KAN Brief
Kommission Arbeitsschutz und Normung
3/23

LA SÉCURITÉ INFORMATIQUE

Sommaire

© Vector Tradition - stock.adobe.com

Dossier

Thèmes

© berCheck - stock.adobe.com

© momius - stock.adobe.com

Restez toujours informés :

www_kan_de

Kommission Arbeitsschutz und Normung (KAN)

KAN_Arbeitsschutz_Normung

KAN – Kommission Arbeitsschutz und Normung

Benjamin Pfalz
Président de la KAN
Syndicat allemand de la métallurgie (IG Metall)

Cybersécurité : un défi réglementaire et opérationnel

Les entreprises doivent plus que jamais se protéger contre les cyberattaques. Or, il y a longtemps qu'il s'agit aussi d'une question qui concerne la SST. Du fait de l'interaction homme-machine, des équipements de travail télécommandés, des installations de production interconnectées et de l'usage croissant de l'apprentissage automatique, la cybersécurité doit de plus en plus souvent être également prise en compte dans le cadre de l'évaluation des risques au sein de l'entreprise. Les mesures prises pour assurer la sécurité des produits jouent à ce propos un rôle essentiel.

Les organes réglementaires se sont de plus en plus saisis de ces aspects. En Allemagne, pour les dispositifs de mesure, de commande et de régulation, par exemple, la Règle technique pour la sécurité en entreprise (TRBS) 1115 concrétise l'Ordonnance sur la sécurité dans les entreprises à propos de la détermination et la définition des mesures nécessaires de cybersécurité. Parallèlement, le nouveau règlement de l'UE sur les machines et le futur règlement sur l'intelligence artificielle traitent de ce sujet. Le projet de législation sur la cyberrésilience a été lancé pour réglementer la mise sur le marché de produits et de produits intermédiaires comportant des éléments numériques.

La normalisation doit maintenant étayer de manière appropriée le niveau de la réglementation. Le mandat de normalisation relatif au règlement sur l'IA cible clairement le thème de la cybersécurité. Les organismes européens de normalisation y réagissent déjà en examinant les normes existantes et en assignant le traitement du sujet à leurs structures.

La voix de la SST ne doit en aucun cas être absente de ce processus. C'est pourquoi la KAN se saisit du sujet à tous les niveaux, par exemple dans le cadre d'un colloque consacré la normalisation ayant une incidence sur la SST dans le contexte du règlement sur l'IA, colloque qui aura lieu dans le courant de l'année. «

Règlement de l'UE : pour une sécurité accrue dans l'univers des dispositifs et machines connectés

Les fabricants de produits « comportant des éléments numériques » devront à l'avenir garantir la cybersécurité pendant tout leur cycle de vie : c'est ce que prévoit la Commission européenne avec la législation sur la cyberrésilience.

Face aux cyberattaques répétées, impliquant notamment des chevaux de Troie de cryptage, la Commission européenne maintient la pression pour que soient sécurisées les failles informatiques. Après des textes tels que la loi sur la cybersécurité adoptée en 2019, qui établit la base d'un cadre de certification à l'échelle européenne pour la sécurité informatique des appareils, systèmes et services connectés, ou après le récent amendement de la directive sur la sécurité des réseaux et des systèmes d'information (SRI 2), elle a lancé en septembre 2022 une proposition de législation sur la cyberrésilience (Cyber Resilience Act – CRA)[1]. Selon le projet de règlement, les produits « comportant des éléments numériques » – tant les produits matériels que les logiciels – devront à l'avenir présenter moins de vulnérabilités lors de leur mise sur le marché.

Le champ d'application de la proposition est vaste. La Commission veut notamment couvrir « tout produit logiciel ou matériel et ses solutions de traitement de données à distance », y compris leurs composants, même s'ils sont mis sur le marché séparément. L'une des priorités devrait porter sur l'internet des objets ou sur les routeurs à usage privé qui, en raison de nombreuses failles de sécurité intégrées, sont aujourd'hui souvent faciles à pirater. Le règlement ne s'applique pas aux produits « développés exclusivement à des fins de sécurité nationale ou à des fins militaires, ni aux produits spécifiquement conçus pour traiter des informations classifiées. » Les secteurs tels que l'aviation, les dispositifs médicaux ou l'automobile ne sont pas non plus concernés, car ils sont déjà soumis à des exigences qui leur sont propres.

