
- Nouvelles vulnérabilités, risque résiduel imprévisible et potentiellement catastrophique.

2

Les qualités uniques des opérateurs humains seront toujours nécessaires à la sécurité

La formidable accélération technologique, notamment en matière d'IA, interroge la place et le rôle de l'homme au regard de ses capacités humaines uniques, dans le management, mais aussi dans la gouvernance de la sécurité (Bieder, à paraître).

Premièrement, malgré l'automatisation massive et l'autonomie grandissante des systèmes liées à l'essor des technologies reposant sur l'IA auto-apprenante, les interventions humaines sont toujours nécessaires dans la plupart des opérations. Par exemple, dans le secteur militaire particulièrement en pointe en matière de technologies autonomes, comme l'a exposé (De Boisboissel, 2022) les hommes restent indispensables aux opérations. En effet, malgré la délégation de tâches à des machines, les opérateurs sont les plus à même d'apprécier une situation réelle évolutive au plus près ; de son côté, le leader doit toujours garder le contrôle sur les systèmes autonomes et reste responsable de la prise de décision. De plus, l'humain est la composante la plus capable d'adaptation des systèmes complexes à évolution rapide et imprévisible, celle qui, dans de nombreux cas, leur permet de continuer à fonctionner malgré les failles (Cook, 2020). L'essor des nouvelles technologies et notamment celui de l'IA, qui modifie son comportement en fonction de son apprentissage, favorise l'émergence de nouvelles incertitudes. Opérer en toute sécurité dans ces conditions plus incertaines sollicite plus que jamais des caractéristiques spécifiquement humaines. Comme les travaux de (Shorrock, 2022) sur les personnels de santé pendant la crise Covid le montrent, c'est leur analyse et leur compréhension de la réalité du travail de terrain, leur imagination et leur intelligence collective qui a permis à ces professionnels de faire face aux défis rencontrés et de prévenir au mieux les préjudices pour les patients comme pour les soignants.

Ainsi, anticipation, imagination, intelligence collective, adaptabilité, diversité, perspicacité, créativité, empathie, sagesse… apparaissent comme autant de propriétés spécifiques à l'homme qui sont essentielles à la sécurité (Dekker, 2015) et le resteront sans doute encore longtemps.

Défi #2 : Les qualités uniques des opérateurs humains seront toujours nécessaires à la sécurité

Point clé

L'humain :

- ▷ garde le contrôle des systèmes autonomes ;
- ▷ conserve la responsabilité de la prise de décision ;
- ▷ est capable d'adaptation en situation à évolution rapide et imprévisible.

Valeurs et propriétés spécifiques à l'humain (éthique, morale, créativité, empathie, intelligence collective, adaptabilité…) restent essentielles à la sécurité.

3

Le « challenge de compétences », y compris pour assurer la sécurité, sera considérable

Si les trois premières révolutions industrielles correspondent respectivement à l'avènement de la machine à vapeur, de l'électricité et des ordinateurs personnels, la période que nous vivons et que l'on désigne parfois comme quatrième révolution technologique, fait référence à la création et au déploiement de nouvelles technologies qui fusionnent les mondes physique, numérique et organique, impactant toutes les disciplines, les différentes économies et l'ensemble des industries (Balliester & Elsheiki, 2018).

Cette nouvelle ère est celle des technologies de l'information et de la communication, des technologies associées telles que l'IA, l'automatisation, la robotisation, les véhicules autonomes, l'IoT[6], etc. Parmi ces technologies, la robotisation et l'automatisation ne sont pas nouvelles, mais le rythme de leur développement en association avec la digitalisation et l'IA s'est considérablement accéléré et on peut imaginer que cela va se poursuivre dans un avenir proche. Un enjeu majeur pour l'industrie est d'adopter ces technologies afin de rester compétitive ; cela représente un énorme défi en matière de compétences. Cette évolution verra inévitablement certains emplois disparaître. Cependant, souvenons-nous que l'on a eu tendance à surestimer le volume d'emplois qui devaient être détruits par la première vague d'automatisation (Frey & Osborne, 2013). Si des emplois vont disparaître, de nombreux autres seront probablement créés (NESTA, 2017). Dans cet élan technologique (ainsi qu'au regard d'autres mégatendances telles que le vieillissement, le développement de l'économie verte, l'attractivité pour certains secteurs industriels qui chute fortement…), plutôt que de diminuer en nombre, des emplois vont se transformer. Et les pays occidentaux pourraient faire face non pas à une pénurie d'emplois, mais à un manque de main-d'œuvre qualifiée. Les réservoirs de jeunes talents se trouveront plutôt en Asie et, si le solde migratoire pourra en partie compenser cette pénurie de travailleurs hautement qualifiés, environ 1 milliard de personnes dans le monde (un tiers de la population active actuelle) devront être requalifiées d'ici 2025 (Zahidi, 2020). La reconversion des travailleurs dans les nouvelles technologies restera difficile d'ici 2030. Cinquante pour cent des travailleurs européens devront suivre une requalification professionnelle permanente, mais notre modèle actuel est trop lent et inadapté pour répondre à cette demande (Balliester & Elsheiki, 2018). La polarisation des emplois pourrait s'accélérer, les projections montrant une diminution des postes moyennement qualifiés au profit, d'une part d'un besoin croissant de travailleurs hautement qualifiés et, d'autre part, dans une plus large proportion, d'emplois moins qualifiés et moins bien rémunérés.

6. *Internet of Things* : internet des objets.

