Préface

La cybersécurité est l'une des grandes préoccupations de notre époque. Les risques de cyber-attaques accompagnent en effet le développement des systèmes numériques et leur mise en réseau, au travers d'Internet notamment. Ces risques concernent tous les types d'installations, et les attaques peuvent être le fait d'intervenants isolés – les « hackers » qui, selon leur éthique (pour autant qu'ils en aient une) vont être qualifiés de « white, grey ou black hats » –, mais elles peuvent être également l'œuvre d'organisations criminelles internationales, voire de services d'États agissant au niveau de l'offensive comme de la contre-offensive.

Les motivations de ces attaques sont très diverses : volonté de perturber, de nuire voire détruire, vol d'informations, menace, intimidation, chantage, vengeance, extorsion de fonds, démonstration de force, etc. Les exemples en sont à présent innombrables et les systèmes industriels, petits ou grands, que l'on a crus longtemps protégés du fait de leurs spécificités et de leur isolement du monde extérieur (le fameux *air gap*), ne sont plus à l'abri de menaces de forme et d'ampleur très diverses.

Les conséquences d'attaques réussies peuvent être lourdes car, dans le monde industriel, on cherchera bien sûr à protéger le système d'informations et les données qu'il comporte, mais l'objectif premier est d'éviter que des perturbations graves ne surviennent au niveau des procédés contrôlés. Ces perturbations peuvent entraîner des arrêts de production insupportables pour les industriels, quelle que soit leur taille, et générer des dommages à l'environnement, aux biens et aux personnes, avec des conséquences qui peuvent être majeures. Il est aisé d'imaginer des scénarios catastrophes susceptibles d'affecter des installations sensibles dans les domaines de la production d'énergie, du traitement de l'eau, des transports et plus généralement des grandes infrastructures.

L'industrie se trouve donc confrontée à un vrai problème qu'elle ne peut plus ignorer et chaque responsable a le devoir d'évaluer les risques auxquels l'installation dont il a la charge est exposée, et de prendre des mesures de protection appropriées. Les responsables industriels restent cependant perplexes sur les mesures à prendre et sur l'organisation à mettre en place. S'ils veulent bien admettre la réalité du risque, ils ont souvent du mal à en percevoir l'origine et l'ampleur, et à en admettre les conséquences possibles.

Pourtant, depuis longtemps, l'industrie s'est habituée à traiter de la sécurité fonctionnelle et des risques de défaillance de constituants et de composants, et d'erreurs de manipulation d'opérateurs pouvant affecter des fonctionnalités essentielles. L'appréhension de ces risques a donné naissance à des normes internationales : l'IEC 61508 relative à la sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables, et l'IEC 61511 spécifique au secteur des industries de transformation, elle-même issue du standard ISA-84 développé par l'ISA (International Society of Automation). Ces problèmes peuvent se traiter de façon probabiliste à partir des données issues de l'expérimentation et de l'expérience, car les menaces sont non intentionnelles.

Dans le cas de la cybersécurité, on sait qu'il existe des menaces, qui vont provenir de l'extérieur, peut-être aussi de l'intérieur, mais sous quelle forme, avec quelle ampleur et avec quelle probabilité ? S'agissant de menaces d'actions intentionnelles, on est dans un domaine d'appréciation purement subjectif pouvant donner lieu à une surestimation, entraînant alors un niveau de protection qui sera préjudiciable à la compétitivité de l'entreprise, ou à une sous-estimation qui fera poser sur l'entreprise un risque intolérable.

En outre, les techniques d'attaque évoluent et se perfectionnent. Des simples virus des années 1990, détectables par leur signature, on est passé à des logiciels malveillants qui sont des constructions informatiques complexes capables de communiquer avec l'extérieur, pouvant s'enrichir et se propager, et aptes à prendre à distance le contrôle d'installations. Certaines attaques sont ciblées, comme l'ont été, à la fin des années 2015 et 2016, les attaques contre les réseaux électriques ukrainiens, d'autres sont à spectre large, comme les attaques Wannacrypt et NotPetya, qui ont créé des perturbations sérieuses sur de nombreuses installations industrielles, y compris en France.

Les entreprises peuvent faire l'objet de demandes de rançon à partir de rançongiciels (*ransomwares*) dont la pratique est devenue courante ; elles peuvent aussi être complices à leur insu d'attaques en déni de service distribué, car les objets connectés – tout particulièrement ceux qui sont connectés de façon permanente à Internet tout en étant insuffisamment protégés : caméras de surveillance, imprimantes, boxes – peuvent être enrôlés dans des réseaux de zombies (*botnets*), manipulés à distance pour participer à des attaques massives.