Selon le projet, les fabricants concernés devront à l'avenir répondre à des exigences fondamentales en matière de cybersécurité pour la conception, le développement et le processus de fabrication avant de mettre un appareil sur le marché. Ils doivent être tenus d'en surveiller les vulnérabilités tout au long de son cycle de vie, et d'y remédier par des mises à jour automatiques et gratuites. S'ajoute pour les fabricants l'obligation de signaler à l'ENISA (l'agence de cybersécurité de l'UE) tout incident ayant des répercussions sur la sécurité d'un produit matériel et logiciel, et ce dans un bref délai de 24 heures. D'une manière générale, il est prévu de mettre en place une politique de divulgation coordonnée des vulnérabilités.

Selon le futur règlement, les surfaces d'attaque des appareils concernés doivent être limitées, et l'impact des incidents réduit à son strict minimum. Les produits concernés doivent garantir la confidentialité des données, par exemple par le biais d'un cryptage. Il est prévu de rendre obligatoire la protection de l'intégrité et du traitement des informations et des valeurs mesurées indispensables au fonctionnement d'un article.

En plus de ces exigences de base, la Commission européenne a identifié des domaines à haut risque particulièrement critiques. Elle divise les produits correspondants en deux classes, pour lesquelles il est prévu de mettre en place une procédure de conformité différente. Font notamment partie de la classe I les logiciels de gestion des identités, les navigateurs, les gestionnaires de mots de passe, les logiciels antivirus, les pare-feux, les réseaux privés virtuels (VPN), les systèmes de gestion des réseaux, les systèmes informatiques complets, les interfaces réseau physiques, les routeurs et les puces. S'y ajoutent les systèmes d'exploitation pour smartphones ou pour ordinateurs de bureau, les microprocesseurs et l'internet des objets dans les entreprises qui ne sont pas considérées comme particulièrement sensibles.

Soumise à des risques plus élevés, la classe II comprend les ordinateurs de bureau et appareils mobiles, les systèmes d'exploitation virtualisés et intégrés par exemple dans des machines, les émetteurs de certificats numériques, les microprocesseurs à usage général, les lecteurs de cartes à puce, les composants de détection de robots, et les compteurs intelligents. Doivent également faire partie de cette classe les dispositifs de l'internet des objets, les routeurs et les pare-feux destinés à un usage industriel, ce dernier étant considéré généralement comme « environnement sensible ». Il y a long-

temps en effet que les failles de sécurité informatiques ont des répercussions massives sur les machines et les installations qui, étant de plus en plus connectées, ne sont plus uniquement accessibles dans l'enceinte de l'entreprise, et ont de ce fait également un impact sur la SST.

Les fabricants doivent faire évaluer la conformité de leurs produits soit par une procédure interne, soit par contrôle effectué par un organisme notifié. Si le fabricant opère en conformité avec des normes harmonisées, ou a déjà obtenu un certificat dans le cadre d'un système européen de certification en matière de cybersécurité, on peut partir du principe que le matériel ou le logiciel concerné est conforme au règlement. Les importateurs et distributeurs sont tenus de vérifier que le fabricant a respecté les procédures pertinentes, et que l'appareil porte le marquage CE. Pour les produits peu critiques, les fabricants sont autorisés à établir eux-mêmes une déclaration de conformité. Pour la classe II, une évaluation effectuée par un tiers sera obligatoire.

La Commission estime qu'il y a urgence à agir : en 2021, on avait en effet déjà estimé que les coûts provoqués chaque année par la montée de la cybercriminalité se chiffraient à 5,5 billions d'euros. Dans un environnement connecté, tout incident de cybercriminalité ciblant un produit peut avoir un impact sur toute une entreprise, voire sur toute une chaîne d'approvisionnement, et se propager, souvent en quelques minutes seulement, au-delà des frontières du Marché intérieur, comme cela a été le cas pour le virus informatique WannaCry. Cela pourrait avoir pour effet de stopper des activités économiques et sociales, voire de mettre des vies humaines en péril.

Des critiques vis-à-vis du projet

Dans une prise de position[2], l'Assurance sociale allemande des accidents du travail et maladies professionnelles (DGUV) critique déjà le fait que le terme central de « cybersécurité » n'est pas clairement défini. Dans diverses normes et réglementations, il désigne tour à tour un état, une activité ou un produit. D'une manière générale, les mots comportant le préfixe « cyber », mais non spécifiés précisément, posent problème. Ainsi, selon certaines sources, les attaques par radio ou par clé USB ne sont pas considérées comme étant des événements relevant de la cybersécurité.