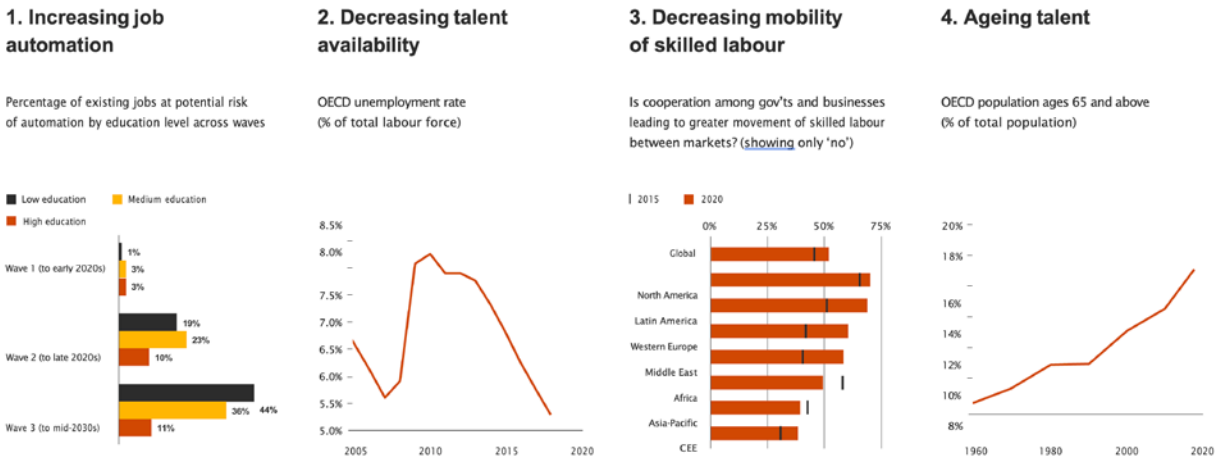

FIGURE 6 : Source : PwC, Will robots really steal our jobs? An international analysis (PWC, 2020)

Ensuite, la cohabitation entre les anciennes et les nouvelles technologies évoquées dans le point 1 illustre clairement un autre volet du défi de compétence auquel l'industrie à haut risque est déjà confrontée. Elle met non seulement en évidence la nécessité d'adapter la requalification ou l'embauche de personnel pour faire face à la pénurie de compétences numériques, mais pose également la question du transfert des compétences et savoir-faire de sécurité des travailleurs âgés, qui sont les derniers à utiliser les anciens systèmes et à en avoir une connaissance fine, aux jeunes générations.

Enfin, comme cela a été illustré lors de l'atelier sur la sécurité dans le monde ferroviaire du futur, les systèmes numériques sont aujourd'hui relativement génériques, et développés par des personnes qui connaissent mal les systèmes physiques en place et leurs caractéristiques opérationnelles (Foncsi, 2021). Plus généralement, la déconnexion entre les industries à haut risque et l'industrie numérique « désincarne » la conception de la partie IA des systèmes technologiques (Bieder, à paraître). Ainsi, au sein des organisations à risque, les compétences nécessaires à la vérification et l'approbation de technologies numériques seront de moins en moins disponibles, rendant de plus en plus probable une délégation à un tiers. La situation sera d'autant plus critique dans le cas où les réglementations entre le pays où les algorithmes sont développés et celui où ils sont mis en œuvre diffèrent, ce qui posera de sérieuses questions de responsabilité (Bieder, à paraître).

Défi #3 : Le « challenge de compétences », y compris pour assurer la sécurité, sera considérable

Point clé

Les évolutions en termes d'emplois en France et en Europe :

- plus de transformations que de destructions ;
- manque de mains d'œuvre qualifiée plutôt que pénurie d'emplois ;
- polarisation.

Le « challenge de compétences » en sécurité :

- modèle de formation qui peinera à assurer la (re)qualification d'une grande partie de la main-d'œuvre pour les nouvelles technologies ;
- difficile transfert des compétences et savoir-faire de sécurité des travailleurs âgés rompus aux technologies anciennes qui perdureront aux jeunes générations ;
- déficit de disponibilité de compétences numériques dans les entreprises à risque qui conduiront à une délégation à des tiers externes de la vérification et certification de technologies numériques.

4

Les décalages de culture organisationnelle, générationnelle…, mettront la culture de sécurité à l'épreuve

Les mutations que connaît notre monde telles que les évolutions socio-démographiques, l'accélération de la fragmentation et de l'interconnexion des organisations, la généralisation de l'externalisation remettent en question la culture de sécurité, que ce soit au sein des organisations ou entre elles (Bieder & Villena-Lopez, 2022). L'évolution des modalités de travail conduit à des équipes et des collectifs de travail plus éclatés. Ainsi, la construction et le maintien d'une culture de sécurité au sein de communautés de pratiques impliquent des modalités renouvelées de coopération, de collaboration et de communication.