Le développement de l'Internet industriel des objets va élargir fortement les surfaces d'attaque avec la mise en réseau d'un nombre considérable d'appareils divers qu'il sera impossible de surveiller individuellement, et dont on devra se méfier de l'origine, des conditions de développement et de la façon dont ils stockent et échangent les informations.

Les industriels sont souvent désorientés sur la façon d'aborder le problème, mais le contexte normatif et réglementaire les pousse à ne pas rester inactifs. En France, l'ANSSI a été chargée, par la loi sur la programmation militaire du 18 décembre 2013 et les décrets du 27 mars 2015, de veiller à la sécurité des systèmes d'information des opérateurs d'importance vitale. Plus récemment, la directive européenne NIS (*Network and Information Security*), transposée en droit français par la loi du 26 février 2018 et le décret du 23 mai 2018, a introduit des obligations pour tous les opérateurs de services essentiels.

Il est probable que les assureurs exerceront également une pression croissante pour que toutes les entreprises prennent des mesures de protection appropriées.

L'ouvrage de Jean-Marie Flaus vient donc à point nommé et répond à un besoin essentiel. Il constitue un outil extrêmement précieux pour mieux comprendre les enjeux de la cybersécurité et les solutions auxquelles on peut faire appel. Jean-Marie Flaus est professeur à l'université Grenoble Alpes. Il est aussi enseignant-chercheur et responsable du département Gestion et conduite des systèmes de production au laboratoire G-SCOP, Sciences pour la conception, l'optimisation et la production. Le laboratoire G-SCOP est un laboratoire pluridisciplinaire créé à Grenoble en 2007 par le CNRS, Grenoble-INP et l'Université Grenoble Alpes, afin de répondre aux défis scientifiques posés par les mutations du secteur industriel. La cybersécurité est clairement de ceux-là.

L'auteur l'aborde dans son ouvrage avec un œil d'enseignant et de praticien. Son approche est volontairement didactique et vise à faire comprendre, par le détail, la nature et l'ampleur des menaces auxquelles l'industrie est confrontée. Son propos n'est pas d'alarmer inutilement, mais de donner les clés d'une évaluation aussi objective que possible des risques encourus qui seront, au passage, collationnés avec ceux qu'une analyse de sécurité fonctionnelle aura pu faire apparaître, afin d'aboutir à une identification des risques industriels encourus aussi complète et aussi homogène que possible.

Mais Jean-Marie Flaus est aussi un praticien, animant en particulier les travaux du groupe « Cybersécurité des installations industrielles et de l'Internet des objets » au sein de l'Institut pour la maîtrise des risques (IMdR). Une fois dressé le panorama des menaces et des vulnérabilités, l'auteur expose la démarche à suivre pour y faire face, en

s'appuyant notamment sur les référentiels normatifs auxquels il est possible de faire appel. Le tissu des normes est souvent considéré comme complexe et abscons mais, sans se perdre dans leur arcanes, Jean-Marie Flaus en explique la philosophie et la démarche, en mettant l'accent sur les deux plus importants : la série des normes ISO 27000 et la série IEC 62443. Cette dernière série normative résulte d'un long travail, entrepris au sein du comité ISA99 de l'ISA, il y a plus de dix ans et aujourd'hui en voie de complétion. La norme IEC 62443 est le seul texte de caractère normatif spécialement dédié aux systèmes de contrôle industriel ; elle a un double mérite :

– d'une part, elle segmente les obligations à satisfaire tout au long du cycle de vie d'un système de contrôle selon le rôle que l'on y joue : développeur ou fabricant de produits, fournisseur de services d'intégration, exploitant, fournisseur de services de maintenance ;

– d'autre part, elle réalise la jonction et la synthèse entre les mesures de nature technique et les mesures de nature organisationnelle nécessaires pour atteindre un niveau de sécurité donné à l'issue d'une analyse de risque.

Comme l'explique fort bien Jean-Marie Flaus, l'organisationnel et le technique doivent aller de pair. Il ne sert à rien d'installer des pare-feu si la façon de les exploiter et de les programmer n'est pas définie. Inversement, les « policies & procedures », aussi sophistiquées qu'elles soient, n'ont aucun intérêt si elles ne sont pas supportées sur le plan technique.