La DGUV voit également d'un œil critique l'obligation qu'ont les fabricants de signaler dans les 24 heures, avec force détails, toute faille de sécurité. Dans de nombreux cas, procéder à un contrôle dans un laps de temps aussi court n'est pas réaliste. De plus, il n'est pas absolument indispensable de transmettre des détails susceptibles d'être utilisés pour une attaque. Dans sa prise de position, la DGUV plaide pour que soient transmises uniquement les données dont les autorités ont vraiment besoin, par exemple pour mettre en garde contre un produit ou pour évaluer l'impact d'une faille. La DGUV estime aussi que le délai de deux ans qui est prévu pour une adaptation aux nouvelles exigences est trop court pour les fabricants qui sont tributaires d'autres produits et doivent par exemple attendre une évaluation de conformité.

Comme le déplore aussi Jonas Stein, qui dirige le groupe de travail Security de la DGUV, il est impossible de contrôler de manière adéquate les systèmes d'exploitation, car ils évoluent constamment. De plus – comme c'est le cas notamment pour Linux – ils s'agit souvent de systèmes d'exploitation open source. Or, les logiciels libres ne proviennent pas d'un seul et même fabricant qui serait responsable de la procédure de conformité. Le monde de l'open source craint lui-même de tomber dans le piège de la responsabilité, car dans le cas d'œuvres communes créées par plusieurs développeurs, chacun d'entre eux aurait à répondre de failles potentielles. Comme le déplore la Free Software Foundation Europe (FSFE), « En raison du manque de financement et de ressources nécessaires pour suivre les procédures proposées pour la conformité CE, il est possible que certains de ces projets doivent être totalement abandonnés. »

Dr Stefan Krempl
Journaliste indépendant
sk@nexttext.de

Le Conseil des ministres de l'UE et la Commission de l'industrie du Parlement européen, en charge du dossier, ont pris position mi-juillet sur la proposition de la Commission, de sorte que les négociations portant sur un compromis final pourront bientôt commencer. Les États membres plaident notamment pour une simplification de la déclaration de conformité, pour un soutien accru pour les petites entreprises, et pour une clarification par les fabricants de la durée de vie escomptée des produits. Par ailleurs, ce n'est pas à l'ENISA, mais aux autorités nationales compétentes qu'il conviendrait de signaler les vulnérabilités exploitées ou les incidents de sécurité. Les députés, quant à eux, réclament des définitions plus précises, des calendriers réalisables et une répartition plus équitable des responsabilités. Ils insistent par ailleurs pour que les appareils pour la maison intelligente, les montres connectées et les caméras de sécurité privées soient également inclus dans la classe à haut risque.

1 https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52022PC0454
2 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Legislation-sur-la-cyberresilience-nouvelles-regles-en-matiere-de-cybersecurite-concernant-les-produits-numeriques-et-les-services-accessoires/F3376532_fr (en allemand)

© Vector Tradition - stock.adobe.com

Des connaissances avérées dans de nouvelles spécifications sur la sécurité informatique industrielle

Les composants de sécurité fonctionnelle protègent la vie et la santé des personnes, par exemple en empêchant l'accès aux zones dangereuses des machines et installations. Il est également important que les manipulations extérieures n'impactent pas la sécurité. Il est essentiel pour cela que l'état de l'art soit systématiquement mis en œuvre et que les fabricants et exploitants réagissent de manière appropriée à toute faille de sécurité.

Pour que les fonctions de sécurité d'un système de commande puissent fonctionner fiablement, il faut que ce système soit lui-même sûr, et donc protégé contre les pannes et manipulations. On ne peut qu'être effrayé face au nombre croissant de catastrophes relatées dans le domaine de la sécurité informatique industrielle. Mais il y a tout lieu d'être optimiste, l'état de la technique permettant de fait d'éviter très facilement la quasi-totalité des failles de sécurité, comme le montre l'exemple caractéristique suivant :

Dès 1883, Auguste Kerckhoffs énonçait six règles fondamentales à respecter pour assurer la confidentialité d'une communication. La deuxième était la suivante : « Il faut que le système n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi. » De toute évidence, Guglielmo Marconi ne connaissait pas ce texte. Pour garantir une communication confidentielle, sa télégraphie exigeait que personne n'entre en possession de l'un des appareils ou en construise un identique et le règle sur la même fréquence. En 1903, Nevil Maskelyne mettait le doigt sur le problème en transmettant en morse des messages injurieux, parasitant une démonstration de Marconi. Il est considéré depuis comme étant l'un des premiers hackers de l'histoire. Bien que le chiffrement sécurisé à l'aide de méthodes cryptographiques soit connu depuis longtemps, ce même défaut de conception apparaît encore aujourd'hui, par exemple dans les commandes radio de feux de circulation[1] ou de grues industrielles[2].

