AIDES
A LA REFLEXION

La marguerite de l'IA en sécurité industrielle

Une cartographie détaillée des promesses et des risques du déploiement de l'intelligence artificielle

Travail commenté et nourri par le groupe d'experts industriels du « Vivre avec » de la Foncsi

René Amalberti

n° 2026-02

THÉMATIQUE

Transition numérique

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.

Fondation pour une Culture de Sécurité Industrielle
Fondation de recherche, reconnue d'utilité publique

www.FonCSI.org

6 allée Émile Monso – CS 22760
31077 Toulouse cedex 4
France

Courriel : contact@FonCSI.org

Abstract

Title	AI for Industrial Safety: A Comprehensive Mapping of the Opportunities and Risks of Deployment
Keywords	artificial intelligence, industrial safety, opportunities, risks
Authors	René Amalberti
Publication date	June 2026

Artificial Intelligence (AI) is rapidly making its way into all areas of corporate life, including the field of safety. Its development is generating high expectations, concerns, and questions regarding its deployment, governance, and organizational impact.

This document presents an overview of the opportunities and concerns associated with AI deployment through a graphical representation of six application domains, depicted as the petals of a flower: risk anticipation; distancing operators from the most hazardous situations; protection of exposed operators; enhanced human knowledge and decision-making; automation of the monitoring and maintenance of technical systems; and, finally, the enrichment of experience feedback. As part of the FonCSI initiative *Safety of the Future: "Living with" Uncertainty, Complexity, and New Expectations*, this document draws on the literature as well as the work of a foresight workshop that has brought together, since 2025, around twenty experts from industry and regulatory authorities, along with external contributors.

About the authors

This document was written by René Amalberti, director of the FonCSI and author of numerous books and articles on safety management in industry and healthcare. He is also a member of the French Academy of Technologies.

To cite this document

Amalberti, R. (2026), *AI for Industrial Safety: A Comprehensive Mapping of the Opportunities and Risks of Deployment*. Number 2026-02 of the *Cahiers de la Sécurité Industrielle*, Foundation for an Industrial Safety Culture, Toulouse, France (ISSN 2100-3874). DOI: 10.57071/iam478. Available from FonCSI.org/en.

Résumé

Titre	La marguerite de l'IA en sécurité industrielle : Une cartographie détaillée des promesses et des risques du déploiement de l'intelligence artificielle
Mots-clefs	sécurité industrielle, IA, prospective, risques, promesses
Auteurs	René Amalberti
Date de publication	juin 2026

L'intelligence artificielle (IA) arrive à grand pas dans tous les secteurs de la vie de l'entreprise, y compris dans le champ de la sécurité. Cette arrivée suscite à la fois de fortes attentes, des craintes ainsi que des interrogations quant à son déploiement, son encadrement et son impact organisationnel.

Ce Cahier présente un cadre général de promesses et de craintes liées au déploiement de l'IA, à travers une représentation en « marguerite » composée de six domaines applicatifs, schématisés sous la forme de pétales : le risque anticipé ; l'éloignement de l'opérateur des situations les plus dangereuses ; la protection de l'opérateur exposé ; l'homme éclairé en matière de connaissance et de décision ; l'automatisation du suivi et de la maintenance des systèmes techniques ; et enfin, l'enrichissement du retour d'expérience. Inscrit dans l'initiative de la Foncsi « Sécurité du futur : "vivre avec" l'incertitude, la complexité et les nouvelles attentes », ce document s'appuie sur la littérature et les travaux d'un atelier prospectif réunissant, depuis 2025, une vingtaine d'experts issus d'entreprises et d'autorités de tutelle, ainsi que des contributeurs extérieurs.

À propos des auteurs

Ce document a été rédigé par René Amalberti, directeur de la Foncsi et auteur de nombreux ouvrages et articles sur la gestion de la sécurité dans l'industrie et le monde de la santé. Il est également membre de l'Académie des technologies.

Pour citer ce document

Amalberti, R. (2026), *La marguerite de l'IA en sécurité industrielle*. Numéro 2026-02 des *Cahiers de la Sécurité Industrielle*, Fondation pour une Culture de Sécurité Industrielle, Toulouse, France (ISSN 2100-3874). DOI : 10.57071/iam478. Disponible à l'adresse FonCSI.org/fr.

Table des matières

Introduction

Contexte

L'intelligence artificielle (IA) arrive à grands pas dans tous les secteurs de la vie de l'entreprise, y compris dans le champ de la sécurité. Cette arrivée suscite à la fois de fortes attentes, des craintes ainsi que des interrogations quant à son déploiement, son encadrement et son impact organisationnel.

Ce Cahier présente un cadre général de promesses et de craintes liées au déploiement de l'IA, à travers une représentation en « marguerite » composée de **six domaines applicatifs**, schématisés sous la forme de pétales.

On comprend que cette marguerite des grands domaines applicatifs de l'IA en sécurité industrielle sera plus pérenne à échelle macro que le détail produit par sa lecture pétale par pétale portant sur de multiples applications à venir. Le lecteur du document doit garder en vue que ces applications sont par essence datées à la mi 2026, toutes **destinées à évoluer rapidement** comme tout développement en matière d'IA.

Le groupe d'experts industriels « Vivre avec » de la Foncsi

Ce Cahier s'inscrit dans l'initiative de la Foncsi « Sécurité du futur : "vivre avec" l'incertitude, la complexité et les nouvelles attentes ». Il s'agit d'un travail de réflexion global et systémique sur l'impact des grands changements (changement climatique, digitalisation, mutations économiques et géopolitiques) de notre société sur la sécurité.

Le concept de « Vivre avec » renvoie à un changement de posture : il ne s'agit plus seulement d'anticiper et de maîtriser des risques identifiés, mais de composer durablement avec des environnements instables, incertains et en constante évolution. Cette perspective invite à interroger les cadres établis de la sécurité, depuis les pratiques opérationnelles jusqu'aux logiques de pilotage et de régulation, en intégrant de nouvelles attentes sociales et organisationnelles.

Ce Cahier poursuit les réflexions engagées dans un premier Cahier de la Foncsi, *La sécurité à l'ère du « vivre avec » : Incertitude, complexité et nouvelles attentes* **[Bieder et al. 2024]** qui constitue le socle conceptuel de cette démarche. Il mobilise à la fois une revue de la littérature et les apports d'un dispositif de réflexion collective structuré autour d'ateliers prospectifs.

Mis en place en 2025, le groupe d'experts industriels « Vivre avec » de la Foncsi réunit une vingtaine d'experts des entreprises et des représentants des autorités de tutelle de la sécurité industrielle, tous mécènes de la Fondation, qui se réunissent deux fois par an pour échanger et approfondir la réflexion sur les changements à venir de la sécurité industrielle. Le groupe comprend aussi quelques experts invités externes aux mécènes de la Fondation, anciens directeurs industriels, directeur actuel de l'IMdR, experts de l'Anssi, et représentants syndicaux. Sa composition volontairement stable permet d'inscrire les échanges dans une temporalité longue, propice à une réflexion approfondie.

Le présent Cahier s'appuie plus spécifiquement sur les travaux et les échanges du second atelier prospectif de ce groupe, tenu le 2 avril 2026 à Paris sur le sujet : *Les usages de l'IA dans les entreprises : quels enjeux de sécurité, positifs et négatifs associés ?* Cette rencontre a été organisée et animée par l'équipe de la Foncsi : René Amalberti, Corinne Bieder, Fiona Fadat, Clotilde Gagey, Caroline Kamaté, Hervé Laroche, Éric Marsden, Thomas Merlet et Jean Pariès. Elle a rassemblé des représentants d'organisations variées ainsi que des organisations syndicales (CGT, CFE-CGC). Elle prolonge les échanges initiés lors d'un premier atelier, tenu le 25 mars 2025 à Toulouse, consacré aux impacts des grandes transformations sur la sécurité industrielle.