Le lecteur trouvera dans l'ouvrage une description des techniques de protection classiques et des plus avancées d'entre elles, mais aussi un énoncé des règles et de la méthode à suivre pour construire un système de gestion de la sécurité de l'information adapté au cas de chaque installation industrielle. Il faut, pour qu'un tel système soit complet, penser « protection » mais agir également au niveau de la « prévention » et de la « détection précoce » des intrusions, notamment des trafics anormaux permettant de penser qu'une attaque est en préparation. Il faut aussi, car l'hypothèse d'une attaque réussie ne peut être écartée, réfléchir à la façon de la contenir, par une défense en profondeur appropriée, et de restaurer le fonctionnement normal du système en commençant par les services essentiels.

De tout ceci, Jean-Marie Flaus fait un exposé clair et précis, sans jamais tomber dans l'abstraction, et en traitant également d'une démarche simplifiée de maîtrise des risques, lorsque les enjeux sont faibles et ne justifient pas des analyses trop sophistiquées.

C'est un livre d'où l'on peut extraire certains chapitres pour en faire une lecture approfondie ; c'est aussi un ouvrage qui peut se lire dans son intégralité, sans ennui et où l'on apprend beaucoup. C'est à coup sûr un travail qui deviendra un ouvrage de référence

que chaque industriel devra avoir *a minima* consulté et conserver à proximité, et qui sera extrêmement précieux à tous les professionnels de la cybersécurité pour mieux en faire comprendre les enjeux et les solutions.

Jean-Pierre HAUET
Président d'ISA-France
Voting member du comité ISA99

Introduction

I.1. La cybersécurité industrielle, qu'est-ce que c'est ?

De nos jours, de plus en plus de systèmes physiques fabriqués par l'homme sont pilotés par un système informatique. C'est le cas des systèmes autonomes comme les véhicules, les appareils du quotidien et c'est aussi le cas des systèmes de production industriels ou des systèmes de distribution d'eau ou d'énergie. Ces systèmes sont aussi pour la plupart connectés d'une façon ou d'une autre à Internet.

La sécurité informatique de ces équipements devient une question majeure pour le monde industriel. C'est tout particulièrement vrai aujourd'hui, dans le contexte de l'usine du futur, appelée aussi Industrie 4.0, qui est présentée comme la quatrième révolution industrielle, et qui se caractérise par des systèmes de plus en plus connectés et par l'intégration de plus en plus forte des technologies numériques dans les processus de fabrication.

L'actualité est riche en cyber-attaques spectaculaires : celles-ci visent à voler des identifiants, à faire en sorte que certains systèmes ou sites Web soient dans l'incapacité de fonctionner correctement, ou essaient de bloquer des postes de travail en chiffrant les données dans le but d'obtenir une rançon.

Les systèmes de pilotage des installations industrielles sont eux aussi l'objet d'attaques, soit par effet collatéral d'une attaque informatique, comme dans le cas de Wanacry (Symantec 2017 ; May *et al*. 2018), ce qui peut entraîner des arrêts d'usine et des pertes d'exploitation importantes, soit de façon spécifique avec une attaque des systèmes industriels. C'est le cas de l'attaque Stuxnet (Falliere *et al.* 2011) qui avait pour objectif de détruire les capacités de production d'uranium en Iran, ou de l'attaque Triton (White 2017) qui visait à rendre inopérants les systèmes de sécurité. D'autres attaques récentes sont présentées dans le chapitre 4.

Les dommages potentiels qui peuvent être engendrés sont nombreux et vont de simples pertes de rendement à des dommages matériels et humains, en passant par des pertes d'information qui peuvent être très graves. Compte tenu de l'importance de l'impact de ces dommages potentiels, et compte tenu de la fréquence des attaques, le risque lié à la cybersécurité des systèmes industriels est devenu important.

Pendant longtemps, ce risque a été négligé : les installations industrielles étaient peu connectées aux réseaux de l'entreprise ou à Internet, et les systèmes de contrôle industriels (ICS, *Industrial Control Systems*) semblaient protégés. L'évolution de la technologie, des usages et des besoins a conduit à relier ces systèmes aux autres réseaux, que ce soit pour le transfert de données de production vers les systèmes informatiques de l'entreprise, pour la maintenance à distance ou pour les mises à jour. Parallèlement, la convergence des protocoles vers des standards communs a augmenté la vulnérabilité des systèmes de contrôle. L'idée que les systèmes industriels pouvaient être considérés comme isolés du reste du monde, ce qu'on appelle parfois le mythe de l'*air gap*, est irréaliste de nos jours.