La plupart des pays européens seront confrontés au vieillissement de leur main-d'œuvre comme c'est déjà le cas au Japon. Le recul de l'âge de la retraite, s'il ne s'accompagne pas d'une véritable stratégie amont de gestion des carrières longues, pourrait impacter la sécurité et la pérennité de la culture sécurité. Ainsi, pour éviter que les postes de direction ne soient monopolisés par les seniors et donc peu accessibles à la relève, le Japon expérimente des solutions opérationnelles, invitant les seniors à occuper des postes de formateurs en fin de carrière (Tosé & Tazi, 2022). La transposition d'une telle approche en Europe et notamment en France reste cependant pour le moins hypothétique. Ce vieillissement de la main-d'œuvre signifie également un élargissement de la fourchette d'âge du personnel d'une même organisation. Ceci entraine une diversité en matière d'aptitudes et de compétences, de relation au travail et à l'entreprise, parmi des employés qui sont appelés à travailler ensemble. Cela pourrait rendre le développement et le maintien d'une culture de sécurité commune plus difficile (Bieder & Villena-Lopez, 2022). La construction d'une culture de sécurité durable peut également être difficile dans des organisations fragmentées et diversifiées dont les objectifs peuvent différer voire devenir antagonistes, où le sentiment d'appartenance à une organisation, à une industrie, diminue, où les relations de travail se dégradent y compris en matière de sécurité (Bieder & Villena-Lopez, 2022).

La situation financière fragilisée de plusieurs grands acteurs industriels français pourrait avoir un impact majeur d'ici 2030, notamment entrainer un changement d'actionnariat et le transfert à l'étranger des comités de direction. Cela pourrait conduire à un décalage culturel significatif, avec une vision des pratiques et de la gestion de la sécurité au quotidien très différente de celle des Français. Plus frappant encore, l'émergence de 5 ou 6 poids lourds trans-sectoriels de l'industrie mondiale (énergie, transports, santé) pourrait, selon un modèle type GAFAM[7], représenter plus de 40 % de l'industrie à haut risque d'ici 2050. Cela fragiliserait considérablement le rôle des autorités nationales ou régionales dans la gouvernance des risques.

Défi #4 : Les décalages de culture organisationnelle, générationnelle…, mettront la culture de sécurité à l'épreuve

Point clé

Vieillissement des travailleurs, cohabitation de plusieurs générations de travailleurs, fragmentation, externalisation… :

- culture de sécurité fragilisée au sein des organisations à risque ;
- évolution des modèles industriels et économiques : délocalisation, mondialisation de la chaîne de valeur, logique actionnariale, montée en puissance de poids lourds trans-sectoriels ;
- décalage culturel impactant la gestion de la sécurité occidentale.

7. Google, Apple, Facebook (Meta), Amazon et Microsoft.

5

Les parties prenantes de la sécurité se multiplieront et se diversifieront

Initiée il y a des décennies, la fragmentation des organisations s'amplifie. Les industries à haut risque deviennent de plus en plus dépendantes de nouvelles activités et d'organisations associées qui ne font pas partie de leur industrie en tant que telle. À cet égard, la diffusion des technologies numériques conduit à brouiller les frontières industrielles. Cette multiplication et cette diversification des acteurs posent la question de nécessairement accroître la coordination entre ces organisations variées qui contribuent à l'exploitation des systèmes à haut risque. Parmi les nouveaux entrants, on citera les développeurs de logiciels, les fournisseurs de services de télécommunication ou les fournisseurs de données. Et il est à noter que la sécurité n'occupe pas toujours une place importante dans les préoccupations des diverses organisations impliquées dans les opérations des industries à risque (Bieder, à paraître).

Sur le plan des parties prenantes non-industrielles, les choses seront amenées à encore évoluer. Au-delà des industries à risque, le modèle actuel de gouvernance de la sécurité implique des régulateurs et des autorités de contrôle qui sont supposés être indépendants et représenter la voix du public (Bieder & Villena-Lopez, 2022). Cependant, si le rôle de la société civile dans la gouvernance des risques est renforcé dans les textes, la société civile en tant que telle reste absente de ce modèle. Parallèlement, la montée des attentes sociétales en matière de santé, d'environnement et d'éthique, la confiance décroissante envers les experts et les institutions, conduisent à une moindre acceptabilité sociale, voire au rejet des industries à haut risque et polluantes. Comme l'a encore démontré l'incendie de l'usine chimique Lubrizol dans le nord de la France (Rouen, 26 septembre 2019), les accidents, incidents et conséquences de la pollution s'étendent largement aux sphères sociales et politiques (Groupe de travail « Risques et territoires », 2023). Et même sans causer de décès ou de dégâts importants et immédiats, un événement peut avoir des répercussions sanitaires et sociales catastrophiques et à long terme. Face à cette volonté croissante d'implication des citoyens dans la gouvernance des risques industriels et des pollutions parce que ce sont des sujets qui les préoccupent, s'oriente-t-on dans un futur proche vers un modèle de gouvernance de la sécurité où les décisions seraient davantage entre les mains de la société civile et des politiques ? Quelles conséquences peut-on en attendre ?

Point clé

Défi #5 : Les parties prenantes de la sécurité se multiplieront et se diversifieront

Entrée de nouvelles parties prenantes industrielles dans l'écosystème des organisations à risque :

- frontières entre organisations brouillées ;
- dépendance accrue des organisations à risque d'entités externes à leurs secteurs ;
- une sécurité qui n'occupe pas forcément une place prioritaire chez les nouveaux entrants.

Montée des attentes de la société civile en termes d'environnement et de participation aux décisions concernant les activités industrielles à risques :

- conséquences sociales des incidents et accidents amplifiées ;
- exigence de portage réel des voix des riverains de sites à risques et, plus largement, des citoyens, impacte les modes de gouvernance de la sécurité des organisations à risque.

