Focus normalisation

DE LA VULNÉRABILITÉ À LA NORME : L'UE REDÉFINIT LES RÈGLES SUR LA CYBERSÉCURITÉ

JONAS STEIN
Institut pour la sécurité et la santé au travail de la DGUV (IFA)

ARNE SONNENBURG
Institut fédéral de la sécurité et de la santé au travail (BAuA)

Les failles de sécurité dans les logiciels de produits passent souvent inaperçues, mais les nouvelles réglementations de l'Union européenne (UE) devraient changer la donne. Le règlement sur la cyberrésilience et le règlement Machines définissent des exigences claires en matière de protection des systèmes de commande contre toute corruption accidentelle ou intentionnelle. C'est maintenant à la normalisation qu'il appartient, en tenant compte du futur guide pour le règlement Machines, de créer les fondements d'une technique sûre et fiable sur le marché européen.

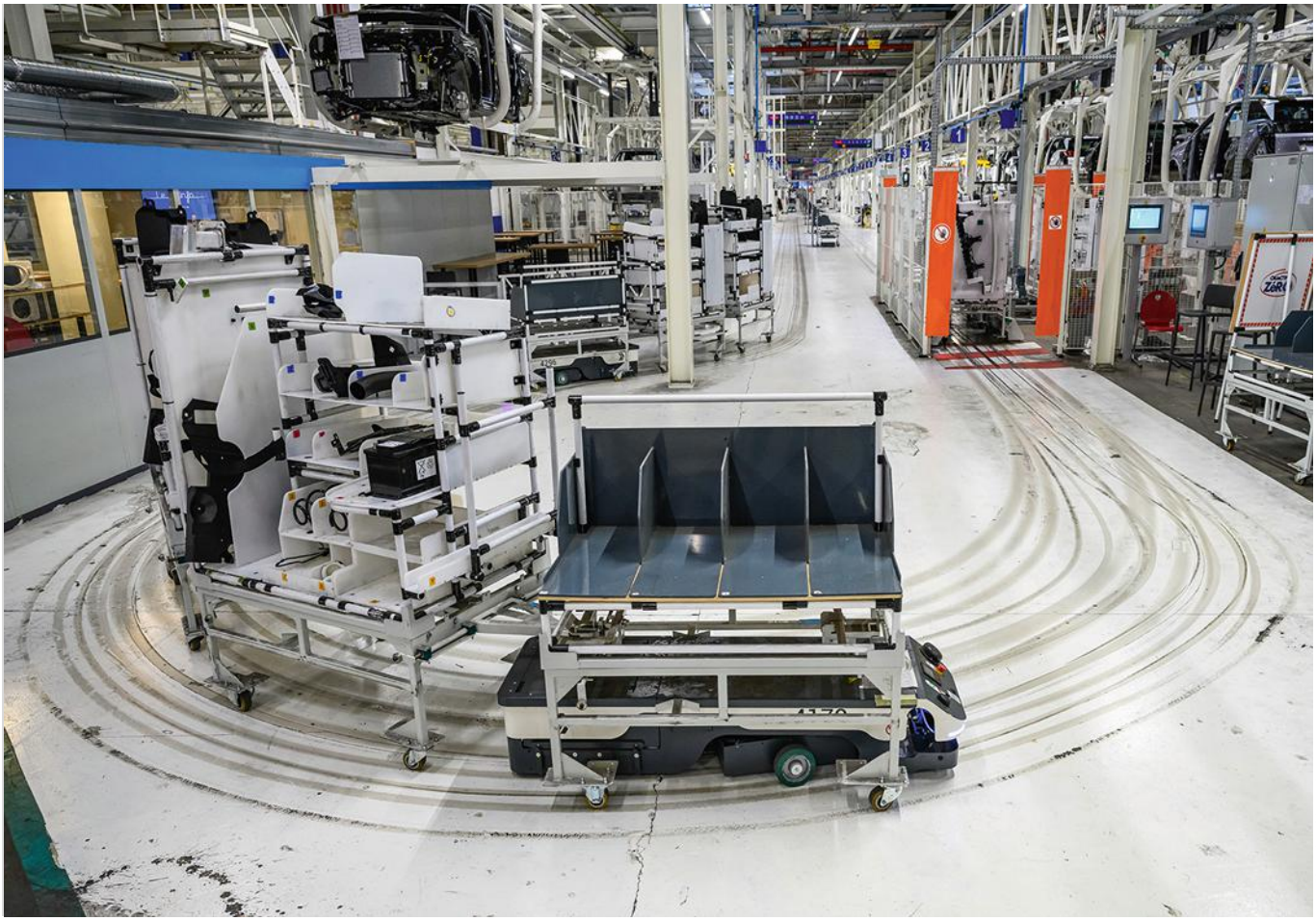
FROM VULNERABILITY TO STANDARDISATION: THE EU REDEFINES THE RULES ON CYBERSECURITY – *Security breaches in product-related software often go unseen, but the new EU regulations should change things. The Cyber Resilience Act (CRA) and Machinery regulation define clear requirements to protect control systems against accidental or intentional corruption. Standardisation, based on the future guide for the application of the new Machinery regulation, will now lay the foundations for safe and reliable technology on the European market.*