Le facteur aggravant de cet état de fait est que, comme la plupart des technologies et protocoles ont été conçus à une époque où les cyber-attaques n'existaient pas, ils sont peu sécurisés et très vulnérables. De nombreuses installations les utilisent encore. Le taux de renouvellement des systèmes et des matériels utilisés dans les ICS étant très faible, des appareils relativement anciens sont encore en service. La durée de vie des installations, beaucoup plus importante pour les ICS que pour les systèmes informatiques classiques, constitue une vulnérabilité supplémentaire. Pour les installations les plus récentes qui sont en train de se mettre en place autour de l'Internet des objets industriel, un nouveau facteur de risque fait son apparition, celui lié à la complexité et la flexibilité des installations.

Le risque est donc bien réel et ne peut être ignoré. Il convient donc de le maîtriser. Comme dans les autres domaines, le risque zéro n'existe pas, il faut faire en sorte de le contenir dans une zone acceptable. Par conséquent, il faut évaluer le risque et le traiter de manière appropriée, c'est-à-dire choisir les actions pertinentes à mettre en place. En fonction des enjeux et du contexte, les réponses seront bien sûr différentes. Les mesures ne peuvent pas se limiter à des actions techniques, elles doivent s'inscrire dans un plan de management des risques qui peut rester simple (chapitre 3), mais qui doit être global et prendre en compte les aspects humains et organisationnels. Par ailleurs, comme le risque zéro n'existe pas, il est utile de mettre en place un plan de reprise et de continuité d'activité, voire un plan de gestion de crise. Celui-ci pourra s'appuyer sur un système de détection et une chaîne d'alerte. L'ensemble de la démarche doit bien sûr prendre en compte le ratio coût-bénéfice.

I.2. De la sécurité de l'information à la cybersécurité

La sécurité d'un système d'information (SI) concerne tous les aspects liés à la maîtrise des risques du SI et a pour objectif de garantir :

– le fonctionnement optimal du SI permettant d'obtenir la meilleure qualité de service ;

– qu'aucun dommage inacceptable ne pourra affecter les différents éléments du SI (au-delà d'un niveau fixé) ;

– qu'aucun fonctionnement non souhaité ne pourra entraîner, directement ou indirectement, des dommages inacceptables pour le reste de l'entreprise ou les partenaires (au-delà un niveau fixé).

Le terme « cyber » est un préfixe provenant du mot grec *Kubernêtikê* signifiant « diriger, gouverner ». En 1948, Norman Wiener a introduit le terme « cybernétique » pour désigner les sciences relatives au contrôle et à la communication entre l'être vivant et la machine. « cyber » est devenu relatif à ce qui est lié à l'informatique, et on parle de cyberespace pour désigner l'extension de notre espace naturel par Internet.

La cybersécurité concerne la sécurité informatique des systèmes connectés à Internet et appartenant au cyberespace. Les cyber-attaques sont des attaques informatiques dans le cyberespace, s'ajoutant aux menaces existantes pour les systèmes d'information.

Par abus de langage, on parle souvent de cybersécurité pour tout ce qui est relatif à la sécurité informatique (Niekerk et Solms 2016).

I.3. Y a-t-il vraiment un risque pour les systèmes industriels ?

Les cyber-attaques ne concernent pas beaucoup les systèmes industriels ou cyber-physiques.

Il est vrai que la plupart des attaques concernent les systèmes informatiques classiques. Ces attaques ne se comptent plus et les outils pour créer des attaques se démocratisent. Les moyens mis en œuvre par le cybercrime organisé ont pris une ampleur considérable.

En ce qui concerne les systèmes industriels, les attaques sont en nombre limité et, souvent, montrent que l'attaquant a une connaissance très pointue des systèmes attaqués et a mis en œuvre une attaque sur mesure.

Faut-il en déduire que le risque lié à la cybersécurité des systèmes industriels est faible ? La réponse est bien sûr non. Le niveau de risque est fonction de la gravité des

dommages et de leur possibilité de réalisation. Pour une installation industrielle ou une installation nucléaire, les dommages peuvent être catastrophiques, et impacter la population. La possibilité de réalisation des dommages est au moins du même niveau que pour les systèmes informatiques de gestion. Le niveau de risque est donc très important. Il suffit pour s'en convaincre d'observer l'évolution des obligations réglementaires, comme par exemple la LPM (Loi de programmation militaire) en France, la directive NIS (*Network and Information Security*) en Europe ou le *Critical Infrastructures Protection Act* aux États-Unis.

Le système est isolé d'Internet, donc il ne risque rien.