6

Le modèle de gouvernance basé sur le triptyque réglementation-contrôle-certification sera revisité

Les modalités de gouvernance actuelles englobent les trois domaines suivants : réglementation, certification et contrôle. Les organes de régulation et les autorités de contrôle indépendantes sont les piliers de ce modèle. Néanmoins, les mégatendances actuelles telles que l'accélération technologique, le déficit et la migration de compétences, le déplacement des grands centres de puissance industrielle, les évolutions sociétales concernant l'acceptation des risques, la confiance/défiance envers les décideurs et l'« autonomisation » des autres acteurs secouent et brouillent déjà ce schéma, et pourraient amener à revoir l'ensemble du modèle de réglementation et de surveillance tel qu'il existe aujourd'hui.

De nos jours, les exigences réglementaires sont élaborées par des organismes de réglementation soutenus par les principaux acteurs industriels occidentaux et imposées à une industrie dans son ensemble, à travers différentes organisations et même à l'échelle mondiale pour des secteurs réglementés au niveau international, comme l'aviation. Le conflit ukrainien et les évolutions de la Chine vont-ils exacerber la fragmentation en gros blocs géopolitiques, affaiblissant ainsi la coopération inter-blocs et renforçant la coopération intra-bloc ? Au contraire, la tendance précédemment engagée d'un déplacement des grandes entreprises d'Europe et d'Amérique du Nord vers l'Asie, et d'influence croissante des régulateurs non occidentaux se confirmera-t-elle à l'avenir ? Si cette dernière hypothèse se vérifiait, cela pourrait déstabiliser les régimes actuels de gouvernance de la sécurité (Bieder & Villena-Lopez, 2022). Cela conduirait-il à l'élaboration de nouvelles normes ? Les entreprises à haut risque déplaceraient-elles leur siège social dans des pays où les réglementations en matière de sécurité sont moins strictes ?

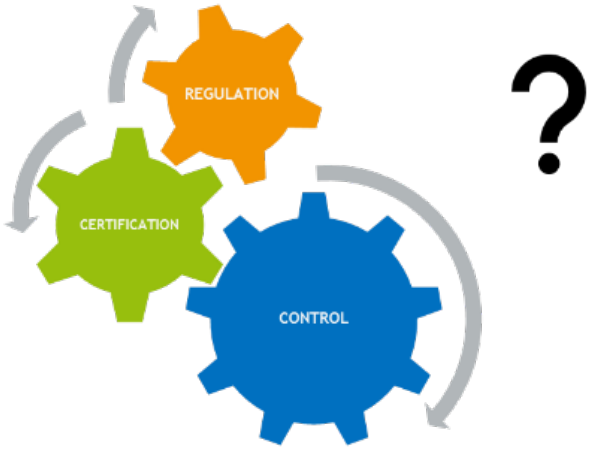

FIGURE 7 : Quelle évolution du modèle «classique» de gouvernance de la sécurité ?

Au niveau national, une redistribution des rôles, des responsabilités et du pouvoir entre les dépositaires historiques de la gouvernance de la sécurité, à savoir le régulateur, les autorités de contrôle et les opérateurs industriels, se dessine, basée sur la capacité (ou non) de ces acteurs à accéder aux compétences adaptées aux mégatendances. Or, les autorités de contrôle et de régulation font face à un manque croissant d'agents hautement qualifiés, en partie parce que ces derniers migrent vers le secteur privé, plus attractif. De plus, les autorités de sécurité adoptent et affichent certaines normes et standards élaborés par le secteur privé (qui n'est pas neutre) parce qu'elles n'ont pas toujours les moyens d'en assumer les coûts de développement ou de suivre le rythme

des évolutions notamment technologiques. Si le pouvoir des acteurs économiques devait s'accroître par rapport à celui des États et des autorités de régulation, on pourrait dans certains cas observer une « capture » des autorités de régulation, ce qui remettrait fortement en cause leur indépendance en matière de gouvernance de la sécurité (Baram & Bieder, 2022). Il existe un double déséquilibre entre acteurs industriels et autorités de contrôle, au détriment de ces dernières, pour ce qui est de l'accès aux données (stratégiques) concernant le fonctionnement détaillé des systèmes, et aux aptitudes et compétences requises pour traiter ces données. Cela place les autorités de sécurité dans une position où ces accès doivent être négociés avec les industriels. Cela pourrait éventuellement conduire à des conflits entre concepteurs, exploitants et autorités (Bieder & Villena-Lopez, 2022 ; Foncsi, 2021).

Parmi les enjeux liés aux évolutions technologiques, la certification des systèmes d'IA est certainement l'un des plus importants et soulève des questions sur le rôle des autorités de régulation et de contrôle et leurs relations avec les opérateurs industriels. Nous sommes, à ce jour, incapables de comprendre le fonctionnement des systèmes de *deep learning* sous une forme analytique qui permettrait de démontrer leur sécurité avec les méthodes reconnues. Cet enjeu majeur mobilise la plupart des efforts et, si l'aviation a initié un programme d'établissement de normes sur l'intelligence artificielle, dans d'autres secteurs cela reste difficile (EASA, 2020 ; ANITI, 2022).

Défi #6 : Le modèle de gouvernance basé sur le triptyque réglementation-contrôle-certification sera revisité

Point clé

Déficit de compétences chez autorités de contrôle et de régulation :

- contrôle et développement des standards sécurité migrent vers le secteur privé ;
- risque de « capture » des autorités ;
- accès aux données de sécurité et compétences pour les traiter : enjeu pouvant induire négociations voire conflits entre concepteurs, exploitants et autorités.

