Préface

Les experts dans la sécurité de l'industrie des procédés ont vu leur métier évoluer au cours de la dernière décennie. L'arrivée de l'industrie 4.0, avec ses systèmes de contrôle tous numériques et communicants par l'Internet, a permis l'intégration et le contrôle à distance des unités de production. Ceci nous donne une efficacité et une réduction de coûts importantes, mais il ouvre le chemin à des acteurs malveillants provenant de n'importe où dans le monde. Il n'y a plus de sécurité des procédés sans penser à la cybersécurité. Et bien sûr, il faut aussi intégrer la « SST classique », la santé et sécurité au travail, dans cette démarche. L'industrie 4.0 a besoin d'une approche globale à sa sécurité : la « sécurité 4.0 ».

Cet ouvrage, qui s'adresse à une audience internationale, tente de démontrer l'importance de cette intégration et de définir les éléments qui la construisent. Il nous fournit des exemples, provenant de différents points dans l'univers très diversifié de l'industrie des procédés. Il nous invite à en tirer des leçons générales applicables à beaucoup d'autres activités. Le point principal à retenir de ces exemples est la nécessité d'impliquer des experts en sécurité dès le début de la conception de nouveaux systèmes ou de la mise à jour de systèmes existants. Il ne suffit pas de les convoquer pour valider – ou encore pire, ajouter une couche « sécurité » à – un développement conçu sans leur participation.

Or – ceci est aussi très clairement défini dans cet ouvrage –, nous n'allons pas nous arrêter à l'industrie 4.0 telle qu'elle est aujourd'hui. Nous voyons déjà beaucoup d'exemples de l'intensification de l'industrie des procédés et nous allons sûrement en découvrir davantage, que ce soit la miniaturisation, le remplacement des procédés discontinus par des procédés continus, la multifonctionnalité, ou d'autres approches et technologies de rupture. Et ceci peut représenter un défi considérable pour la sécurité – un des rapports du projet IMPULSE cité dans ce livre déclare que « la gamme des conditions optimales de réaction est presque congruente avec le danger d'une réaction

non contrôlée ». Sans doute certains des développements contribueront directement à la sécurité – les mots-clés sont « intrinsèquement sûr » et « sécurité propre » – mais le livre nous démontre aussi certaines des difficultés associées à ces mots-clés.

Et une dernière considération : même avec tous les outils d'analyse décrits dans ce livre, il y a un élément fondamental de la maîtrise des risques qui a besoin de l'imagination humaine et de la gamme d'expériences la plus large possible – l'identification des dangers. L'expérience du Bureau des risques d'accidents majeurs de la Commission européenne nous démontre qu'un bon nombre d'accidents dans l'industrie des procédés implique un danger non apprécié lors de l'analyse des risques de l'établissement.

Donc, il y a du travail à faire !

Neil MITCHISON
Ancien chef, Bureau des risques d'accidents majeurs,
Commission européenne
Ancien président, conseil scientifique, INERIS