Pendant longtemps, on a cru que le fait de ne pas être connecté à Internet suffisait à éviter tout risque de piratage informatique. On parle parfois du mythe de l'*air gap*. En fait, la situation est plus complexe :

– tout d'abord, même si un système n'est pas connecté, il peut être victime de malveillances informatiques, Stuxnet en est un exemple démonstratif. Le vecteur d'attaque était une clé USB ;

– souvent, le réseau industriel est connecté au réseau d'informatique de gestion (IT) : celui-ci peut être victime d'attaques et héberger des programmes malveillants qui tentent dans un second temps de corrompre le réseau industriel, ou il peut même laisser passer directement des attaques ;

– dans un réseau industriel, il existe parfois des connections directes à Internet, plus ou moins officielles et parfois temporaires, pour la maintenance ou la configuration, et celles-ci représentent une réelle vulnérabilité.

Ajoutons à cela qu'avec les besoins croissants de remontée des données vers le SI ou le *Cloud*, avec les systèmes de mises à jour depuis un site du constructeur et avec la maintenance à distance, l'isolation des systèmes industriels est de plus en plus illusoire.

L'enjeu est faible.

Une idée très répandue est que le risque est faible lorsque l'appareil de production ne met pas en œuvre des machines ou des procédés dangereux.

Pour ce type d'installations, il est clair que les dommages pour l'environnement et les personnes seront d'une ampleur limitée. Cependant, pour l'entreprise, l'impact peut être énorme puisqu'une attaque peut se traduire par un arrêt de la production pendant une période longue, une sous-qualité des produits fabriqués, voire une destruction de l'appareil de production. Il faut analyser les conséquences économiques et mener une analyse coût/bénéfice pour déterminer le niveau des mesures de cybersécurité qui doivent être prises.

Les postes sont équipés d'antivirus et il existe un pare-feu, nous sommes protégés.

Utiliser un antivirus est une mesure élémentaire à prendre. Il permet la protection des postes de travail informatique, fonctionnant sous Windows ou macOS. Cependant, dans un système industriel, il existe de nombreux équipements fonctionnant avec un système d'exploitation temps réel ou un système Linux embarqué, voire un système propriétaire. Pour ces systèmes, il n'existe pas forcément d'antivirus et ils sont donc vulnérables.

Ajoutons qu'un des problèmes des antivirus pour les postes d'informatique industrielle est qu'ils ne sont pas toujours mis à jour.

Les limites des pare-feu sont aussi bien connues : la première est que les règles de filtrage ne sont pas toujours bien configurées, la seconde, que même si les flux sont limités, cela n'empêche pas le passage de toutes les attaques. Comme cela est détaillé dans le chapitre 4, le système de gestion de l'énergie électrique attaqué en Ukraine en 2015 comportait des pare-feu qui n'ont rien n'empêché.

Nous utilisons un VPN, donc pas de problèmes.

Une autre idée très répandue est que l'utilisation d'un VPN permet une protection efficace. Cette idée est elle aussi erronée pour deux raisons principales :

– la première est qu'un nombre important de VPN emploient des technologies considérées comme dépassées et sont donc vulnérables. Un étude de 2016 (High-Tech Bridge Security Research 2016) a montré que 77% des VPN testés utilisent toujours un protocole basé sur SSLv3, créé en 1996, voire même sur SSLv2, alors que la plupart des standards comme le PCI DSS ou NIST SP 800-52 (voir chapitre 6) prohibent son usage ;

– la seconde est que, même avec un VPN bien configuré, si l'un des postes connectés à ces VPN a été compromis, il peut compromettre le reste du réseau, et ceci d'autant plus facilement que les données transportées sont chiffrées et donc difficiles à filtrer.

La SSI coûte cher et génère beaucoup de contraintes limitant l'efficacité.

Une idée communément répandue est que la SSI coûte cher et impose un grand nombre de contraintes pour l'exploitation, qui sont incompatibles avec celles de l'informatique industrielle.

Ces contraintes apparaissent d'autant plus importantes qu'un ICS utilise des équipements très hétérogènes, et que ses utilisateurs apprécient une certaine souplesse pour l'exploitation. Par exemple, l'utilisation de terminaux nomades se répand de plus en plus, car elle est très utile pour un pilotage localisé des systèmes.

