Focus normalisation

PASSAGE À L'INDUSTRIE 4.0: LES ASPECTS LIÉS À LA SÉCURITÉ

Industrie 4.0 signifie interconnexion totale entre hommes, machines et installations. Du fait de l'interaction entre ces partenaires, la sécurité fonctionnelle (*functional safety*, par exemple l'arrêt d'une machine en cas de passage d'une barrière lumineuse) n'est pas le seul aspect pertinent pour la protection des individus. La sécurité de l'information (*'security'*, par exemple la protection de la programmation d'un robot contre des manipulations extérieures) joue un rôle tout aussi important.

ASPECTS OF SAFETY AND SECURITY IN THE EMERGENCE OF INDUSTRY 4.0 –
Industry 4.0 stands for the networking of human beings, machines and installations. Owing to the interaction between these communication partners, it is not sufficient for functional safety (such as the halting of a machine when a light barrier is penetrated) to be considered in order for human beings to be protected. Information security (such as the protection of a robot's programming against manipulation over the network) is equally important.

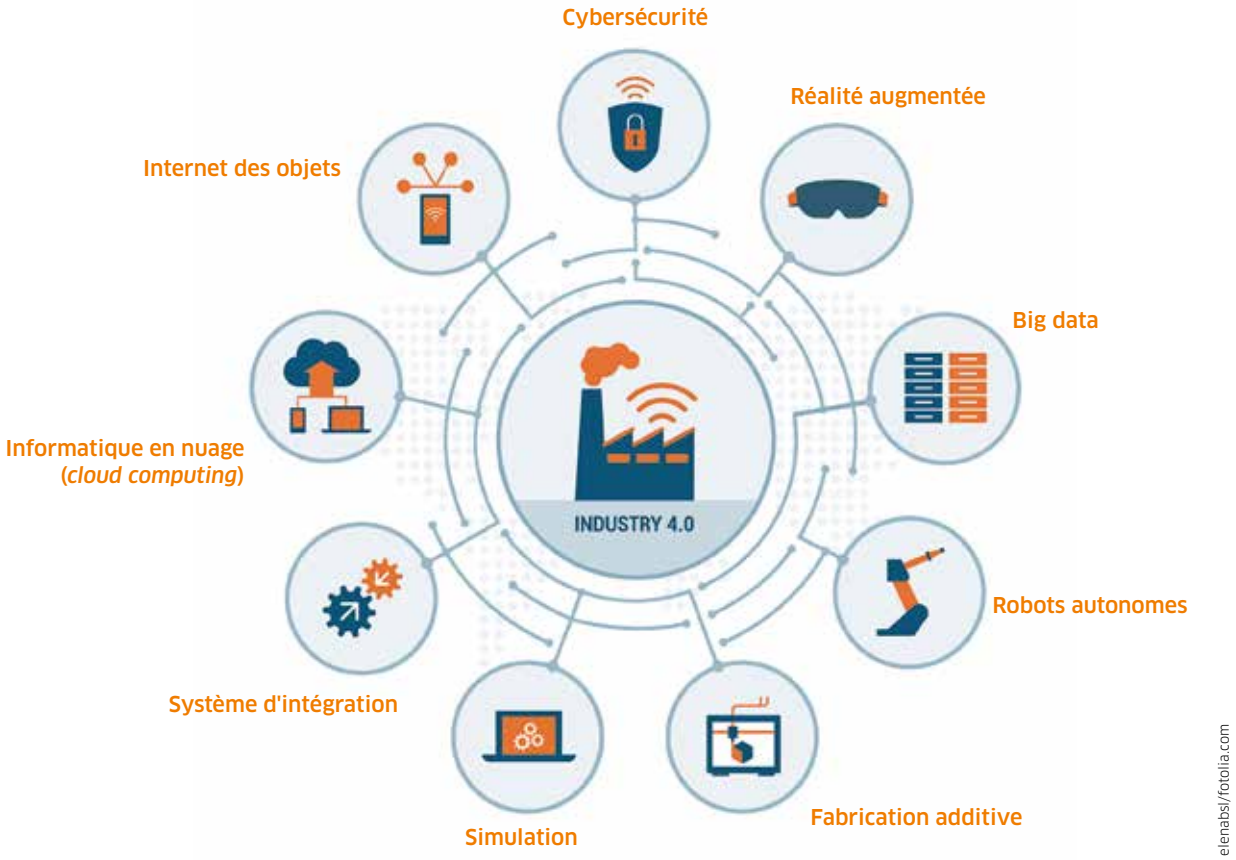
SEBASTIAN KORFMACHER, CORRADO MATTIUZZO
chargés de mission, secrétariat de la KAN

Le rapport entre sécurité fonctionnelle et sécurité de l'information est décrit dans la règle d'application VDE-AR-E 2802-10-1:2017-04[1]. Elle préconise de faire la distinction entre ces deux formes de sécurité pour détecter tout conflit d'intérêt lors de l'évaluation des risques.
Lors de l'atelier « Functional safety & cybersecurity » du Comité européen de normalisation (CEN), les experts ont estimé qu'il était improbable qu'une attaque provenant de tiers, par exemple sous forme de piratage, cause des préjudices humains ou environnementaux[2], les pirates informatiques favorisant surtout les cibles potentiellement lucratives. Ceci n'exclut toutefois pas des dommages causés involontairement à l'homme ou à l'environnement. À une époque marquée par le terrorisme, il n'est en outre pas exclu que l'homme et l'environnement constituent aussi une cible primaire.