KAN Brief

Cet article est issu du bulletin d'information *KAN-Brief* n° 2/25 (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

Chaque année, les chercheurs spécialisés dans la cybersécurité signalent des milliers de failles informatiques dans des produits, allant des portes dérobées dans les systèmes de commande industriels jusqu'aux commandes radio qui font aveuglément confiance à n'importe quel émetteur. Nombreux sont les utilisateurs qui ne sont même pas conscients de ces failles de sécurité. Et jusqu'à présent, rien n'incitait vraiment les fabricants à investir dans davantage de ressources pour remédier à ces failles. Constatant que le marché ne parvenait pas à résoudre le problème, la Commission a réagi en adoptant un vaste ensemble réglementaire.

- **Le règlement sur la cybersécurité**[1] définit le mandat de l'Agence de l'Union européenne pour la cybersécurité (ENISA). L'agence a pour mission d'améliorer la communication sur les vulnérabilités entre les lanceurs d'alerte, les fabricants, les exploitants et les autorités en Europe. Elle a, à cet effet, mis en place une base de données européenne.
- **La directive NIS 2**[2] définit, pour des entités et entreprises essentielles et importantes, des exigences auxquelles doit répondre la sécurité de leurs réseaux et systèmes d'information (NIS), ainsi que des règles contraignantes pour la notification d'incidents. À l'heure actuelle, de nombreux États membres sont en retard dans la transposition de cette directive au niveau national.
- **Le règlement sur la cyberrésilience (CRA)**[3] stipule les obligations des fabricants en matière de l'évitement et de la gestion des vulnérabilités, qui doivent notamment mettre en place un point de contact d'urgence joignable en permanence. Concernant la communication, plusieurs spécifications librement accessibles se sont établies.



© Gaël Kerbaol/INRS/2023

Acheminement de pièces détachées aux postes de travail à l'aide d'AGV (véhicules à guidage automatique) dans l'industrie automobile.

Elles définissent notamment des standards uniformes permettant de décrire le niveau de criticité des failles de sécurité, ainsi que les formats de données à utiliser pour les décrire :

La spécification RFC 9116 de *l'Internet engineering task force (IETF)* décrit comment les entreprises peuvent enregistrer, dans un simple fichier texte accessible dans le monde entier, les contacts d'urgence en cas de faille de sécurité. Le CRA ne stipule pas de format concret pour la nomenclature des logiciels contenus dans un produit *(Software bill of materials – SBOM),* liste que le fabricant doit créer. Les formats qui s'imposent particulièrement aujourd'hui sont le Cyclone DX et la norme ouverte IEC ISO 5692 (*System package data exchange).*

La SBOM permet de signaler automatiquement les produits qui contiennent un logiciel présentant une faille de sécurité connue. Pour les recommandations d'action lisibles par machine exigées par le CRA, c'est le *Common security advisory framework (CSAF)* IEC ISO 20153 qui s'est imposé.