Les participants à l'atelier prospectif du 2 avril 2026 :

COSTE	Didier	Airbus
REUZEAU	Florence	Airbus
ROUGÉ	Sophie	Airbus
DEHARVENGT	Stéphane	Anssi
LARGIER	Alexandre	ASNR
MATHIEU	Pascal	CFE-CGC
MONFORT	Bertrand	CGT / CEA Saclay
NICOLAS	Guilhem	DGAC-DSAC
LABARTHE	Jean-Paul	EDF
LAUGIER	Cécile	EDF
MAGNE	Laurent	EDF
BAUMANN	Pierre	Engie
DEYDIER	Marie-Véronique	Engie
PARIS	Nicolas	EPSF
BOUCAULT	Julien	EPSF
BOISSIÈRES	Ivan	Icsi
LACOSTE	André-Claude	Icsi-Foncsi
ROUSSEAU	Luc	Icsi-Foncsi
GAY	Didier	Ineris
DECAUX	Anne-Sophie	Natran
PÉRINET	Romuald	Natran
CATARINO	David	OPPBTP
MUSCHE	Emmanuel	OPPBTP
HABERSTICH	Philippe	RTE
FRANÇOIS	Yohanna	SNCF
MACHADO-VERHEYE	Soizic	Suez
EURYALE	Anne-Laure	Systra
KLEIN	Michel	TotalEnergies
PAPILLAULT	Virginie	UIC
REPUSSARD	Jacques	IMDR
AUVRÈLE	Patrick	Ex-SNCF
DESCAZEAUX	Michel	Ex-Engie

En parallèle, la Foncsi s'appuie à l'international sur des experts académiques proches de la Fondation — essentiellement norvégiens, étatsuniens, australiens et argentins — grâce à des contacts répétés et des séminaires tenus sur ce même thème du « Vivre avec ». Les résultats sont publiés régulièrement sous forme de livres chez Springer dans la collection en anglais de la Foncsi « SpringerBriefs in Safety Management » et sous forme de « Cahiers de la sécurité industrielle » (en anglais et français), tous ces documents étant accessibles en *open access*.

Objectifs du document

Ce document vise à proposer une **cartographie des promesses** et des craintes liées au déploiement de l'IA en sécurité industrielle, et d'en dégager les impacts, tant positifs que négatifs, imaginés, voire déjà observés dans le secteur de l'industrie.

Structure du document

Le chapitre 1 présente le cadre général proposé pour appréhender les promesses de l'IA en matière de sécurité industrielle, structuré autour d'une « marguerite » composée de six pétales, représentants les six grands domaines applicatifs. Cette représentation vise à donner une **vision d'ensemble**, à la fois synthétique et structurante, des principaux champs dans lesquels l'IA est susceptible de transformer les pratiques de sécurité.

Le chapitre 2 propose une lecture détaillée de cette marguerite, en examinant, pour chacun des domaines, des applications déjà existantes ou en devenir proche. Cette analyse décrit les **opportunités** avec les réticences associées à leurs applications.

Enfin, le chapitre 3 présente les **macro-résultats de l'atelier prospectif**. Il y compare les bénéfices et les inconvénients de chaque pétale, à la fois au sein de chaque domaine et entre les différents domaines. Il vise ainsi à éclairer les choix stratégiques des acteurs industriels, en apportant des éléments d'aide à la **priorisation des usages de l'IA** en matière de sécurité. Également, des scénarios de l'impact de son déploiement sur la sécurité y sont présentés, en se basant sur deux courbes d'évolution de technologies connues.

1

Le cadre général apporté par la Foncsi : la marguerite de l'IA

Le cadrage original proposé (« la marguerite à six pétales ») est le produit d'une réflexion de la Foncsi appuyée sur la littérature.

Les détails du déploiement de chaque pétale de la marguerite proviennent également de la Foncsi. Les illustrations d'exemples proviennent quant à eux de deux sources :

- Le produit du second atelier prospectif du groupe d'experts industriels « Vivre avec » de la Foncsi, le 2 avril 2026 (une vidéo de l'évènement est disponible sur `www.foncsi.org`).
- La littérature publiée sur ces domaines pour compléter les exemples et les enrichir des principales publications clés.

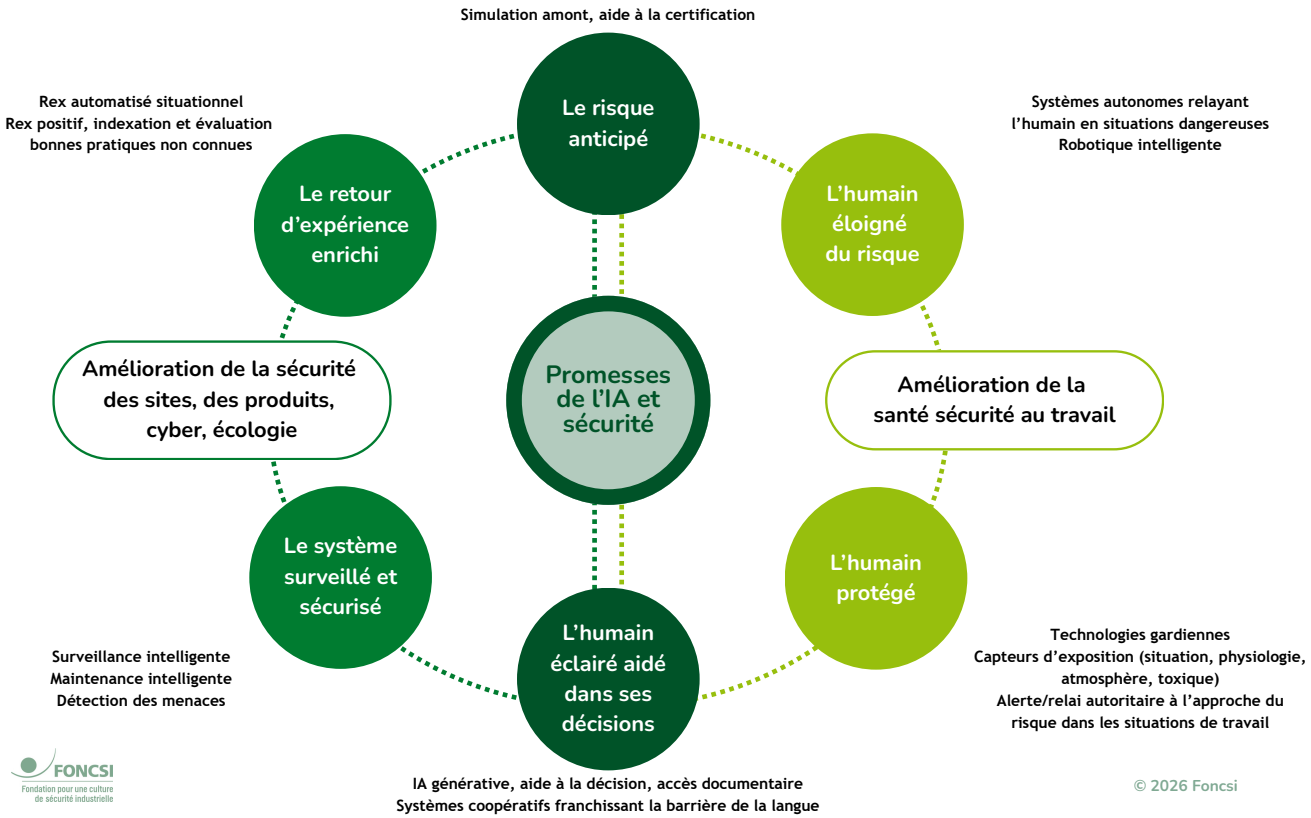

Fig. 1.1 La marguerite du déploiement de l'IA en sécurité industrielle.

L'analyse de la littérature préliminaire au travail en groupe suggère que le déploiement de l'IA en sécurité industrielle peut être représenté par **une marguerite à six pétales** (*cf.* la figure 1.1) couvrant les champs :

- du **risque anticipé** grâce à la conception sûre ;
- des technologies permettant de tenir **l'opérateur éloigné du risque** dans les situations les plus dangereuses ;
- des technologies permettant de **surveiller et protéger l'opérateur** quand il reste directement exposé ;
- des technologies augmentées de **l'homme éclairé dans sa connaissance et ses décisions** ;
- des technologies appliquées au **système technique surveillé et maintenu automatiquement** ;
- et, des technologies permettant une **amélioration du retour d'expérience**, pour l'enrichir et/ou mieux l'exploiter.

Si certains usages de l'IA pour la sécurité sont présents dans la littérature, leur déploiement effectif n'est pas généralisé dans toutes les industries et toutes les organisations à ce jour. Par ailleurs, nombre de ces usages en sont encore à **un stade exploratoire**. La « marguerite » décrit donc un champ des possibles envisagés aujourd'hui.

2

Zoom sur chaque pétale de la marguerite

Ce chapitre résume les grandes directions de déploiement de l'IA et ses impacts pour la sécurité industrielle, pétale par pétale.

2.1 Le pétale du « risque anticipé » : l'IA en conception sûre

Ce domaine se décline en différentes visées applicatives.