Les aspects juridiques

La mise en œuvre de l'Industrie 4.0 dépend essentiellement de la manière dont ce concept sera accepté par les utilisateurs. Ceux-ci attendent que les produits qu'ils utilisent et les opérations interconnectées dans lesquelles ils sont intégrés soient sûrs. En cas d'accès non autorisé par un tiers, la question importante pour l'utilisateur est de savoir qui doit en assumer la responsabilité. Actuellement, les accès non autorisés soulèvent toutefois encore des questions de principe relevant du droit pénal et du droit de la responsabilité civile[3,4]. Déclenchant la présomption de conformité et décrivant les règles de l'art, les normes techniques peuvent avoir un rôle très important à jouer. Pour la KAN (Commission pour la sécurité et santé au travail et la normalisation, *Kommission Arbeitsschutz und Normung*), des questions relevant du droit administratif s'avèrent donc également intéressantes:

- Jusqu'où s'étend la responsabilité du distributeur au titre de la loi allemande sur la sécurité des produits (ProdSG) et des réglementations européennes « Marché intérieur »? Celles-ci couvrent uniquement l'usage normal et tout mauvais usage (raisonnablement) prévisible de la part de l'utilisateur, mais pas un usage abusif résultant d'un acte criminel.
- Avons-nous donc besoin de réglementations supplémentaires? Ou bien pourrait-on généraliser les attaques criminelles éventuelles provenant de l'extérieur comme étant une sorte de « réseau contaminé » et les considérer comme étant des conditions ambiantes prévisibles, comme le seraient les facteurs climatiques ou les pannes sur le réseau électrique? Ceci serait alors couvert par la législation sur le marché intérieur.
- Une norme harmonisée peut-elle être encore considérée comme complète si elle ne traite pas (de manière satisfaisante) les attaques de tiers provenant de l'extérieur sur un produit connecté? Les organismes de surveillance du marché pourraient-ils agir à l'encontre d'un produit qui ne



← FIGURE 1
Le concept d'industrie 4.0 ou industrie du futur.

serait pas suffisamment sécurisé contre les attaques extérieures ?

Déjà en juillet 2014, le Cenelec (Comité européen de normalisation en électronique et en électrotechnique) avait publié le Guide 32[5], actuellement en cours de révision. Il y est demandé que des questions relatives à la sécurité des informations soient prises en compte dans les normes fondées sur la directive Basse tension. En février 2017, l'ISO/TC 199 « Sécurité des machines » a accepté un nouveau projet préliminaire intitulé « Guidance and consideration of related security aspects ». Le rapport technique ISO/TR 22100-4, sur lequel il débouchera, sera un guide décrivant la relation entre l'ISO 12100 « Sécurité des machines » et les aspects de la sécurité de l'information applicables aux machines.

Resserrer l'interaction entre techniciens et informaticiens

De multiples activités relatives à la normalisation dans le domaine de la sécurité fonctionnelle et de la sécurité de l'information sont actuellement en cours au sein du CEN/Cenelec et de l'ISO/CEI, toutefois jusqu'à présent dans des univers distincts. Mais ce ne sont pas seulement les spécialistes en matière de sécurité des produits qui doivent prendre en compte des aspects concernant la sécurité de l'information. Et, à l'inverse, les experts en technique de l'information devront, à l'avenir, être davantage sensibilisés aux aspects de la sécurité fonctionnelle.

Il serait bon que les organismes de normalisation travaillent ensemble à imbriquer plus étroitement les uns dans les autres les domaines de la « sécurité fonctionnelle » et de la « sécurité de l'information », afin de concilier ces deux approches traditionnellement différentes. C'est le seul moyen de prendre en compte à un stade précoce et avec succès les aspects pertinents pour la SST. Il conviendra, en outre, de régler rapidement et de manière transparente un certain nombre d'aspects juridiques si l'on veut que le passage à l'Industrie 4.0 soit une réussite. ●

1. La relation entre sécurité fonctionnelle et sécurité de l'information, à l'exemple de l'automatisation industrielle – Partie 1 : principes.

2. www.kan.de/service/wir-berichten-fuer-sie/detailansicht/workshop-functional-safety-cybersecurity-bei-cen-am-1632017 (en allemand).

3. Rockstroh/Kunkel, IT-Sicherheit in Produktionsumgebungen, MMR 2/2017 (en allemand).

4. Bräutigam/Klindt: Industrie 4.0, das Internet der Dinge und das Recht, NJW 2015, 1137 (en allemand).

5. Guide Cenelec 32 : 2014-07 « Lignes directrices pour l'appréciation et la réduction du risque lié à la sécurité pour le matériel basse tension » ftp://ftp.cencenelec.eu/CENELEC/Guides/CLC/32_CENELECGuide32-FR.pdf

KANBrief

Cet article est issu du bulletin d'information KANBrief 2/17 (consultable sur www.kan.de/fr) de la *Kommission Arbeitsschutz und Normung (KAN).*
The English version of this article is accessible at www.kan.de/en