Avant-propos

Le concept d'industrie du futur repose sur une combinaison de technologies numériques, qui ont comme point commun de permettre une intégration numérique de l'ensemble du fonctionnement d'une unité de production. Cette intégration numérique est un facteur important pour le développement d'un nouveau procédé et pour l'adaptation ou la reconfiguration à la demande d'un procédé existant. Ces technologies de l'industrie 4.0 concernent entre autres les équipements et la façon de les concevoir, ainsi que les systèmes d'acquisition et de traitement des données du procédé. L'utilisation de ces technologies n'est cependant pas sans risque. Une évaluation en est nécessaire, en examinant l'apparition de nouveaux risques et l'accentuation ou le déplacement des risques déjà existants. Dans les installations industrielles classiques, plusieurs mesures de protection, notamment des systèmes modernes de commande avancée des procédés (APC), des systèmes de décompression et de déclenchement automatique, sont en place pour prévenir les risques. Pourtant, les incidents liés à la sécurité des procédés continuent de se produire. Leur fréquence est plus susceptible de se produire lors des phases de démarrage, car la plupart des systèmes APC sont désactivés et les procédés de l'usine fonctionnent alors en mode manuel. Les alarmes sont probablement désactivées ou ignorées, car ces signaux sont conçus pour surveiller les variations du procédé en régime permanent. Parfois, les unités peuvent, pour atteindre la production, fonctionner à la limite de la zone de fonctionnement opérationnel, juste au seuil d'alarme avant le déclenchement, ce qui génère plus d'arrêts et crée plus de redémarrages. Beaucoup d'informations et de données sont collectées sur le procédé, mais la plupart d'entre elles se trouvent dans différents silos de données et sont peu analysées ou intégrées de manière à permettre une surveillance efficace des risques liés à la sécurité des procédés. Avec l'essor des nouvelles technologies numériques de l'industrie du futur, ces silos de données peuvent désormais être combinés et analysés. Cette intégration des données peut révéler par exemple quelles parties de l'usine sont vulnérables et sujettes à plus de problèmes ou à un risque plus élevé. Les données

peuvent également indiquer quel ensemble de paramètres est optimal pour éviter les problèmes et peuvent aider à prédire le prochain dysfonctionnement. La création des environnements virtuels peut permettre aux opérateurs d'acquérir une expérience pratique grâce à la simulation afin d'identifier les bons réglages pour la température, la pression, le débit, la position des vannes, etc. Ces méthodes de réalité virtuelle aident les opérateurs à prendre des décisions dans différents scénarios afin de réduire les erreurs, les confusions et les risques.

L'objectif de l'ouvrage *Vers la sécurité 4.0 des procédés de l'usine du futur* consiste à identifier et répertorier différents attributs et éléments essentiels de la sécurité industrielle, afin de contribuer à la sensibilisation des différentes parties prenantes, en mettant l'accent sur l'implication de la sécurité 4.0 des procédés de l'industrie 4.0.

Le chapitre 1, « L'ère de la révolution industrielle 4.0 », présente d'abord un rappel de la chronologie historique des différentes révolutions industrielles. La définition de l'usine du futur est indiquée. Les technologies numériques de rupture ou d'innovation, de la communication, de l'interconnexion et de la gestion des données de l'industrie 4.0 sont ensuite détaillées. Enfin, l'impact potentiel sur la sécurité de la structuration des technologies numériques est discuté.

Le chapitre 2, « Le concept de sécurité 4.0 », définit le concept de sécurité 4.0, examine l'histoire de l'évolution de la sécurité industrielle et propose un cadre de convergence de l'usine du futur et d'un nouveau management de la sécurité.

Le chapitre 3, « Santé et sécurité au travail », identifie d'abord l'impact des technologies numériques sur les conditions de travail des parties prenantes. Une revue détaillée des caractéristiques communes et distinctes des rôles de la santé et sécurité au travail et de la sécurité des procédés est ensuite développée. Un inventaire des différentes méthodes et techniques traditionnelles d'analyse des risques industriels est établi. Leurs concepts, leurs paradigmes, leurs bases de structuration, les natures de leurs couplages et leurs complexités sont précisés. L'applicabilité des méthodes à chacun des deux types de sécurité (SST et procédés) est commentée.

Le chapitre 4, « Sécurité des procédés et cybersécurité », débute par la comparaison des points de vue des démarches respectives de la cybersécurité et de la sécurité des procédés. Les méthodes respectives EBIOS et de l'arbre d'attaque de l'analyse des risques des systèmes d'information industrielle sont décrites. Une approche coordonnée et de réconciliation des méthodes d'analyse des risques de sécurité des procédés et de cybersécurité montre la richesse de leurs synergies et interactions. Les nombreuses analogies, telles que l'analyse préliminaire des risques et la Cyber APR, les méthodes HAZOP et Cyber HAZOP, les graphes du nœud papillon et cybernœud papillon, les méthodes LOPA et Cyber LOPA et la méthode intégrée dite ATBT sont soulignées.