En réalité, la SSI des systèmes industriels doit être adaptée aux enjeux, et il est important de réaliser une analyse des risques et de mettre en regard l'importance de ceux-ci et le coût des mesures pour les réduire et les contraintes qu'elles imposent. Cela dit, la sécurité est souvent considérée comme une source de dépenses qu'il est difficile de justifier par un retour sur investissement (ROI). Il est plus pertinent de la mesurer par rapport à une perte potentielle, par exemple sur la quantité de production, si le système est indisponible, ou sur le coût de remise en état, s'il est détruit.

Quant aux contraintes d'exploitation, il est important de mettre en place des solutions en concertation avec les utilisateurs et en prenant en compte la réalité du terrain. Il faut accompagner les nouveaux modes d'exploitation et ne pas chercher à limiter de façon excessive les possibilités des utilisateurs.

I.4. Vulnérabilité des ICS

Les systèmes informatiques sont vulnérables aux cyber-attaques et aux agressions physiques. Les ICS, qui, comme nous l'avons vu, sont connectés de façon directe ou non à Internet, le sont aussi.

Pour des raisons historiques, et à cause des différences de culture, les systèmes de commande industriels sont encore plus vulnérables que les systèmes informatiques classiques.

De façon générale, une installation industrielle est réalisée pour une période relativement longue. Des systèmes de plus de dix ans se rencontrent couramment. Par ailleurs, l'objectif essentiel est de faire fonctionner en continu le système de production, et tout ce qui nécessite ou peut générer un arrêt est évité. De plus, pour des raisons de comptabilité, les protocoles utilisés sont de conception assez ancienne et ils sont peu, voire pas du tout, sécurisés.

Mais les ICS sont devenus au fil du temps fortement connectés. Tout d'abord, les processus de production et de gestion de la chaîne logistique sont intégrés avec les principaux logiciels de gestion, et les données de production sont utilisées dans les applications de gestion de l'entreprise. Par ailleurs, de façon à permettre une meilleure réactivité, la maintenance et la surveillance sont réalisées à distance. Enfin, certaines installations sont isolées et supervisées à distance (station de traitement d'eau, distribution d'énergie, etc.).

Les systèmes industriels ont aussi la spécificité d'être très hétérogènes et construits à partir d'éléments génériques (COTS, *Commercial off-the-shelf*), choisis avant tout pour leurs fonctionnalités et non pour leur sécurisation. Les produits utilisés sont peu sécurisés, pas toujours complètement testés. La mise à jour des logiciels, des systèmes

d'exploitation ou du *firmware* est difficile et n'est pas toujours réalisée régulièrement. Enfin, au niveau des équipements, la gestion de l'authentification est difficile, et les mots de passe par défaut ne sont pas toujours changés.

Les utilisateurs n'ont pas toujours conscience de la vulnérabilité des ICS : beaucoup de ports physiques (USB, RJ45) sont peu protégés, et il peut être facile de s'y connecter. Il existe même parfois des connections « pirates » vers Internet, qui ont été créés pour des raisons liées à la maintenance ou à l'accès à distance.

En outre, les ICS sont utilisés dans le monde de la production, où la culture est souvent basée sur des principes comme produire d'abord et ne pas prendre le risque de modifier quelque chose qui fonctionne. Cela entraîne par exemple que les mises à jour ne sont pas systématiques et que la gestion de l'authentification n'est pas aussi rigoureuse que celle du monde IT avec des mots de passe qui peuvent être partagés.

Enfin, dans de nombreux cas, il n'existe aucune politique de management de la sécurité des ICS : la gestion des sous-traitants et intervenants ne fait pas l'objet de mesures spécifiques, et il n'existe pas de politique de gestion des droits d'accès des utilisateurs définissant leurs possibilités d'action et interdisant les accès des employés n'appartenant plus à l'entreprise.

I.5. Cybersécurité et sécurité fonctionnelle

Les installations industrielles et les systèmes cyber-physiques peuvent être sujets à des défaillances ou à des erreurs de manipulation qui peuvent conduire à des fonctionnements dommageables ou à des pannes. L'étude de ces risques est l'objet de la sûreté de fonctionnement ou de la sécurité fonctionnelle.

Les sources de dysfonctionnement prises en compte sont nombreuses : elles peuvent être techniques, humaines ou organisationnelles. Dans les origines techniques, une catégorie fait l'objet d'une attention particulière, il s'agit des composants électriques, électroniques ou électroniques programmables. La norme 61508 (chapitre 8) décrit la démarche pour l'analyse des risques liés à leurs défaillances potentielles. L'idée est de caractériser l'installation par un niveau de probabilité de défaillance sur une période de temps donnée. En la couplant à une analyse des impacts en cas de dysfonctionnements, il est possible d'évaluer le niveau de risque d'une installation ou d'un système et de satisfaire des objectifs donnés.