Le poids du CRA se reflète aussi dans de nouveaux projets de normalisation : rien qu'en 2025, quelque 40 propositions de nouvelles normes seront soumises au vote en vue d'être harmonisées conformément au CRA.

Un guide de l'UE concrétise les exigences de sécurité du règlement Machines

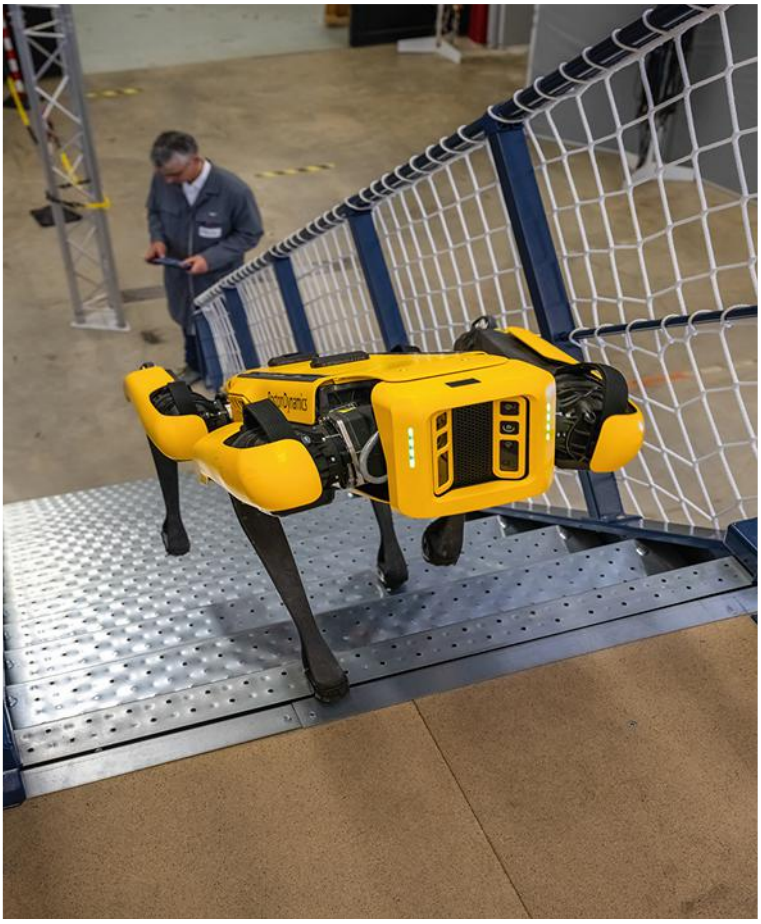
Le règlement Machines[4], qui s'adresse aux fabricants, stipule à l'annexe III, paragraphes 1.1.9 et 1.2.1, qu'une protection adéquate contre la corruption accidentelle ou intentionnelle doit être prévue dès la conception, et que la preuve d'une intervention légitime ou illégitime dans les logiciels ou le matériel informatique doit être recueillie.

La Commission européenne prévoit de publier, au plus tard en janvier 2027, un guide fournissant des explications pratiques des termes employés, et clarifiant les obligations. L'un des cinq groupes de travail élaborant le guide se penchera sur les sections du règlement consacrées à la protection contre la corruption. Le guide est une interprétation du règlement et constituera ainsi un instrument important pour la normalisation.