Analyse préliminaire des risques et exploration des scénarios

L'IA peut être utilisée pour explorer des espaces de scénarios de risques plus vastes que ce que permet une analyse humaine seule. L'IA apporte une exhaustivité accrue des combinaisons de défaillances, une détection de scénarios « non intuitifs » et une meilleure anticipation des effets émergents. Quelques applications industrielles :

- Industrie de procédés/énergie : usage de modèles d'IA couplés à des jumeaux numériques pour **identifier des combinaisons dangereuses** de paramètres (température, pression, vieillissement, erreurs humaines) avant même la conception détaillée.
- Aéronautique et défense : conception en amont de fonctions d'aide à la décision ou d'autonomie partielle, avec **exploration systématique de conditions « extrêmes mais plausibles »**, au-delà des scénarios nominalement envisagés par les ingénieurs.

Vérification de conception et détection d'incohérences

L'IA est utilisée dans ce cas comme outil de relecture intelligente des modèles de conception, des exigences de sécurité et des architectures système, réservée aux phases d'ingénierie amont et de vérification interne. L'IA est déjà utilisée comme outil d'aide à la décision mais **jamais comme décideur final**. Quelques applications industrielles :

- Aéronautique (Europe, États-Unis) : **analyse automatique de cohérence** entre exigences de sécurité, fonctions et allocations systèmes (complément aux méthodes ARP4754A / ED-79), ICAO.
- Systèmes ferroviaires et industriels complexes : **outils de détection d'incohérences logiques** dans les modèles d'architecture ou de sûreté de fonctionnement.

Inspection, validation et retour d'expérience (REX)

L'IA est dans ce cas massivement utilisée sur demande. Dans la quasi-totalité des cas, l'IA n'est pas la barrière de sécurité, mais un système de surveillance ou d'alerte supplémentaire. Quelques applications industrielles :

- Industrie lourde, énergie, infrastructures : inspection visuelle automatisée (fissures, corrosion, boulonnerie critique) par vision artificielle, souvent via drones ou robots.
- Usines automatisées : détection en temps réel de situations dangereuses (intrusion humaine, EPI manquant, comportements à risque), sans être intégrée directement à la fonction de sécurité certifiée.

IA et certification

C'est un domaine plus délicat, où l'on doit distinguer des usages déjà acquis pour aider à la certification, et le point noir de la certification de systèmes intégrant de l'IA.

L'IA comme outil d'aide à la certification est déjà utilisée par les industriels, parfois les autorités, pour analyser des dossiers, essais, REX et historiques d'incidents. Cependant, la certification de systèmes intégrant de l'IA à base d'apprentissage entre en tension directe avec les principes historiques de certification. **On certifie des processus, des garde-fous et des architectures, beaucoup plus que « l'algorithme en lui-même ».** On peut noter toutefois quelques initiatives en cours :

- ISO/IEC TR 5469 (2024) : première tentative de cadrage entre IA et sécurité fonctionnelle ;
- UL 4600, ISO 21448 (SOTIF) pour qualifier des systèmes autonomes (véhicules robots) ;
- Travaux EUROCAE WG-114 / SAE G-34, appliqués à la certification en aéronautique.

2.2 Le pétale de « l'homme éloigné du risque »

Ce pétale comprend de nombreuses applications de robotiques autonomes dont le principal bénéfice de sécurité est la suppression de scénarios mortels par exposition aiguë (logique d'élimination de l'exposition humaine au danger). Les effets sont très bien documentés par le BIT **[ILO 2025]** et le US *National Safety Council* **[NSC 2023]**.

- **Dans le nucléaire** (déconstruction, inspection, gestion post-accident) : irradiations aiguës, contaminations internes, atmosphères confinées inconnues.
  - Robots téléopérés semi-autonomes pour inspection, découpe et manipulation de déchets hautement radioactifs (Sellafield, Fukushima, Tchernobyl) **[Lopez et al. 2025]**.
  - Drones et robots quadrupèdes pour cartographie radiologique (Boston Dynamics/Spot).
  - Couplage de l'IA et de jumeaux numériques pour une planification sûre des opérations.
- **Dans les industries lourdes, chimie et oil & gas** (zones ATEX, toxiques) : risques d'**explosions, d'intoxications, d'incendies et travaux à chaud**.
  - Robots mobiles et bras téléopérés pour l'inspection, l'échantillonnage et la manipulation de substances dangereuses.
  - Drones IA pour la détection de fuites (gaz, vapeurs toxiques).
  - IA de surveillance continue des paramètres critiques (pression, température, gaz).
- **Dans les mines, carrières et tunnels** : risques d'effondrements, d'explosions et d'asphyxies (atmosphères pauvres en oxygène).
  - Robots autonomes pour une reconnaissance post-tir et une inspection de galeries.
  - Téléopération pour la manipulation d'explosifs ou du déblaiement.
  - Éloignement des opérateurs des phases les plus létales (post-blast, reconnaissance initiale).
- **Dans la construction et manutention lourde** (AGV, AMR, robots de chantier) : risques **d'écrasement, de collision ou de chute**.
  - Robots mobiles autonomes pour le transport de charges.
  - Robots d'inspection en hauteur ou en zones instables.

Les **effets empiriques mesurés** sont qu'une hausse modérée de la densité robotique est associée à une baisse d'environ 1,2 blessure pour cent travailleurs/an **[Gihleb et al. 2022]**.

L'effet positif porte principalement sur les blessures graves, avec un impact indirect sur la mortalité.

2.3 Le pétale de « l'homme protégé » des risques de proximité

Ce pétale sur les valeurs gardiennes de la sécurité et sur la réduction de la gravité des accidents du travail est cité déjà depuis plusieurs années comme un des gains les plus immédiats et urgents du déploiement de l'IA dans l'entreprise (voir **[Malenfer et al. 2022]**). On y retrouve l'alerte précoce (avant la perception humaine), la protection des travailleurs isolés, la réduction du temps de réaction, l'aide à la prévention plutôt qu'à la sanction, la surveillance continue sans fatigue et la détection des presque-accidents.

- **Casques ou gilets « intelligents » qui perçoivent le danger avant l'humain** : l'opérateur porte un casque ou un gilet équipé de capteurs (gaz, chaleur, bruit, mouvements et/ou localisation) dont les signaux sont analysés en continu par l'IA. Par exemple, si le gilet détecte une légère hausse anormale de gaz toxique avant que l'odeur ne soit perceptible, le système vibre, émet une alerte sonore et envoie une alerte au poste de sécurité. Une revue de littérature est disponible sur les applications dans le secteur du bâtiment et les sites dangereux **[Sakshi et al. 2024]**.
- **Capteurs de proximité entre humains et machines mobiles** : le port de balises par les opérateurs et les machines (chariots, robots) permet à l'IA de calculer des trajectoires et vitesses relatives.
- **Caméras intelligentes qui, avec l'aide de l'IA, reconnaissent des situations dangereuses** : un opérateur entre dans une zone à risque sans casque, la caméra le détecte et émet une alerte immédiate. Si un piéton s'approche trop près d'un chariot élévateur, la caméra le détecte et alerte le conducteur et le piéton, ou encore lorsqu'un geste dangereux répété est détecté (posture ou fatigue).
- **Détection de fatigue, de chute ou de malaise** : un dispositif combinant des capteurs de mouvement, de posture et de paramètres physiologiques, associés à de l'IA, permet de détecter une chute ou une immobilité anormale. Il identifie également des signes de fatigue thermique ou de surmenage et déclenche automatiquement un appel aux secours si l'opérateur ne réagit pas.
- **Anticipation des accidents grâce aux capteurs associés à l'IA** : l'IA apprend à partir de milliers de signaux faibles (vibrations, gestes et/ou incidents mineurs) pour donner des alertes de risques imminents[1].

2.4 Le pétale de « l'homme éclairé et aidé dans ses décisions »

L'utilisation de l'IA générative dans le domaine de la sécurité industrielle constitue aujourd'hui l'un des usages les plus répandus de l'intelligence artificielle en matière de sécurité. L'offre grandit rapidement, et ses applications sont souvent aisées à s'approprier (en tout cas pour un usage superficiel) pour les opérateurs déjà familiers avec l'IA générative dans la vie courante[2]. On note toutefois une littérature croissante sur des inquiétudes associées à ce déploiement rapide, tous azimuts, peu accompagné et peu testé **[Huber et al. 2025]**.