La sécurité fonctionnelle, telle que définie par l'IEC 61508, n'inclut pas la sécurité des systèmes d'information, qui n'était pas un risque identifié comme tel en 2002, à la date d'écriture de la norme, et même les dernières mises à jour ne font que commencer à l'évoquer. On notera que la SSI n'est pas non plus prise en compte explicitement

dans les analyses de risque des installations dangereuses (ICPE) appelées « études de danger ».

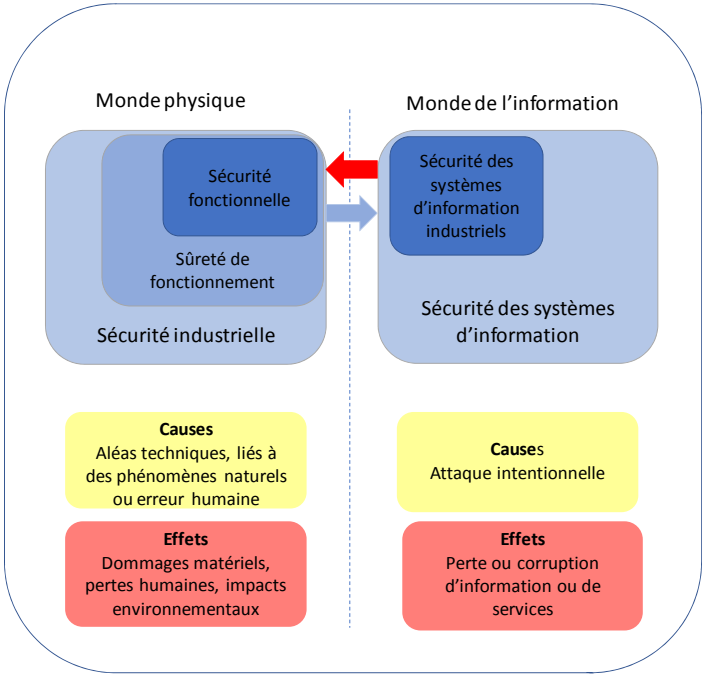

Figure I.1. *Relations entre sécurité fonctionnelle et sécurité des systèmes d'information*

La sécurité de l'information et la sûreté de fonctionnement des systèmes physiques sont gérées par des approches différentes :

– d'un côté, le processus de management des risques des systèmes d'information est décrit dans les standards de la famille 27000 (chapitre 6). Les méthodes d'analyse de risque utilisées (chapitre 9) sont par exemple les méthodes EBIOS ou OCTAVE ;

– de l'autre, on trouve les méthodes d'analyse des risques des processus industriels comme l'APR, HAZOP, FMEA ou LOPA (chapitre 8) et la norme 61508.

Pour la sécurité des systèmes d'information (IT), l'impact du monde physique sur le système d'information, comme par exemple une panne électrique ou une surchauffe, est pris en compte. En revanche, l'influence inverse (flèche rouge) n'est pas considérée pour ces systèmes, puisqu'ils ne manipulent que de l'information.

Dans le cas des systèmes cyber-physiques comme les systèmes industriels automatisés ou les infrastructures critiques, cette influence existe et peut avoir des conséquences dommageables très importantes. Pour ces systèmes, il apparaît que les deux aspects ne sont pas indépendants et doivent être traités de façon coordonnée.

En effet, même si les causes des événements redoutés sont différentes, les conséquences et dommages produits sont pour la plupart communs : atteintes aux biens, aux personnes et à l'environnement par un procédé dont on perd le contrôle. Par exemple, un dysfonctionnement d'un automate de sécurité pourra trouver ses causes à la fois du côté de la sûreté de fonctionnement et de la SSI. Dans tous les cas, les conséquences seront des dommages pour l'installation.

La norme IEC 62443 (chapitre 7) vise à transcrire un certain nombre de concepts de la sécurité fonctionnelle, notamment les niveaux SIL, pour la cybersécurité, de façon à aligner les approches. Pour l'analyse des risques, des approches unifiées commencent à être proposées (chapitre 9).

I.6. Évolution de la perception de la cybersécurité

L'évolution technologique qui a permis la mise en œuvre de systèmes automatisés à grande échelle est l'invention du microprocesseur, en 1971, par Intel. On a alors assisté au développement de l'informatique personnelle et, quelques années plus tard, à celui des systèmes de contrôle industriel. Ces systèmes ont d'abord été connectés par des liaisons filaires point à point, puis dans les années 1990 on a assisté à la généralisation de la communication par réseau Ethernet avec le protocole TCP/IP. Les principaux protocoles industriels ont été « encapsulés » et ont permis le développement des systèmes de contrôles industriels comme nous les connaissons.