Boîte noire de fonctionnement de l'intelligence artificielle :

- certification de l'IA représente un enjeu majeur et questionne la sécurité.

7

L'approche actuelle et dominante de la sécurité fondée sur l'anticipation et le prescrit sera bousculée

Comment la sécurité est-elle actuellement « produite » dans l'industrie à haut risque ? Deux modes principaux peuvent être mentionnés. Nous désignons le premier comme « la sécurité telle que démontrée » : un modèle macro qui sous-tend la façon dont les industries sont attendues par des tiers (société, régulateurs) pour assurer la sécurité de leurs opérations. Ce modèle repose principalement sur l'anticipation, le respect des règles et la justification à l'externe. L'industrie à haut risque opère donc dans un cadre extérieur très strict avec des organismes de réglementation produisant des lois et des autorités de sécurité chargées de la certification et de la surveillance. Les industries à risque sont aussi fortement procéduralisées de l'intérieur, leurs pratiques étant régies par des procédures techniques et des processus organisationnels. Si la tendance, depuis les années quatre-vingt-dix, est celle d'une approche moins basée sur la conformité, et davantage sur la performance sécurité, permettant de prendre en compte les variabilités de contexte, plus de marge de manœuvre et plus d'implication des organisations industrielles dans la définition des normes, ce macro-modèle reste en pratique encore majoritairement basé sur l'anticipation, la normalisation, l'attribution claire des responsabilités reposant sur une approche de réduction de l'incertitude pour assurer le contrôle (total) des risques. Cependant, ce modèle visible de « sécurité telle que démontrée » coexiste avec un certain nombre de pratiques réelles, en situation, et cela à des niveaux opérationnels comme à celui de la gouvernance, qui ne sont pas totalement en ligne avec lui. Cet autre volet de production de sécurité, nous le désignerons par « sécurité telle que pratiquée ». Il comprend un ensemble de stratégies de sécurité élaborées pour s'adapter à une réalité instable, incertaine et complexe. Il ne peut pas être saisi par des audits et, au niveau de la gestion et de la gouvernance, ne reflète pas les limites formelles des rôles entre les acteurs et les organisations (Bieder & Villena-Lopez, 2022).

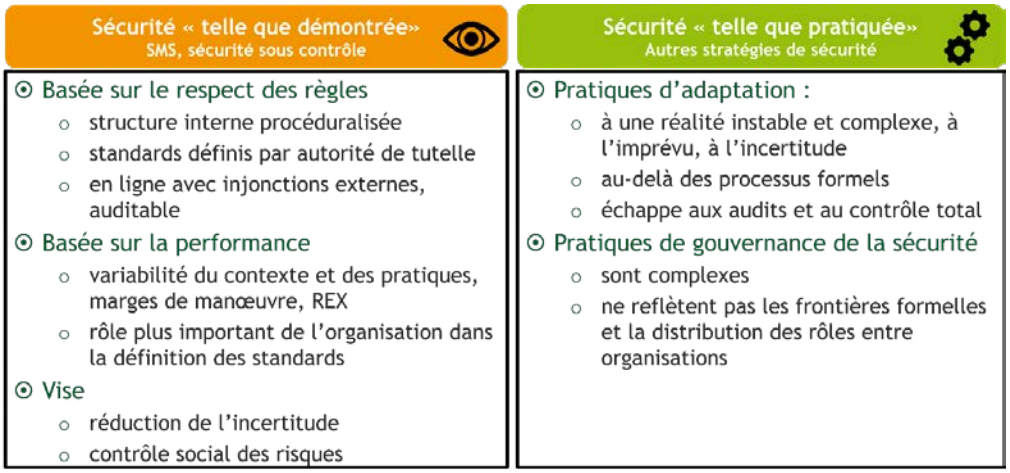

FIGURE 8 : Sécurité « telle que démontrée » et sécurité « telle que pratiquée »

Les mégatendances à l'horizon 2030-40 pourraient avoir un impact sur l'équilibre entre ces deux modèles de sécurité. Et les points de vue divergent sur la question de savoir de quel côté la balance penchera, si les deux types de fabrique de sécurité pourraient se renforcer mutuellement, voire même si nous ne sommes pas à l'orée d'un nouveau paradigme. Des arguments existent pour les diverses conjectures faites, mais l'humilité doit prévaloir quand on essaie d'imaginer des futurs possibles.

Défi #7 : L'approche actuelle et dominante de la sécurité fondée sur l'anticipation et le prescrit sera bousculée

Point clé

Actuellement, gestion et démonstration de sécurité des organisations à risques sont majoritairement basées sur l'anticipation, la réduction de l'incertitude, le respect des règles et la justification à l'externe, i.e. la sécurité « telle que démontrée ».

Les mégatendances évolutives en cours pourraient :

- déplacer le curseur vers une approche intégrant plus la fabrique moins visible et moins comptable de la sécurité reposant sur les pratiques d'opération et de gouvernance en situation réelle, i.e. la sécurité « telle que pratiquée »
- faire émerger un nouveau paradigme de gestion et de gouvernance de la sécurité des organisations à risque.