- **Éclairage situationnel et compréhension du contexte** (sensemaking) : l'IA générative transforme des flux complexes (capteurs, alarmes, historiques) en récits explicatifs simples et compréhensibles par l'opérateur. Des applications existent déjà dans plusieurs secteurs :
  - Dans les secteurs du nucléaire et de l'énergie pour fournir des explications en langage naturel d'une situation « hors nominal » (enchaînement d'alarmes, dérive progressive, comparaison avec des incidents passés).
  - Dans les procédés chimiques, il y a des mises en récit d'une évolution lente de paramètres (température, pression) que les seuils classiques ne détectent pas encore.
  - Dans les transports, aéronautiques et ferroviaires, des systèmes sont introduits pour produire une synthèse intelligible de plusieurs signaux faibles avant incident.
- **Accès intelligent, ciblé et simplifié à la documentation technique**. L'objectif est à la fois un gain de temps, moins d'erreurs de procédure et de contournements informels. **L'IA devient un intermédiaire cognitif** entre l'opérateur et des corpus vastes

[1] Compliance quest, *How AI is Transforming Safety Incident Prediction*, August 28th, 2025.

[2] Lire par exemple le International AI safety report, 2026.

(procédures, manuels, REX). Les exemples sont nombreux en maintenance industrielle où l'IA permet d'accéder rapidement aux procédures pertinentes en contexte. D'autres applications concernent les industries à forte conformité réglementaire (nucléaire, *oil & gas*, santé), en procurant un **accès instantané** aux parties pertinentes des exigences normatives, ou encore, sur des installations anciennes, en proposant une réconciliation entre documentation historique, modifications successives et situation réelle.

- **Aide à la décision en situation normale ou dégradée**. L'IA ne décide pas, mais propose des hypothèses, des options ou des compromis, en explicitant leurs conséquences. En **gestion de crise industrielle**, elle permet une **comparaison de scénarios** (stabiliser ou arrêter, continuer ou isoler).
- **Aide à la communication en environnements multilingues et multi-profils**. L'objectif est l'aide à la coopération, à la réduction des malentendus et à l'alignement rapide des acteurs. Pour cela, l'IA peut jouer un rôle de **traducteur technique et culturel**, pas seulement linguistique, qui peut devenir précieux sur les chantiers internationaux (traduction instantanée contextualisée des termes métier et sécurité), avec des équipes hétérogènes (opérateurs, ingénieurs, sous-traitants), en reformulant aussi les messages critiques selon le profil du destinataire. Certaines applications concernent les cellules de crise en proposant des synthèses de sources et de langues multiples.

2.5 Le pétale du « système surveillé et sécurisé »

Maintenance prédictive : L'IA apprend le « comportement normal » et détecte les dérives faibles, non accessibles à la perception humaine **[Azeta et al. 2026]**.

- Déjà de nombreuses applications dans les raffineries, centrales électriques et usines chimiques **appliquées aux machines tournantes** (pompes, turbines, compresseurs) : des capteurs mesurent en continu les vibrations, la température, la pression et l'acoustique avec pour usage concret, par exemple, de détecter un roulement qui s'use lentement, anticiper une rupture d'arbre ou un grippage, et planifier l'arrêt avant une panne brutale.
- D'autres applications concernent les équipements critiques intermittents (vannes de sécurité, soupapes) où **l'IA corrèle les données rares** (ouverture/fermeture, micro-fuites) avec l'historique pour repérer une vanne qui fonctionne mal sans jamais être testée en conditions réelles avec pour objectif de réduire les essais intrusifs.

Surveillance en temps réel pour « voir ce que l'opérateur ne peut pas voir » afin de réduire les alarmes unitaires, et d'augmenter les alertes « système » intelligentes. La détection d'anomalies de procédé avec l'IA repose sur la surveillance simultanée de centaines de paramètres (températures, débits, pressions, compositions) pour identifier des combinaisons anormales (et non une valeur isolée) et alerter avant un emballement thermique ou une dérive chimique. Autre exemple : l'IA exploite des micro-variations de pression, des signaux acoustiques, l'imagerie thermique pour détecter une fuite d'hydrogène ou d'ammoniac avant odorisation ou capteurs seuil **[Zaidi et al. 2026]**.

L'IA au service de la cybersécurité des systèmes industriels. L'IA apprend le trafic réseau industriel « normal » et détecte des commandes inhabituelles, des séquences incohérentes et toute activité suspecte sur automates **[Aslam et al. 2025]**. Mais le bénéfice attendu pourrait aussi avoir une contrepartie, en « ouvrant » les systèmes industriels à base d'IA à de nouvelles vulnérabilités d'attaques cyber. Le cabinet Gartner rappelle que d'ici 2028 les applications d'IA sur mesure pourraient représenter **50% des efforts** de réponse aux incidents de cybersécurité en entreprise, contre moins de 5% en 2024. Selon les prévisions de Gartner, ces systèmes, souvent déployés sans tests de sécurité suffisants, seront bien plus difficiles à sécuriser dans la durée[3].

Vision par ordinateur pour les zones dangereuses. Cela rejoint le pétale de « l'homme protégé des risques » de proximité avec en objectif direct, une réduction des accidents graves et mortels avec des caméras intelligentes qui détectent automatiquement la présence humaine en zone interdite, le non-port d'EPI ou les fuites visibles (panache, flamme, écoulement). Ces dispositifs sont déjà très présents dans les secteurs de l'*oil & gas*, de la chimie lourde, et sur les

[3] ICTjournal, 2026, Gartner alerte sur les défis de sécurité liés aux applications IA sur mesure.

sites Seveso pour la surveillance de torchères, bacs de stockage et zones ATEX [Vukicevic et al. 2024].

2.6 Le pétale du « retour d'expérience enrichi »

La littérature scientifique converge sur un point clé : **l'IA n'améliore pas le REX parce qu'elle « l'automatise »**, mais parce qu'elle rend possible un apprentissage transversal, rapide et systémique à partir de volumes d'événements inaccessibles à l'analyse humaine classique.

L'IA pour améliorer la remontée d'informations critiques (au-delà du reporting formel). Dans de nombreuses industries (manufacture, énergie, construction), les déclarations d'incidents ou de presque-accidents sont très courtes, subjectives et hétérogènes. Il s'agit de textes libres. Des plateformes intégrant l'IA analysent ces récits libres, les commentaires, et parfois même des échanges informels (tickets, mails ou messages internes), pour détecter des motifs récurrents (fatigue, contournement de règles ou mauvaise coordination), ou des signaux faibles que personne n'avait catégorisés explicitement. L'IA joue ici le rôle d'un lecteur infatigable de milliers de petits récits, capable de dire : *« attention, on voit apparaître de plus en plus souvent cette combinaison de conditions »* [Hashmi et al. 2024].

L'IA et la production du REX : du stockage à l'apprentissage réel. Ceci correspond au passage de l'enquête d'incident à l'analyse systémique d'événements :

- ▷ Les systèmes traditionnels enregistrent les événements, ils n'apprennent pas.
- ▷ Les systèmes assistés par IA cherchent au contraire des *patterns* : regroupement automatique d'événements similaires, reconstruction de chaînes typiques de dégradation et identification de *précurseurs* récurrents.

L'IA pour anticiper des scénarios critiques (avant l'accident). À partir du REX, l'IA simule des « futurs plausibles » dans lesquels elle peut estimer où, quand, dans quelles conditions un scénario dégradé est le plus probable. Certaines plateformes parlent déjà de ***predictive safety***, ***leading indicators*** issus des données historiques pour produire une statistique des futurs possibles, construite à partir des erreurs passées… y compris celles qui n'ont « rien cassé » (voir la revue de littérature multisecteurs sur ces possibilités, [Park et Kang 2024]).

L'IA et le REX positif : apprendre à partir de ce qui a bien marché. C'est un exemple encore émergent, mais conceptuellement très fort. Il s'agit d'identifier les adaptations réussies des opérateurs. L'IA peut analyser des récits d'événements où un problème sérieux est survenu mais a été rattrapé intelligemment par les équipes. En comparant des situations proches, certaines qui ont mal tourné, d'autres bien récupérées, elle peut mettre en évidence des stratégies d'adaptation efficaces, des formes tacites d'expertise, des compromis opérateur-système qui fonctionnent. Même si ce point reste peu industrialisé, il est explicitement discuté dans les approches récentes de **learning systems** et dans la critique des REX centrés uniquement sur l'échec (voir publications de la Foncsi citées plus haut).