Enfin, la prudence de l'usage des matrices de risques et des matrices concaténées est conseillée.

Le chapitre 5, « Exemples : sécurité 4.0 et procédés », regroupe de façon inédite différents exemples illustrant la place et l'influence de la sécurité 4.0 dans la conception, la mise en œuvre, l'exploitation, la reconfiguration et la reconception des procédés du futur. La diversité des 16 exemples sélectionnés montre pratiquement la nature spécifique de chaque approche et la pluralité des technologies numériques mises en œuvre.

Le chapitre 6, « Intensification et sécurité propre : mythe ou réalité ? », rappelle au début quelques éléments essentiels de l'intensification des procédés. Ensuite, neuf exemples de procédés d'intensification sont décrits en soulignant systématiquement l'aspect sécurité 4.0. Un essai de rationalisation et un cadre général pour la synthèse et la conception d'équipements intensifiés, intégrant des indicateurs et des limitations complexes de la sécurité, sont proposés. Le mythe et/ou la réalité *a priori* de la sécurité 4.0 sont auscultés méthodiquement à l'aide d'outils et de méthodes dédiés à la sécurité intrinsèque. Leur application à l'examen détaillé de six exemples montre l'existence de conflits avérés de la sécurité 4.0 par rapport au procédé, en particulier lors de l'étude du comportement dynamique des procédés d'intensification.

L'exigence des enjeux des produits et procédés de l'industrie 4.0 implique simultanément les bonnes pratiques de la prévention des risques, de la santé et sécurité au travail, de la sécurité des procédés et de la cybersécurité, ainsi que l'acceptation sociétale et la responsabilité environnementale. Le contenu de ce livre devrait inciter à un dialogue réciproque entre les professionnels des technologies numériques et les acteurs de la sécurité industrielle. La diversité des nombreux exemples présentés devrait permettre d'aborder par analogie les problèmes et questions relatives à la sécurité 4.0 de nouveaux procédés émergents de l'industrie du futur. L'appropriation du concept de sécurité 4.0 et de sa mise en œuvre doit être l'affaire de toutes les parties prenantes.

Remerciements

J'exprime toute ma gratitude et toute mon amitié à Jean-Pierre Corriou, professeur émérite à l'Université de Lorraine, qui a partagé avec une disponibilité exceptionnelle toutes les incertitudes scientifiques et matérielles de la progression de l'ouvrage. Ses contributions pragmatiques et sémantiques en réponse à mes inlassables sollicitations et interrogations ont été stimulantes.

Je suis très honoré que monsieur Neil Mitchison ait accepté de bien vouloir écrire la préface de ce livre et je l'en remercie vivement. J'ai eu la chance de partager et d'apprécier au sein de l'INERIS ses compétences internationalement reconnues dans

le domaine de la sécurité dans ses différentes fonctions professionnelles au sein de la Communauté européenne à Bruxelles (Belgique) et Édimbourg (Écosse) et au Joint Research Center d'Ispra (Italie).

J'adresse aussi mes chaleureux remerciements à Roda Bounaceur, Bruno Delfolie, Gérard Verdier et Valérie Warth, ingénieurs au service Réseaux, administration, informatique et développement du LRGP, qui ont établi avec professionnalisme les conditions robustes d'équipements en matériels et en logiciels me permettant de travailler en distanciel.

J'associe à mes remerciements Laure Thomas-Geoffroy pour sa résiliente assistance à la documentation scientifique.

Je salue la fidèle présence à mes côtés de mes collègues Laurent Perrin et Olivier Dufaud, professeurs de sécurité des procédés à l'Université de Lorraine, qui m'accueillent au sein du groupe SAFE.

Je ne saurais terminer sans souligner le soutien constant de ma famille.