À l'époque, le problème principal était la performance, et personne n'imaginait que la sécurité prendrait les proportions qu'elle a aujourd'hui.

Les premiers virus informatiques datent de la fin des années 1980. Le virus Brain qui infecte dans le secteur de *boot* des PC a été écrit en 1986 par les frères Basit et Amjad Farooq Alvi (Brain virus n.d.). Il est reconnu comme le premier virus sur MS-DOS. En 1998, le vers Morris se propageant sur Internet a été écrit par R. Tappan. C'est en 1990 qu'est apparu l'un des premiers antivirus (Norton Antivirus). Les progrès des virus furent rapides, car c'est aussi en 1990 que le premier virus polymorphique a fait son apparition (Chamelon, écrit par R. Burger).

Dès le milieu des années 2000, la question de la vulnérabilité des ICS a été posée (Abshier 2004 ; Wooldridge 2005). En 2008, le projet Aurora (Meserve 2007), une expérimentation supervisée par l'Idaho National Laboratory, a prouvé la possibilité de détruire un générateur d'énergie grâce à une cyber-attaque.

En 2010, une étude sur les systèmes de production d'énergie électrique réalisée par Red Tiger, à la demande du US Department of Homeland Security (Pollet 2010), a montré que la sécurité informatique de ces systèmes n'était pas au niveau de celle du monde IT. Par exemple, de nombreuses failles rendues publiques n'étaient pas corrigées et laissaient donc ces systèmes vulnérables.

Depuis 2010, divers réglementations et projets de loi sont apparus dans plusieurs pays. Citons :

– le *National Cybersecurity and Critical Infrastructure Protection Act* of 2013, US ;

– l'article 22 de la Loi de programmation militaire en 2013, en France ;

– le *IT Security Act* en 2016, en Allemagne ;

– la directive NIS en Europe en 2016.

Par ailleurs, depuis les années 2010, un certain nombre de guides et ouvrages ont été publiés sur ce sujet (Macaulay et Singer 2012 ; Knapp et Thomas 2015), et des outils méthodologiques ont été proposés pour améliorer la SSI des installations industrielles (ANSSI 2012a ; Stouffer *et al.* 2015).

La perception du risque est néanmoins restée limitée et les démarches ont tardé à se mettre en place. Cependant, avec des attaques de plus en plus courantes et médiatisées, la prise en compte de la cybersécurité dans les nouveaux projets apparaît progressivement, et devient incontournable avec les obligations réglementaires de 2018 (chapitre 6).

I.7. Organisation de l'ouvrage

Cet ouvrage est organisé de la façon suivante[1] :

– le chapitre 1 présente les différents éléments d'un système de contrôle industrie, SCADA et IIoT ;

– le chapitre 2 décrit l'architecture de ces systèmes et les différentes caractéristiques des réseaux utilisés, dans les SCADA ou les systèmes IIoT ;

– le chapitre 3 présente les notions de base en sécurité de l'information et en management des risques ;

– les chapitres 4 et 5 détaillent le principe des attaques et l'analyse des vulnérabilités des ICS ;

1. Des informations complémentaires peuvent être trouvées à l'adresse suivante : http://industrialcybersecurity.io/.

– les chapitres 6 et 7 présentent les normes et la réglementation, un chapitre étant dédié à la norme IEC 62443, qui est la norme de référence ;

– le chapitre 8 présente les notions utiles de sûreté de fonctionnement ;

– le chapitre 9 s'intéresse aux méthodes d'analyse de risque : la méthode EBIOS et les méthodes plus spécifiques pour les systèmes industriels : Cyber APR, Cyber HAZOP et cyber-nœud-papillon ;

– le chapitre 10 présente des méthodes et outils pour sécuriser un ICS : inventaire de l'installation, sécurisation de l'architecture, dispositifs techniques comme les systèmes de détection d'intrusion, les *data-diodes* et composants IIoT sécurisés. Des notions de cryptographie sont données dans l'annexe 1 et la *blockchain* pour l'IoT est introduite dans l'annexe 2 ;

– le chapitre 11 propose une démarche complète pour la sécurisation. Elle s'appuie sur les standards et méthodes exposés précédemment, et est présentée dans une version simplifiée et une version détaillée.