3

Les macro-résultats de l'atelier

Ce chapitre présente les résultats de l'atelier prospectif organisé par la Foncsi à la mi-2026. Il s'appuie sur les contributions des participants, qui proviennent d'horizons et d'organisations variés. Les participants étaient invités à échanger très librement sur les opportunités et difficultés rencontrées, ainsi que, sous forme de prospective, sur des scénarios de l'impact du déploiement de l'IA sur la sécurité.

3.1 Un déploiement effectif de l'IA pour la sécurité industrielle en pleine extension

À la mi-2026, l'usage de l'IA pour des applications de sécurité industrielle dans les entreprises présentes à l'atelier prospectif est déjà évident pour au moins trois pétales. Notamment, et de la manière la plus distribuée parmi les entreprises présentes, pour les applications de l'IA générative sur la documentation de sécurité (conception, usage en ligne, simplification documentaire). Également, pour la robotique autonome dans des applications d'environnements à hauts risques. Enfin, avec une adoption croissante, pour des systèmes de surveillance par vision intelligente de situations de travail à risque, vulnérables à des attaques, ou de maintenance.

Les gains espérés pour la sécurité sont immenses. L'IA et la robotique sont extrêmement efficaces pour éliminer l'exposition létale :

- en aidant à une conception plus sûre par sa capacité à fouiller en profondeur les données disponibles, à proposer des scénarios de situations futures à risque, et à vérifier les codes de conception ;
- en décuplant le retour d'expérience actuel, sous une forme quasi automatique ;
- en améliorant fortement la détection précoce des défaillances et menaces dans les installations à risque, notamment détecter des signaux atypiques ;
- en prévenant, par tous moyens d'alerte, les opérateurs dans les situations de travail de dangers de proximité, et réduire ainsi les accidents graves et mortels. Cela est encore plus évident quand l'IA permet de remplacer les opérateurs dans des situations dangereuses par de la robotique autonome ;
- enfin, l'IA générative possède un formidable potentiel d'outil coopératif intelligent sur l'aide en ligne au diagnostic et à l'accès à la documentation.

Toutefois, **la majorité des usages restent en devenir pour les participants** : ils sont davantage imaginés qu'observés sur le terrain. Souvent avec l'aveu de ne pas être au courant et de découvrir *a posteriori* la réelle pénétration des applications IA dans les services, sans analyse de risque associée, tant la diffusion est large, voire systémique à l'échelle de l'entreprise. Enfin, il en est de même avec des effets souvent redoutés, mais encore sans preuves, avec une expression toujours au conditionnel et incantatoire.

Un **usage grand public qui pénètre en même temps l'entreprise** : plusieurs des entreprises présentes lors de cet atelier prospectif n'ont parfois pas encore de connaissance d'application pour la sécurité sur le terrain « officiellement » validées. Toutefois, toutes admettent **un usage déjà quasi « sauvage »**, difficile à encadrer, de l'IA générative par les opérateurs et les services, avec des formes d'assistance plus ou moins officielles : dans les bureaux, sur le terrain, avec parfois son propre téléphone ou tablette, et même dans les services de conception

où l'utilisation et le traçage de l'IA comme aide au codage est encore peu encadré. On conçoit que le lien entre ces usages généraux déjà présents dans l'entreprise, sans trop d'encadrement, et la sécurité industrielle soit plus indirect mais potentiellement réel, et nécessite une certaine prudence.

3.2 Des craintes de nature générique autour de la table, avec quelques éclairages originaux apportés en plus de l'atelier

3.2.1 Les grandes craintes traversant la communauté industrielle

L'atelier prospectif a repris à son compte le contenu d'une littérature abondante à charge, encore presque uniquement exprimée au conditionnel. Cette littérature a déjà été largement résumée dans des publications récentes de la Foncsi **[Marsden et Steyer 2025 ; Le Coze et Antonsen 2023 ; Bieder et al. 2026]**.

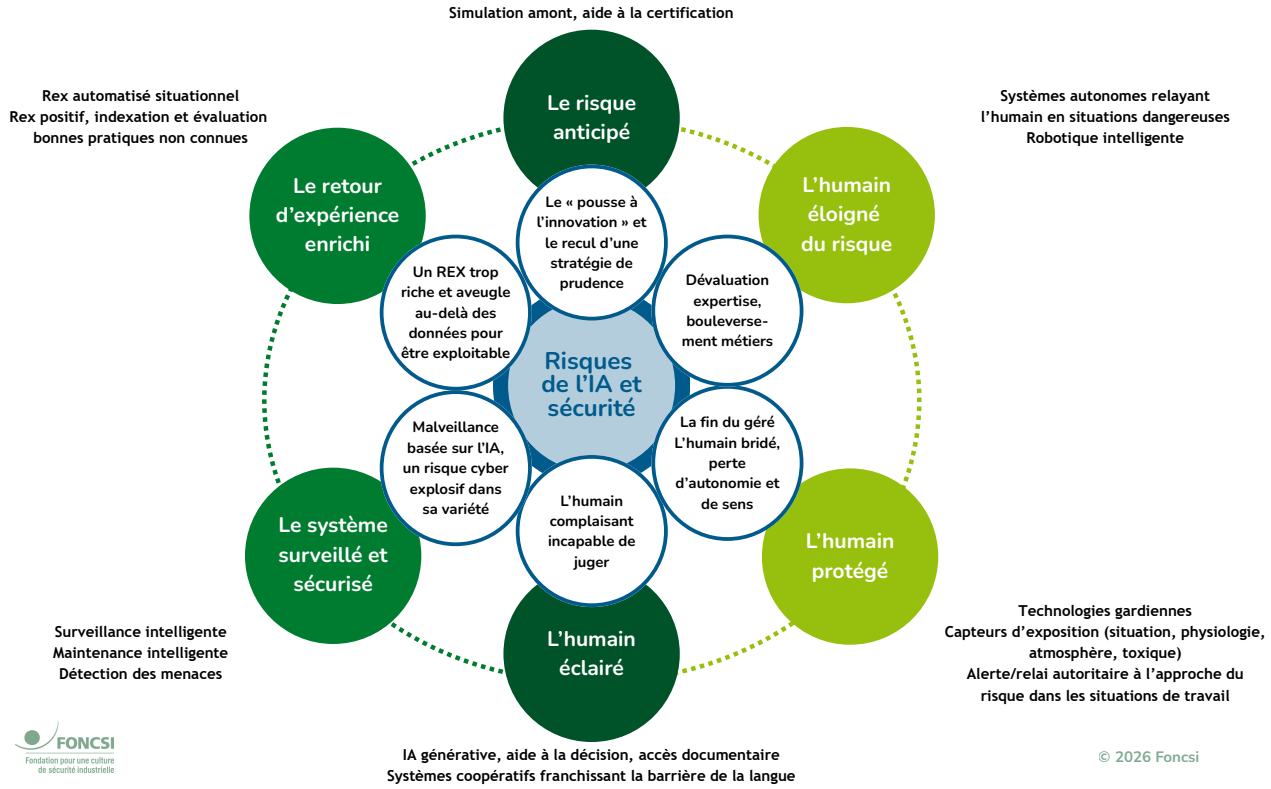

Fig. 3.1 Les principales craintes en matière de la sécurité industrielle suscitées par l'introduction de l'IA dans les entreprises à risques.

On retient de ces acquis quatre grandes craintes génériques, représentés dans la figure 3.1 :

1. Une **difficulté à comprendre le raisonnement de la machine et à coopérer** : la nouvelle capacité d'apprentissage des systèmes à base d'IA, avec un considérable effet « boîte noire », n'a pas d'équivalent dans le passé technologique. Cela ouvre une ère de très grande complexité et de nouveaux risques dans la compréhension mutuelle et la coopération entre humains et systèmes autonomes. C'est le domaine le mieux décrit dans la littérature (voir documents Foncsi opus cités).
2. Une **perte de compétences**, avec une érosion redoutée des compétences critiques (***skill fade***) couplé à un effet « distance au réel » et une surconfiance avec une disparition progressive du savoir tacite des opérateurs experts.
3. Une **difficulté à reprendre la main**, nourrie par le point précédent, avec une moindre capacité à diagnostiquer une situation dégradée quand l'automatisation échoue et un risque d'acceptation aveugle d'une solution « statistiquement performante ».
4. Un **risque de nouvelles failles cyber** susceptibles d'exploiter des biais et des angles morts techniques. L'IA apprend sur des situations passées et peut ne pas détecter des

scénarios nouveaux, qu'ils soient injectés intentionnellement ou non, dans les failles critiques. Ce risque rejoint le domaine de « nouveaux modes de défaillance » avec des attaques ou manipulations de données, ainsi que plus globalement une dépendance à des infrastructures numériques fragiles.