Deuxième partie

3 pistes pour appréhender la sécurité industrielle à l'horizon 2030-40

1

Adopter une approche plus ouverte de la sécurité

Comme précédemment évoqué, au regard des capacités d'anticipation grandissantes dans les domaines de fonctionnement connu des systèmes, le niveau global de sécurité devrait continuer à augmenter. Cependant, dans le même temps, la complexité croissante liée à l'accélération technologique, mais aussi aux autres mégatendances constatées, devrait entraîner une fragilisation, avec de nouveaux accidents « normaux », liés non pas à des anomalies, mais à l'imprévisibilité du comportement « normal » du système. Même si le niveau global de sécurité augmente, le risque résiduel d'accident imprévisible et catastrophique qui illustre les limites du contrôle invoqué par les discours officiels de sécurité, pourrait ne pas être accepté par la société dont les attentes évoluent également (Pariès, 2022).

Les mégatendances observées, si elles se confirment, impliquent un changement de regard sur la sécurité des organisations industrielles à risque. Penser la sécurité pour le futur nécessite d'adopter une approche plus ouverte « verticalement », en s'affranchissant d'un traitement isolé, niveau par niveau de la sécurité.

L'approche se doit également d'être plus ouverte « transversalement », c'est-à-dire en élargissant l'unité d'analyse ou de réflexion de la sécurité. Il s'agit de considérer la sécurité au même titre que les autres enjeux stratégiques, sans l'en dissocier, de sortir des sphères qui lui sont consacrées, en connectant la sécurité aux autres dimensions de l'entreprise mais aussi, dans une démarche plus globale, en replaçant l'industrie à risques en contexte dans un monde en pleine évolution.

Adopter cette approche plus large, plus intégrative, a des conséquences en termes de modèle et méthode de gestion de la sécurité, mais également en matière de déclinaison organisationnelle. Ces conséquences sont brièvement décrites dans la suite du propos.

Piste #1 : Adopter une approche plus ouverte de la sécurité

Point clé

Une approche plus ouverte de la sécurité :

- ▷ verticalement :
  - favoriser une vision d'ensemble de la sécurité de l'organisation qui dépasse son traitement niveau par niveau ;
- ▷ transversalement :
  - ne pas dissocier la sécurité des autres enjeux stratégiques de l'organisation ;
  - replacer l'organisation à risque dans le contexte évolutif global.

2

Dépasser les stratégies actuelles de gestion et de gouvernance de la sécurité

De nouvelles vulnérabilités systémiques sont donc générées par la complexification liée à l'accélération technologique. De plus, la croissance mondiale, le changement climatique, la multiplication des interfaces entre les différents acteurs de la société (entreprises, régulateurs, pouvoirs publics, ONG, médias, citoyens, etc.), l'hybridation des technologies, l'interconnexion galopante et la mise en réseau sont également source de complexification, d'incertitude. Une manifestation frappante de cette complexification du monde, entre autres, est le brouillage des frontières entre les risques, les rôles et responsabilités des acteurs, rendant la gestion et la gouvernance de la sécurité en silos moins pertinentes. Par exemple, la numérisation massive augmente l'exposition aux cybermenaces, qui peuvent avoir un impact sur la sécurité des organisations à haut risque. Or, la sûreté et la sécurité industrielles sont historiquement abordées séparément, que ce soit au niveau de la gouvernance, du management, ou des méthodes et même en termes de recherche (Bieder & Villena-Lopez, 2022). Un autre exemple qui appelle à une approche plus intégrative concerne les risques technologiques et naturels. En effet, le réchauffement climatique conduit à l'intensification et à la multiplication des événements climatiques extrêmes et à l'avenir, nous risquons d'être de plus en plus confrontés à des accidents NaTech[8] comme la catastrophe de Fukushima au Japon en 2011. Gérer la sécurité autrement signifie probablement qu'elle devrait plutôt être abordée dans son ensemble, au niveau du management, mais aussi au niveau de la gouvernance. Cesser de travailler en silos pour les autorités représenterait assurément une rupture avec l'approche actuelle de la gouvernance. Cela conduirait à une évolution des structures et des moyens de contrôle et, peut-être, des acteurs de la gouvernance (Matyjasik & Guenoun, 2019).

Le modèle de sécurité actuel, qui repose essentiellement sur la fiabilité des composantes des systèmes et sur les différentes juridictions de la gouvernance selon les familles de risque, devient insuffisant face aux tendances évolutives constatées. Il n'est, par nature, pas équipé pour faire face à l'imprévisible lié à la complexité. Penser la sécurité pour l'avenir implique de mettre les efforts sur un modèle plus englobant, avec des stratégies axées sur la fiabilité des systèmes dans leur ensemble et non composante par composante. D'autre part, jusqu'à présent, les démonstrations de sécurité relèvent majoritairement du volet visible et justifiable à l'externe des décisions et actions menées par les entreprises pour assurer la sécurité. Pour autant, on sait que la sécurité est produite aussi de manière moins prescrite, dans les pratiques en situation réelle et que, face à l'incertitude et l'instabilité grandissantes, cette « sécurité telle que pratiquée » pourrait voir sa contribution augmenter. Cela suppose pour l'avenir de plus intégrer ce volet moins visible, moins démontrable à l'externe de fabrication de la sécurité, de manière conceptuelle, mais aussi de mieux capitaliser dessus concrètement dans l'organisation. Attention, aller au-delà des stratégies de sécurité actuelles ne signifie pas pour autant qu'il faille les abandonner ! Ce modèle a fait ses preuves et a permis d'atteindre les très hauts niveaux de sécurité que connaissent actuellement les industries à risques. Cependant, pour faire face aux défis à venir, la stratégie de sécurité doit s'inscrire dans une approche fondée sur une théorie « plus forte », qui prend explicitement en compte les effets de la complexité.

