Focus normalisation

DOSSIER DE SÉCURITÉ POUR LES MACHINES ET ÉQUIPEMENTS CONNECTÉS DANS LES USINES FLEXIBLES

Dans les usines flexibles de l'industrie du futur (4.0) aussi, il faut garantir la sécurité des salariés. Du fait du degré élevé de connectivité, il faut se pencher non seulement sur la sécurité fonctionnelle, mais aussi, dans une plus large mesure, sur la sécurité contre les attaques venues de l'extérieur, et sur les interactions entre ces deux aspects. Il faut aussi examiner dans quelle mesure les méthodes actuelles d'évaluation des risques sont encore adaptées aux futures machines flexibles.

SAFETY RECORD FOR CONNECTED MACHINES AND EQUIPMENT IN FLEXIBLE FACTORIES – ***In flexible factories of industry 4.0, the safety of employees must also be guaranteed. Because of the high degree of connectivity, it is necessary to look into not only functional safety, but also, to a greater extent, safety against external attacks, and the interactions between these two aspects. It must also be determined the extent to which current risk assessment methods are still suitable for flexible machines.***

BJÖRN KASPER, SILVIA VOCK, STEFAN VOSS, Institut fédéral de la sécurité et santé au travail (BAuA)
info-zentrum@baua.bund.de

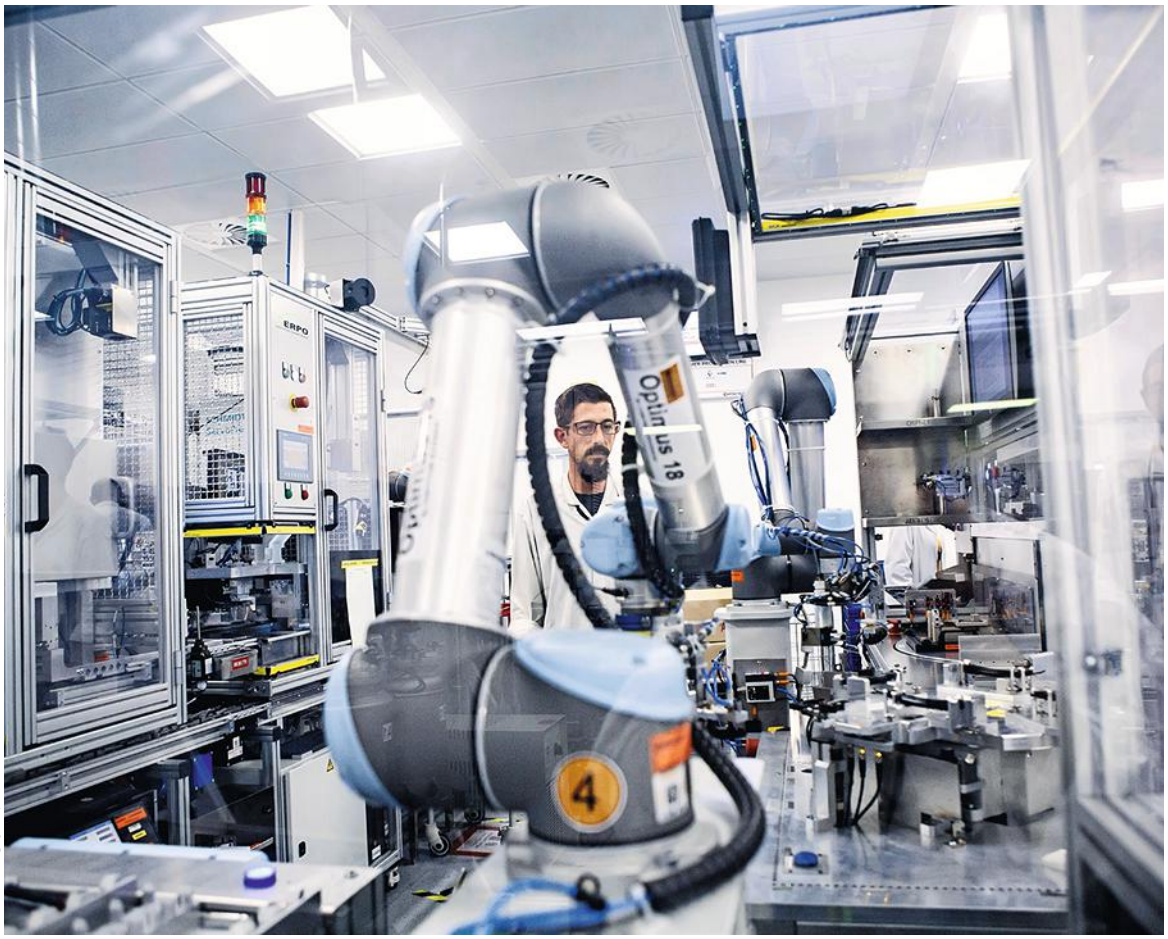
On s'attend à l'avenir à des marchés nettement plus dynamiques et volatils, de sorte que la flexibilité limitée des machines et équipements de production actuels ne serait plus rentable. C'est pourquoi, dans le contexte de l'Industrie 4.0, on discute de la possibilité d'obtenir des machines et équipements extrêmement flexibles. On obtiendrait cette flexibilité grâce à la capacité des modules de production de se recombiner en îlots de production, de s'interconnecter et de se configurer automatiquement, et ce en fonction des commandes. Les modules individuels (par exemple, les capteurs intelligents) sont pour cela interconnectés de manière flexible et le plus souvent, par communication radio.