À ces quatre grandes craintes génériques s'ajoute une déclinaison d'autres **craintes, plus systémiques et organisationnelles**, liées à la bascule du modèle social/sociétal induite par la pénétration de ces technologies :

- **Une ampleur redoutée de pertes d'emplois et de reconversions**. Dans le prolongement du modèle de la destruction créatrice et du rebond d'emplois de Joseph Schumpeter (début du XX^{e} siècle [Schumpeter 1935, 1951]), on pourrait s'attendre à ce que l'introduction de l'IA supprime des postes, mais génère ensuite une création de nouveaux postes en nombre équivalent ou supérieur. Toutefois, pour la première fois, ce modèle de rebond est remis en question avec l'arrivée de l'IA. Le sujet devient majeur pour les ressources humaines (RH) de l'entreprise [Aghion et al. 2025 ; Kogelmann 2025 ; Rizvi 2026], car beaucoup d'auteurs pensent que les créations d'emplois liées à l'IA **ne compensent pas la destruction des trajectoires professionnelles** : les gains se concentrent sur le capital, pas sur le travail. Contrairement au schéma schumpétérien, **les bénéfices de l'IA sont retardés, concentrés et conditionnés** à des réformes organisationnelles lourdes. Paradoxalement, ces mêmes RH sont déjà confrontées à un besoin de nouvelles compétences en sécurité et IA, rarement disponibles aujourd'hui.
- Un **risque organisationnel** avec la classique « illusion de sécurité » (« le robot gère ») se traduisant par l'affaiblissement de la culture de méfiance opérationnelle et *in fine* un sous-investissement dans la formation humaine.
- Un potentiel **impact négatif et significatif sur la qualité de vie au travail pour les travailleurs qui conservent un emploi, avec une surveillance perçue comme un contrôle social**. Les caméras et capteurs peuvent être vécus comme du « **flicage** » et on peut assister à une dégradation de la confiance si la finalité exprimée n'est pas clairement la protection du travailleur. L'IA prend le risque d'un écrasement du sens. Un bon REX est aussi narratif, contextuel et contradictoire, alors que l'IA tendra à aplatir la complexité en catégories « propres » avec un risque de recentralisation normative. L'IA peut devenir un outil renforçant la conformité, au détriment des adaptations locales intelligentes.
- Un **déplacement de la responsabilité (juridique), lié à l'opacité des modèles**. Les décisions deviennent difficiles à expliquer après incident, ce qui soulève un problème de responsabilité (opérateur, industriel ou fournisseur IA).

3.2.2 Quelques apports originaux de l'atelier

Les participants à l'atelier prospectif ont produit une liste de craintes complémentaires qui relèvent de constats par rapport au développement de l'IA dans leur entreprise.

- Il faudra **préciser clairement de quand et de quoi on parle lorsqu'on discute de risques de sécurité liés à l'IA** : s'agit-il de l'opérateur, du client, du système, du pays, et à quel horizon temporel ? L'un des grands bouleversements de l'introduction de l'IA reste la contraction de l'espace-temps et l'approche d'emblée globale de son déploiement tant entrepreneurial que sociétal.
- Certaines entreprises commencent à **acheter sur étagère des systèmes à base d'IA développés « ailleurs »**. On peut s'interroger sur la pertinence d'un système apprenant dans un univers et un pays qui n'est pas le nôtre, et donc celui de l'entreprise, à la fois sur le fond technique, mais aussi culturel. Dans le même registre, les participants constatent que certaines applications IA (surveillance des employés par caméra), déjà largement opérationnelles dans certains pays, auront plus de mal à s'imposer dans la culture française.
- **La plus grande difficulté pour reprendre la main est sans doute à venir, avec un décalage générationnel : tant que des experts seront présents, le système continuera à fonctionner**, mais lorsque ces compétences disparaîtront, qui sera encore en mesure de vérifier ce que propose l'IA ?
- Dans toutes les entreprises présentes, **le déploiement de l'IA est promu et/ou piloté par une unité dédiée et rattachée au plus haut niveau de l'entreprise**. Cette structuration explicite est importante parce qu'elle peut expliquer une attitude un peu duale chez les

participants : concernés, voire impliqués (« c'est un projet global de l'entreprise ») mais pas propriétaires (« il y a des gens qui s'en occupent spécialement » ou « c'est plus grand que moi »).

- Plus globalement, **la gestion du changement pour l'entreprise et pour la sécurité en est encore à ses débuts**. Autant le gain local de l'introduction d'un système à base d'IA est un facteur clé d'adoption locale dans les services, autant la « grande adaptation » systémique de l'entreprise n'est pas encore réellement un sujet prioritaire. Elle le deviendra, avec notamment le risque de « déshumaniser » la sécurité.
- En prolongement du point précédent, les participants notent que **leurs directions des ressources humaines (DRH) ne sont pas prêtes**. Plus globalement, l'IA est plus qu'un simple outil, elle bouleversera les organisations et collectifs de travail. Les DRH seront alors en première ligne sur ces sujets, notamment en matière de dialogue social, même si beaucoup d'incertitudes persistent et que l'agenda de leurs difficultés actuelles peut occulter leurs capacités à penser un futur proche lié à l'IA.
- **Un impact de l'IA encore plus grand sur les postes de managers** : au-delà de la perte d'emploi et d'une hypothétique « destruction créatrice » l'atelier a fortement distingué l'impact sur les cols blancs, de celui sur les cols bleus. En soulignant que, pour la première fois dans l'histoire récente, les pertes d'emplois pourraient être plus importantes chez les cols blancs.
- Une **acceptabilité sociale de l'IA qui questionne fortement le « comment traiter » l'adaptation**, avec un rythme d'innovations dépassant tous les mécanismes classiques d'adaptation industrielle, tant au sein de l'entreprise qu'à l'extérieur.

3.3 Quel scénario pour l'impact du déploiement de l'IA sur la sécurité ?

L'atelier s'est poursuivi en essayant de tracer la courbe de la fréquence des incidents/accidents industriels à long terme, suite à la diffusion progressive des technologies d'IA dans les entreprises et la société.

3.3.1 Deux courbes d'évolution connues comme point de comparaison

L'atelier avait été lancé à partir de la présentation de deux courbes connues d'évolution de l'impact de nouvelles technologies sur l'accidentologie :

- Celle de **l'automatisation en aéronautique**, relativement simple, en trois phases : une sur-accidentalité au début avec beaucoup de difficultés dans la reconversion des pilotes ; un retour d'expérience des accidents a permis des améliorations technologiques, avec le renouvellement générationnel chez les pilotes mais sans pertes d'emplois ; et pour finir une amélioration de la sécurité lente mais continue qui s'est installée sur le temps long.

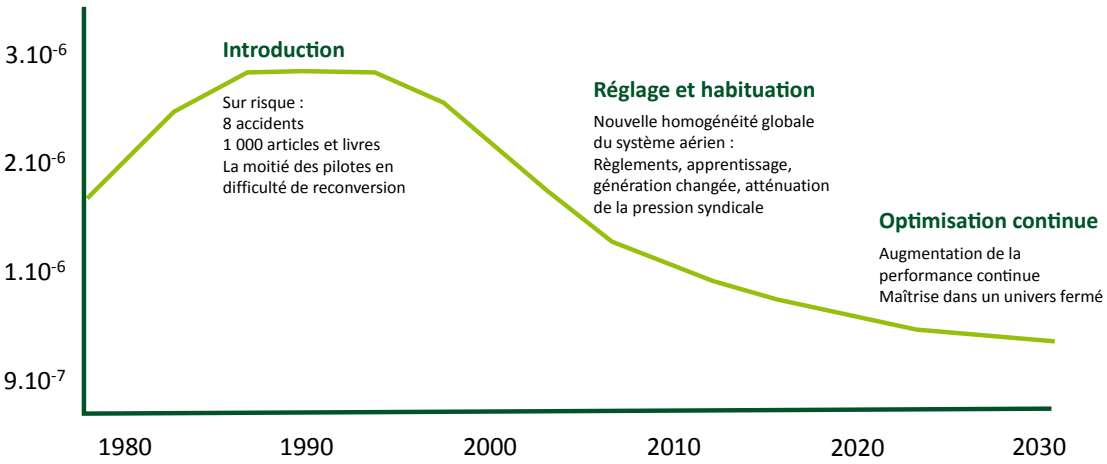

Fig. 3.2 Courbe d'évolution de l'accidentologie suite à l'arrivée de l'automatisation dans l'aviation dans les années 1980-2000.