Les premiers modules pour la protection anti-corruption existent déjà

Au Comité européen de normalisation électrotechnique (Cenelec), les travaux de normalisation sur le projet de norme prEN 50742 ont déjà commencé, norme dans laquelle seront concrétisées

→



© Gaël Kerbaol / INRS / 2024

Étude du comportement d'un robot en laboratoire (INRS).

les exigences du règlement Machines en matière de protection contre la corruption. Cette norme devra, dans la mesure du possible, être compatible avec d'autres normes de sécurité informatique, notamment l'IEC ISO 15408 *(Sécurité de l'information, cybersécurité et protection de la vie privée – Critères communs)*, l'EN 17640 *(Méthode d'évaluation de la cybersécurité pour produits TIC)* ou l'IEC 62443 *(Sécurité informatique des réseaux de communication industriels)*. Elle devra par ailleurs être applicable à une très vaste gamme de produits, allant des visseuses sans fil aux composants de sécurité, en passant par les machines-outils et les ponts élévateurs. Un projet de comité (CD) de la prEN 50742 est attendu pour l'été 2025. Dans l'idéal, la norme devrait être élaborée suffisamment rapidement pour être déjà harmonisée avant l'entrée en application du règlement Machines le 20 janvier 2027.

La révision de la norme EN ISO 12100[5] sur la sécurité des machines reflète, elle aussi, la tendance à prendre en compte non seulement leur sécurité fonctionnelle *(safety)*, mais aussi les questions de la sécurité informatique *(security)*. L'approche la plus prometteuse semble être de recenser, en un premier temps, tous les dangers potentiels dans une analyse classique de risques, analyse dans laquelle seront examinés les phénomènes dangereux que présente la machine sans mesures de protection. L'étape suivante consistera à mettre en œuvre les mesures de protection, qui devront être elles-mêmes protégées contre la corruption pour pouvoir être fiables et efficaces. L'idée directrice est ici d'empêcher la survenue de tout autre nouveau danger dû à une corruption accidentelle ou intentionnelle. Il faut pour cela prendre également en compte la fiabilité d'évaluation des signaux tels qu'une demande d'arrêt d'urgence. L'Institut pour la sécurité et la santé au travail de la DGUV a examiné différents systèmes de commande de machines et a constaté que, dans de nombreux cas, la fonction d'arrêt d'urgence pouvait être corrompue à distance avec une facilité déconcertante. La corruption simultanée de plusieurs machines doit, elle aussi, être prise en compte dans la normalisation. Si par exemple un ascenseur ou une pompe à essence isolés tombent en panne, cela n'est pas très grave, tandis qu'une cyberattaque généralisée contre tous les systèmes dotés d'une commande identique peut avoir des conséquences catastrophiques. Alors qu'il est très improbable que différents systèmes tombent en panne en même temps pour cause d'usure, la corruption généralisée de tous les systèmes identiques constitue un scénario de sécurité d'une gravité extrême.

La première mesure d'urgence que l'on pourrait recommander à toutes les entreprises serait de mettre en place dès aujourd'hui le contact d'urgence décrit dans la spécification RFC 9116. De plus, les éléments essentiels sur la sécurité informatique à intégrer dans les futures normes sont, depuis des décennies, documentés par les milieux scientifiques. Le défi actuel consiste à trouver à ce sujet un consensus sur le risque socialement acceptable, et à élaborer des principes d'essai adaptés à la pratique. ●

1. Voir : https://digital-strategy.ec.europa.eu/fr/policies/cybersecurity-act

2. La directive « Sécurité des réseaux et de l'information » (« NIS », de l'anglais Network and Information System Security*) avait pour but d'assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne (UE). La directive NIS 2 élargit ses objectifs et son périmètre d'application. Elle amène les États membres à renforcer leur coopération en matière de gestion de crise cyber, en donnant notamment un cadre formel au réseau CyCLONe* (Cyber crisis liaison organisation network) *qui rassemble l'ANSSI (France) et ses homologues européens. Voir : https://eur-lex.europa.eu/*

3. Le règlement sur la cyberrésilience renforce les normes de cybersécurité des produits qui contiennent un composant numérique, exigeant des fabricants et des détaillants qu'ils garantissent la cybersécurité tout au long du cycle de vie de leurs produits. Voir : https://eur-lex.europa.eu/

4. Règlement (UE) 2023-1230 sur les machines. Voir : https://eur-lex.europa.eu/

5. Au moment de la publication de l'article, la norme EN ISO 12100 est toujours en cours de révision.