Piste #2 : Dépasser les stratégies actuelles de gestion et de gouvernance de la sécurité

Point clé

- ▷ développer des approches intégratives plutôt que juridictionnelles des risques et de la sécurité :
  - sécurité ET sûreté ;
  - risques naturels ET technologiques.
- ▷ renforcer le modèle de gestion des risques basé sur l'anticipation et aller au-delà en mettant l'effort sur les théories et méthodologies prenant mieux en compte complexité et incertitude.

8. Un accident NaTech est un accident technologique engendré par un événement naturel.

3

Au niveau organisationnel : aligner prescrit, hiérarchie et autonomie

> *On pense au niveau poste de travail quand c'est déjà la conception et les processus qui sont en cause, au niveau processus quand c'est déjà la stratégie de l'entreprise qui est en cause, et au niveau décisionnel stratégique d'une entreprise quand c'est la chaîne de production de valeur mondiale qui génère des instabilités... Et si des études de sécurité sont menées pour les évolutions internes et locales de l'entreprise, ce n'est pas le cas des évolutions majeures qui affectent le monde.*
>
> (Pariès, 2022).

Au sein des organisations à haut risque, la sécurité est généralement gérée par couches successives, d'abord les équipements techniques, puis l'opérateur et son poste de travail, les équipes ou les collectifs de travail, les procédures, les processus, le service, les sites de production, etc. Mais avec l'augmentation de la complexité, les stratégies de sécurité peuvent de plus en plus avoir toujours un niveau de retard et courir le risque de perdre leur pertinence face à l'accélération des changements et des défis (Pariès, 2022).

L'accélération technologique conduit également à un débat sur l'innovation et la régulation de la sécurité, l'agenda des autorités de régulation et de contrôle ne suivant guère les innovations. Et parmi les différents discours, on peut en souligner deux. Celui qui repose sur l'impérieux besoin de benchmarker les nouvelles technologies – malgré des niveaux de sécurité dont il est actuellement impossible de démontrer la conformité ou non – de standardiser, de définir un cadre réglementaire. Et l'autre qui considère la nécessité d'innover, d'adopter rapidement les nouvelles technologies, notamment pour éviter de prendre du retard sur les pays qui osent le faire et se faire dépasser sur le marché. Cela implique de ne pas trop se focaliser sur des contraintes comme les démonstrations de sécurité, les freins techniques, sociétaux ou éthiques… Dans cette optique, attendre des réglementations ad hoc serait particulièrement bloquant et reviendrait à rater le « train de la concurrence ». « *L'innovation mène, la réglementation suit* » (Deloitte, 2016) : on parie sur le fait que ceux qui se lancent seront non seulement gagnants sur le plan économique, mais atteindront également des niveaux de sécurité plus élevés. Cela implique d'être proactif, de développer des « bulles » d'innovation isolées qui permettent de tester les nouveautés en s'affranchissant des lenteurs réglementaires (Foncsi, 2021).

Pour finir, si les dimensions systémiques de la sécurité dépassent la sphère classique des interactions entre industriels, autorités de sûreté et régulateurs, rares sont les lieux où la sécurité est évoquée. En effet, comme indiqué dans l'avant-propos, les mégatendances d'évolution qui affectent l'industrie et le travail sont au cœur des préoccupations du monde industriel ; cette thématique, abordée par de nombreux think tanks, fait l'objet d'études dans des domaines variés, mais peu sous l'angle de la sécurité. L'avenir de l'industrie est largement débattu dans les très hautes sphères nationales et mondiales, mais la sécurité reste plus ou moins une dimension orpheline de la réflexion en cours à ces niveaux-là, pourtant structurants. Elle est encore trop souvent envisagée comme une contrainte, parfois comme une entrave aux autres dimensions de la performance d'entreprise. La sécurité industrielle continue généralement à être pensée en interne, même si les frontières de l'entreprise ont éclaté. Le défi consiste donc aussi à sortir des arènes axées sur la sécurité, à la traiter au même titre que les autres enjeux stratégiques et à porter les questions de sécurité dans les cercles influents et décisionnels qu'elle n'a jusqu'à présent pas vraiment réussi à pénétrer, à créer de nouveaux lieux où elles pourraient être discutées ou à renforcer les rares qui existent déjà (Pariès, 2022).

Piste #3 : Au niveau organisationnel, aligner prescrit, hiérarchie et autonomie

Point clé

- face à l'accélération, s'affranchir des frontières hiérarchiques, des approches chronologiques au sein de l'organisation pour penser la sécurité en intégrant « le coup d'après » ;
- afin de concilier innovation, réglementation et sécurité, créer des « bulles » d'innovation physiques et réglementaires transitoires ;
- sortir de la vision « sécurité = contrainte », l'appréhender aussi sous l'angle de l'opportunité ;
- au même titre que les questions économiques et politiques stratégiques, porter les questions de sécurité dans les hautes sphères décisionnelles.