▷ Celle du **numérique 2.0 puis 3.0 dans l'entreprise** : une évolution plus complexe et difficile au début avec une forte dispersion de l'offre souvent portée par des consultants et couplé à un effet de frein générationnel. Elle est suivie d'une adoption, largement favorisée par celle du grand public qui s'effectue en parallèle, puis d'un déploiement à très grande échelle, plutôt sans perte d'emploi et même en créations positives. Mais, elle s'est heurtée à deux freins inattendus au départ : la dépendance, liée à l'absence de maîtrise d'un cloud souverain, et le risque cyber, intensifié et diversifié au cours du temps.

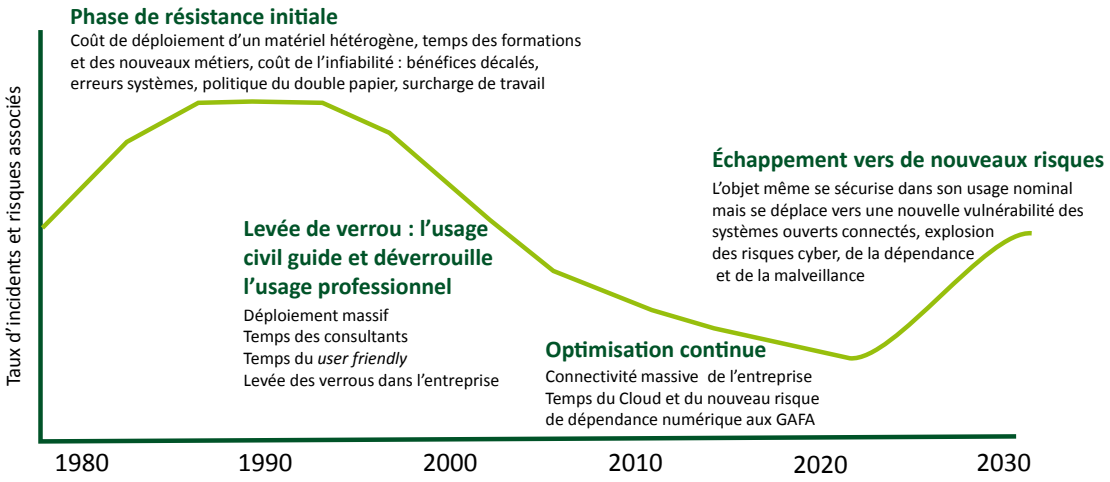

Fig. 3.3 Courbe d'évolution de l'accidentologie suite à l'arrivée du numérique 2.0 puis 3.0.

3.3.2 Propositions des phases d'évolution par les participants de l'atelier prospectif

Cette section respecte la restitution faite par chacune des cinq tables, composées d'experts industriels, pour percevoir ce qui fait consensus et ce qui a été l'apport original des uns et des autres. Il s'agissait, dans une démarche de prospective très ouverte, d'imaginer quelles pourraient être des évolutions possibles de l'accidentologie dans les systèmes industriels à risque d'accident majeur suite à l'introduction de technologies d'IA.

Scénario proposé par la première table :

Il devrait d'abord être observé une courbe d'amélioration continue de l'accidentologie ; toutefois, des effets secondaires pourraient progressivement prendre le pas sur les bénéfices attendus, et provoquer un point d'inflexion politique et économique marqué par une baisse massive du recours à l'IA, s'apparentant à une forme d'« **hiver de l'IA** ».

Par ailleurs, une augmentation constante du nombre de systèmes d'IA serait également constatée, entraînant une intensification continue des performances. Cette dynamique, initialement perçue favorablement par l'entreprise (et parfois même recherchée) **pourrait engendrer des tensions, voire un divorce social** ou une rupture d'acceptabilité du point de vue des travailleurs. Cela conduirait alors à une réduction du déploiement de ces technologies, ou du moins à une limitation de leurs domaines d'application afin d'éviter une crise du travail incontrôlable. Enfin, il serait attendu que la capacité d'apprentissage des systèmes d'IA, proche de formes d'actes créatifs et distincte des systèmes actuels, se traduise par une stabilisation, voire une baisse, du taux d'incidents ; toutefois, un risque de surconfiance et de perte de contrôle, rare mais brutal, pourrait aussi apparaître.

Scénario proposé par la deuxième table :

Deux tendances cohabiteraient, dont une qui a déjà commencé :

▷ Une tendance négative qui renverrait à **l'augmentation redoutée des risques psychosociaux**, par l'intensification du travail, la réduction des tâches à valeur ajoutée, les pertes de repères, avec un impact principalement chez les cols blancs, encore plus que chez les cols bleus. Une nouvelle réalité sociale, marquée par des capacités d'adaptation différentes selon les individus, devrait également être affrontée.

- Une tendance positive concernant les risques d'accidents aux personnes et industriels pourrait être observée, avec un premier plateau d'accidentologie, suivi d'une **baisse significative des risques** ; une troisième phase de rebond pourrait ensuite être constatée, dans la mesure où, une fois l'efficacité de l'IA établie, son intégration accrue dans les processus conduirait à une ré-augmentation des risques.

Scénario proposé par la troisième table :

Une amélioration rapide de la courbe d'accidentologie devrait être observée dans un premier temps. Toutefois, par la suite, des systèmes seraient découverts en cascade et déployés dans des applications multiples, ce qui conduirait à une courbe d'accidentologie plus oscillante, avec des résultats très variables selon le type de sécurité considéré. Dans tous les cas, **une échelle de temps courte serait retenue**, de l'ordre du mois ou de l'année plutôt que de la décennie.

Dans ce contexte, une **intervention de la réglementation** pourrait être constatée et permettrait, possiblement, d'éviter une remontée de l'accidentologie à la suite d'accidents. Par ailleurs, une complexité croissante serait observée, nécessitant des efforts d'apprentissage accrus.

Enfin, sans que cela soit certain, un phénomène d'affolement malveillant et mal maîtrisé pourrait survenir, rejoignant des situations décrites dans la science-fiction.

Scénario proposé par la quatrième table :

Le temps s'accélère avec l'IA. On passe d'une échelle de temps en décennies à une échelle en années. **L'IA devrait affecter différemment la stabilité locale des systèmes** selon la forme de déploiement choisi : soit le déploiement laissera se développer des systèmes autonomes et l'évolution sera sans doute une augmentation des risques dans l'immédiat ; soit il s'agira d'un déploiement où les opérateurs resteront en contrôle, et dans ce cas une réduction de l'accidentologie apparaîtrait immédiatement, même si les *quick wins* risqueraient de s'effacer avec le temps.

Toutefois, la dimension systémique apparaîtrait comme la plus préoccupante : contrairement à des secteurs tels que l'aéronautique, le cadre dépasserait celui de l'entreprise pour affecter l'organisation de la société dans son ensemble, ouvrant la voie à des scénarios d'évolution contrastés.

Dans ce contexte, un environnement instable lié à l'introduction de l'IA pourrait conduire à un **monde profondément remodelé par ses effets**, tant sur les formes d'entreprise que sur la réglementation. De nouveaux types d'accidents pourraient alors survenir, **incluant un risque de « crash » global** (dépassant rapidement le périmètre de l'entreprise et pouvant affecter des filières industrielles, voire des États) avec un effet d'emballement.

Scénario proposé par la cinquième table :

Ce groupe a limité son champ de réflexions à l'IA générative.

Dans la phase actuelle, **la société est presque en avance sur l'entreprise**, le citoyen est prêt à accepter cette réforme ; et il y a un intérêt convergent des individus et des entreprises, comme avec l'arrivée du numérique dans le grand public.

Dans ce contexte, un effet positif devrait être observé dans un premier temps ; toutefois, celui-ci pourrait progressivement s'atténuer en raison d'une perte d'expertise humaine. Si, ensuite, la courbe d'accidentologie venait à remonter à cause de sinistres, une contre-réaction des entreprises pourrait être observée, avec une réintroduction des experts. Parallèlement, les trajectoires professionnelles seraient repensées et des limitations d'usage plus prudentes pourraient être instaurées par la réglementation.

Par ailleurs, une autre dimension de risque serait identifiée, cette fois à l'échelle géopolitique, touchant l'ensemble de la société ainsi que la perte d'emplois qualifiés. En effet, des évolutions réglementaires et politiques pourraient survenir, mais cette contre-réaction interviendrait dans un contexte de réduction des effectifs publics et de dérégulation, déjà engagée, les

administrations étant elles-mêmes confrontées à une complexité croissante. Au bilan, on observerait la **croissance d'un risque sociétal** inefficace face aux problèmes, alors que les entreprises resteraient relativement plus agiles pour s'adapter à leur niveau.