La technique de sécurité de l'Industrie 4.0

Dans l'Industrie 4.0, les modules techniques essentiels sont des « systèmes cyberphysiques » (CPS) intelligents interconnectés. Comme toute machine ou tout équipement classique, les CPS possèdent des fonctionnalités d'opération qui servent à la production des produits et marchandises, et d'autres qui servent à la sécurité fonctionnelle.
En cas de transmission de signaux de sécurité sur de longues distances ou, dans le cas des concepts d'Industrie 4.0, par le biais de réseaux basés sur la communication radio, il faut en outre prendre des mesures appropriées pour empêcher toute manipulation. Du fait de l'interconnexion, toute faille de sécurité (au sens de sûreté) face aux attaques *(security)* ayant pour conséquence une manipulation des organes de commande de la machine, peut entraîner la défaillance des fonctionnalités de sécurité *(safety)*, entraînant ainsi un danger pour les employés[1]. Jusqu'à présent, la méthode veut que ces deux aspects de la sécurité soient considérés individuellement, l'évaluation des risques s'effectuant séparément pour les aspects de « *safety* » et de « *security* ». Or, ces deux aspects pouvant s'influencer mutuellement, ils doivent, de l'avis des préventeurs, être considérés ensemble. C'est l'objet de recherches menées actuellement par le BAuA (Institut fédéral de la sécurité et de la santé au travail).

La validation d'usines flexibles

L'analyse des CPS en termes de sécurité impose des exigences nouvelles à la méthodologie de l'analyse des risques. Il faut notamment examiner les aspects structurels (hétérogénéité, interopérabilité, intensité logicielle, mise en réseau, etc.) et les aspects dynamiques (évolution en fonction du temps,



© Vincent Nguyen pour l'INRS/2019

reconfiguration dynamique, décisions autonomes, etc.). De plus, les standards de sécurité actuels présupposent qu'un système est totalement développé et configuré avant la réception et validation de son système de sécurité (voir en particulier la norme IEC 61508-3:2010[2]).

Dans le cadre d'un projet actuel, le BAuA s'est fixé pour objectif d'évaluer si les méthodes classiques et modernes d'analyse de risques sont applicables aux systèmes flexibles de production. Lors d'une étape ultérieure, il est prévu de tester dans la pratique des méthodes appropriées sur des modèles de systèmes numériques d'installations de production ou de fabrication interconnectées.

Apprentissage automatique

Les systèmes flexibles de fabrication peuvent aussi contenir des algorithmes de l'apprentissage automatique *(machine learning – ML)*. Il faut alors d'abord distinguer la fonction dans laquelle est utilisé l'algorithme de ML. Il peut s'agir :

- d'une fonction de commande pour la gestion adaptative ou l'optimisation des processus ;
- d'une partie d'une fonction de sécurité destinée à accroître la sécurité du système ;
- de l'utilisation (encore visionnaire aujourd'hui) de l'apprentissage automatique pour l'analyse des risques de systèmes complexes et flexibles pendant leur durée de vie.

Les aspects critiques en termes de sécurité doivent être examinés en détail pour chacun des trois scénarios d'utilisation mentionnés, qui peuvent partiellement se chevaucher. Le BAuA travaille actuellement sur la question de savoir comment on pourra, à l'avenir, décrire dans une analyse quantitative des risques l'imprévisibilité des décisions induites par les algorithmes ML par rapport aux composants logiciels classiques.

La normalisation peut apporter une contribution précieuse pour ces questions encore sans réponses et concrétiser l'approche méthodologique des différentes disciplines. Une interaction, à un stade précoce, entre la recherche et le développement, la législation et la normalisation est nécessaire pour pouvoir exploiter pleinement le potentiel de création de valeur des technologies numériques. ●

1. Lire à ce sujet : LAMY P. – Sécurité des machines : le « risque cyber » comme risque émergent ? Hygiène et sécurité du travail, *septembre 2019, 256, pp. 72-79. Accessible sur : www.hst.fr (ndlr).*

2. Norme IEC 61508-3:2010 – Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité. Partie 3 : exigences concernant les logiciels. Afnor, janvier 2011.

KANBrief

Cet article est issu du Bulletin d'information *KANBrief* n° 4/19 (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