Travaux cités

ANITI. (2022). *Certifiable AI.* Récupéré sur ANITI : https://aniti.univ-toulouse.fr/en/ia-certifiable/

Antonsen, S. (2022). Between Natural and Artificial Intelligence—Digital Sustainability in High-Risk Industries. Dans H. Laroche, C. Bieder, & J. Villena-López (Eds.), *Managing Future Challenges for Safety* (pp. 41-50). Cham : Springer. doi : https://doi.org/10.1007/978-3-031-07805-7_5

Balliester, T., & Elsheiki, A. (2018). *The Future of Work : A Literature Review.* International Labour Office. Récupéré sur https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwia-2KOCyY_pAhU9DmMBHVkdCnQQFjAAegQIAR

Baram, M., & Bieder, C. (2022). Standardization and Risk Regulation for High Hazard Industries. Dans H. Laroche, C. Bieder, & J. Villena-López (Eds.), *Managing Future Challenges for Safety* (pp. 85-93). Cham : Springer. doi : https://doi.org/10.1007/978-3-031-07805-7_11

Bieder, C. (à paraître). Bringing together humanity and technology in context. *Cahiers de la sécurité industrielle.*

Bieder, C., & Villena-Lopez, J. (2022). Times are changing and so is safety. Dans H. Laroche, C. Bieder, & J. Villena-López, *Managing Future Challenges for Safety* (pp. 1-12). Cham : Springer. doi : https://doi.org/10.1007/978-3-031-07805-7_1

Boucher, P. (2019). *How artificial intelligence works.* European Parliament. Récupéré sur https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/634420/EPRS_BRI(2019)634420_EN.pdf

Cook, R. I. (2020). How complex systems fail. *HindSight, 31*, pp. 13-16.

De Boisboissel, G. (2022). Evolution in the Way of Waging War for Combatants and Military Leaders. Dans C. B.-L. Hervé Laroche, *Managing Future Challenges for Safety* (pp. 13-24). Cham : Springer. Récupéré sur https://doi.org/10.1007/978-3-031-07805-7_2

Dekker, S. (2015). *Safety differently : Human factors for a new era* (Second ed.). CRC Press.

Deloitte. (2016). *The future of risk-new game, new rules.* Deloitte Development. Récupéré sur https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-the-future-of-risk-new-game-new-rules.pdf#:~ :text=The%20future%20of%20risk%7C%20New%20game%2C%20new%20rules,the%20past%2C%20few%20considered%20hedging%20against%20such%20risks.

EASA. (2020). *Artificial Intelligence Roadmap.* Récupéré sur https://www.easa.europa.eu/sites/default/files/dfu/EASA-AI-Roadmap-v1.0.pdf

Foncsi. (2021). *Sécurité ferroviaire du futur.* Récupéré sur Foncsi : https://www.foncsi.org/fr/blog/atelier-securite-ferroviaire-futur-synthese

Foncsi. (2023). *Participation citoyenne : perspectives 20 ans après la catastrophe de Toulouse. Cahiers de la sécurité industrielle.* Numéro 2023-03. Foncsi, Toulouse.

Frey, C. B., & Osborne, M. A. (2013). *The future of employment : how susceptible are jobs to computerisation?* Oxford Martin Programme on Technology and Employment, University of Oxford.

Gaxie, L., & Obadia, A. (2019). Une carte mentale des mutations du travail. Dans P. V. (Eds), *Le travail en mouvement.* Presses des Mines.

INRS. (2016). *Modes et méthodes de production en France en 2040 : quelles conséquences pour la santé et la sécurité au travail?* Récupéré sur https://www.inrs.fr/media.html?refINRS=VEP%203

Laroche, H., Bieder, C., & Villena-López, J. (2022). *Managing Future Challenges for Safety-Demographic Change, Digitalisation and Complexity in the 2030s.* Cham : Springer. doi : https://doi.org/10.1007/978-3-031-07805-7

Matyjasik, N., & Guenoun, M. (2019). *En finir avec le New Public Management.* Institut de la gestion publique et du développement économique.

NESTA. (2017). *The Future of Skills-Employment in 2030.* Oxford Martin School.

Pariès, J. (2022). Conjectures and Challenges of Safety Management- A Peek at the Future. Dans H. Laroche, C. Bieder, & J. Villena-López (Eds.), *Managing Future Challenges for Safety* (pp. 105-111). doi : https://doi.org/10.1007/978-3-031-07805-7_13

Perrow, C. (1999). *Normal Accidents – Living with High Risk Technologies* (Revised edition ed.). Princeton University Press.

PWC. (2020). *23rd Annual Global CEO Survey- Navigating the rising tide of uncertainty.* Récupéré sur www.ceosurvey.pwc

Shorrock, S. (2022). Adaptive Imagination at Work in Health Care. Dans H. Laroche, C. Bieder, & J. Villena-López (Eds.), *Managing Future Challenges for Safety* (pp. 95-104). Cham : Springer. doi : https://doi.org/10.1007/978-3-031-07805-7_12

Tosé, A., & Tazi, D. (2022). Dans H. Laroche, C. Bieder, & J. Villena-López (Eds.), *Managing Future Challenges for Safety* (pp. 51-57). Cham : Springer. doi : https://doi.org/10.1007/978-3-031-07805-7_6

Zahidi, S. (2020). *Davos 2020.* Récupéré sur World Economic Forum.

Reproduction de ce document

FONCSI
Fondation pour une culture de sécurité industrielle

Fondation pour une culture de sécurité industrielle
Fondation de recherche reconnue d'utilité publique

http://www.foncsi.org/

6 allée Émile Monso – CS 22760
31 077 Toulouse Cedex 4
France

Twitter : @LaFoncsi
Courriel : contact@foncsi.org

ISSN 2100-3874

FONCSI

Fondation pour une culture
de sécurité industrielle

6 allée Émile Monso
ZAC du Palays - CS 22760
31077 Toulouse cedex 4

www.foncsi.org