Enfin, une forte incertitude existe quant au rythme des progrès de l'IA : les capacités actuelles peuvent être comparées à celles d'il y a cinq ans, avec des écarts déjà considérables ; **toute projection à dix ans apparaît particulièrement incertaine**.

4

Conclusion

Cet atelier prospectif sur l'IA appliqué à la sécurité industrielle est largement aligné, dans un grand nombre de ses conclusions, avec les publications existantes. En ce sens, **le contenu n'est pas révolutionnaire**.

On peut toutefois en retenir **sept traits importants** qui sont autant de témoignages des préoccupations du moment, plus originaux en regard des discours convenus sur le sujet :

1. **L'IA est déjà dans l'entreprise**, diffuse, plus ou moins accompagnée, avec une vitesse de pénétration mesurée en mois et en années, plutôt qu'en décennies.
2. L'arrivée de l'IA (surtout générative) n'a pas d'égal dans le passé sur ses effets qui sont d'emblée systémiques et globaux par sa pénétration profonde dans tous les usages de la société. Le **séisme social** induit (emploi, usages, organisation et gouvernance de l'entreprise) sera peut-être plus dimensionnant que le risque d'accident industriel classique.
3. Les entreprises ont, pour certaines, des groupes de réflexion amont, mais le **concret des changements à faire n'est pas encore clair**, particulièrement pour les DRH qui sont en première ligne face à l'impact social de l'arrivée de l'IA.
4. Toutes ces craintes exprimées vis-à-vis de l'IA renvoient à un consensus largement partagé : **il faut absolument que l'homme et l'entreprise restent en contrôle de cette révolution industrielle**… mais tous les participants en doutent un peu dans la réalité du déploiement.
5. Le bénéfice pour la sécurité de l'introduction de l'IA est **potentiellement immense**, et devrait être substantiel particulièrement dans la réduction des accidents graves et mortels.
6. Toutefois, ce bénéfice va aussi se heurter à un **effet secondaire massif** de perte de sens, de désengagement de l'agent humain, et sans doute concerner pour la première fois davantage les cols blancs que les cols bleus.
7. Les premiers accidents de systèmes à bases d'IA seront l'occasion d'une **législation et de nouvelles recommandations**. Le chemin réglementaire pourrait alors infléchir sérieusement à la baisse l'usage de ces systèmes (et conduire à un « hiver de l'IA »).

Bibliographie

Aghion, P., Bunel, S., Jaravel, X. *et al.* (2025). *How different uses of AI shape labor demand: Evidence from France*. AEA Papers and Proceedings, 115:62–67. DOI : 10.1257/pandp.20251047.

Aslam, M. M., Tufail, A., Gul, H. *et al.* (2025). *Artificial intelligence for secure and sustainable industrial control systems - a survey of challenges and solutions*. Artificial Intelligence Review, 58(11). DOI : 10.1007/s10462-025-11320-9.

Azeta, J., Omeche, T. T., Daniyan, I. *et al.* (2026). *Artificial intelligence and robotics in predictive maintenance: a comprehensive review*. Frontiers in Mechanical Engineering, 11. DOI : 10.3389/fmech.2025.1722114.

Bieder, C., Amalberti, R., Pariès, J. *et al.* (2024). *La sécurité à l'ère du « vivre avec » : Incertitude, complexité et nouvelles attentes*. Cahier de la sécurité industrielle 2024-05, Fondation pour une culture de sécurité industrielle. www.foncsi.org, DOI : 10.57071/420yzp.

Bieder, C., Kamaté, C., Laroche, H. *et al.*, Éd. (2026). *Living with the New Safety Landscape I: Rethinking Safety Management in the Context of Cascading Uncertainties*. SpringerBriefs in Safety Management. Springer. ISBN : 978-3032293350.

Gihleb, R., Giuntella, O., Stella, L. *et al.* (2022). *Industrial robots, workers' safety, and health*. Labour Economics, 78. DOI : 10.1016/j.labeco.2022.102205.

Hashmi, F., Hassan, M. U., Zubair, M. U. *et al.* (2024). *Near-miss detection metrics: An approach to enable sensing technologies for proactive construction safety management*. Buildings, 14(4). DOI : 10.3390/buildings14041005.

Huber, J., Anzengruber-Tanase, B., Schobesberger, M. *et al.* (2025). *Evaluating user safety aspects of AI-based systems in industrial occupational safety: A critical review of research literature*. International Journal of Environmental Research and Public Health, 22(5). DOI : 10.3390/ijerph22050705.

ILO (2025). *Revolutionizing health and safety: The role of AI and digitalization at work*. Rapport technique, International Labour Organization. DOI : 10.54394/KNZE0733.

Kogelmann, B. (2025). *Creative destruction and the autonomous life*. Journal of Business Ethics, 197(4):659–671. DOI : 10.1007/s10551-024-05721-z.

Le Coze, J.-C. et Antonsen, S., Éd. (2023). *Safety in the Digital Age: Sociotechnical Perspectives on Algorithms and Machine Learning*. SpringerBriefs in Safety Management. Springer. ISBN : 978-3031326332.

Lopez, P., Erwin, J., Hopper, D. *et al.* (2025). *From traditional robotic deployments towards assisted robotic deployments in nuclear decommissioning*. Frontiers in Robotics and AI, 12. DOI : 10.3389/frobt.2025.1432845.

Malenfer, M., Héry, M. et Clerté, J. (2022). *Intelligence artificielle au service de la santé et sécurité au travail : Enjeux et perspectives à l'horizon 2035*. Hygiène & sécurité du travail, 269:87–96. www.inrs.fr/media.html?refINRS=VP%2036.

Marsden, E. et Steyer, V. (2025). *L'IA et la gestion de la sécurité: enjeux et questions clés*. Cahier de la Sécurité Industrielle 2025-01, Fondation pour une culture de sécurité industrielle (FonCSI). www.foncsi.org, DOI : 10.57071/iae289.

NSC (2023). *Improving workplace safety with robotics*. Rapport technique, US National Safety Council.

Park, J. et Kang, D. (2024). *Artificial intelligence and smart technologies in safety management: a comprehensive analysis across multiple industries*. Applied Sciences, 14(24). DOI : 10.3390/app142411934.

Rizvi, S. A. H. (2026). *The productivity paradox revisited: Artificial intelligence, labour market restructuring, and the inequality trap*. Oxford Journal of student scholarship. DOI : 10.65161/rec4D7lEPE4FTkgap.

Sakshi, G., Shreya, J., Vidya, S. *et al.* (2024). *Enhancing worker safety in the construction industry through smart helmet technology, a review*. International Journal of Creative Research, 12(10). www.ijcrt.org/papers/IJCRT2410466.pdf.

Schumpeter, J. A. (1935). *Théorie de l'évolution économique : Recherches sur le profit, le crédit, l'intérêt et le cycle de la conjoncture*. Dalloz. ISBN : 978-2247004547.

Schumpeter, J. A. (1951). *Capitalisme, socialisme et démocratie*. Payot. ISBN : 978-2228883177.

Vukicevic, A. M., Petrovic, M., Milosevic, P. *et al.* (2024). *A systematic review of computer vision-based personal protective equipment compliance in industry practice: advancements, challenges and future directions*. Artificial Intelligence Review, 57(12). DOI : 10.1007/s10462-024-10978-x.

Zaidi, S. H. H., Shenfield, A., Zhang, H. *et al.* (2026). *A systematic review of anomaly and fault detection using machine learning for industrial machinery*. Algorithms, 19(2). DOI : 10.3390/a19020108.

You can extract these bibliographic entries in BibTeX format by clicking on the paperclip icon.

Reproduction de ce document

La Foncsi soutient le libre accès (“*open access*”) aux résultats de recherche. Pour cette raison, elle diffuse gratuitement les documents qu’elle produit sous une licence qui permet le partage et l’adaptation des contenus, à condition d’en respecter la paternité en citant l’auteur selon les standards habituels.

Vous pouvez télécharger ce document, ainsi que d’autres dans la collection des *Cahiers de la Sécurité Industrielle*, depuis le site web de la Foncsi.

FONCSI
Fondation pour une culture de sécurité industrielle

Fondation pour une Culture de Sécurité Industrielle

Fondation de recherche reconnue d’utilité publique

`www.FonCSI.org`

6 allée Émile Monso – CS 22760
31077 Toulouse cedex 4
France

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