Une définition unique des termes fait défaut

À ce jour, le navigateur de l'Université de Brême dédié aux normes relatives à la sécurité informatique[3] a saisi dans une base de données quelque 800 normes et plus de 2000 résultats pertinents concernant la législation. Le problème est que les documents utilisent des termes différents et ne les définissent pas toujours clairement. Alors que certains documents traitent largement de la « security » ou de la « sécurité informatique », d'autres inventent de nouveaux termes, sous forme de mots-valises composés de « cyber » et d'un autre mot. Ces mots nouvellement créés doivent être définis exactement dans le document, car ils n'ont en soi aucune signification univoque. Le terme « cybersécurité » désigne tantôt une activité, tantôt une mesure prise contre les attaques venues du web, tantôt un état dans lequel le produit est protégé contre les attaques par radio.

Plutôt que de créer de nouveaux mots, il est préférable de travailler avec les termes sans équivoque que sont la sécurité informatique, ou le terme anglais security. S'il s'agit de restreindre la signification, par exemple aux attaques par radio, cette restriction devra alors être clairement précisée. Le Règlement européen sur les machines a opté pour une autre solution très élégante, en exigeant, à l'Annexe III 1.1.9, une « protection contre la corruption », en étant plus clair sur ce point que l'ancienne directive Machines. Se concentrant sur l'objectif de protection selon lequel aucune situation dangereuse ne doit survenir, provoquée notamment par un dispositif distant, le règlement ne précise pas en détail ce qui peut être à l'origine de la corruption.

Un élément décisif : une communication rapide

Une communication rapide et efficace est la clé d'une réaction adéquate aux failles de sécurité. Les déficiences dans ce domaine ont toutefois été mises en évidence en décembre 2021, lorsqu'une faille de sécurité dans la bibliothèque logicielle Log4J a fait les grands titres de l'actualité. Cette bibliothèque fait en effet partie intégrante non seulement de nombreux services de serveur, mais aussi d'une quantité de composants industriels. Alors que, d'un côté, des voix se sont fait entendre, dénonçant une mauvaise utilisation de la bibliothèque, et affirmant qu'on aurait pu éviter les problèmes de sécurité en lisant la documentation, de nombreux fabricants se sont en même temps demandé s'ils étaient victimes des failles de sécurité. Il n'a pas été rare que plusieurs mois s'écoulent avant que les fabricants sachent si leurs produits étaient impactés.

Ce qui a fait défaut, en résumé :

- un contact d'urgence pour la sécurité informatique au sein de l'entreprise,
- un format unique pour les recommandations d'action et
- un standard permettant au fabricant de signaler que tel ou tel produit n'est pas concerné par une faille de sécurité.

Pour pallier le manque d'informations et d'interfaces uniformes, il existe un ensemble de spécifications ouvertes élaboré par divers groupements d'entreprises, d'autorités et d'organisations, et que chaque entreprise peut mettre en œuvre dès à présent (voir tableau). Un contact d'urgence selon la spécification RFC 9116 de l'IETF est consigné sur le site web dans un simple fichier security.txt[4], fichier dans lequel un fabricant peut aussi renvoyer à sa liste de recommandations d'action (CSAF). Chaque produit matériel ou logiciel reçoit un identifiant unique au niveau mondial (CPE), ce qui permet aux messages d'alerte internationaux (CVE) d'être automatiquement et précisément attribués aux produits et versions en question. La criticité de la vulnérabilité est évaluée, aussi que faire se peut, par un système de notation international standardisé (CVSS). La spécification ouverte SPDX permet de documenter, pour chaque projet et sous un format lisible par machine, quelles bibliothèques ont été utilisées. Côté exploitant, un programme peut alors interroger régulièrement tous les produits pour identifier toute alerte de sécurité et afficher les recommandations d'action.

Certaines grandes entreprises ont déjà recours à ces spécifications. Il est maintenant essentiel que toutes les autres entreprises suivent rapidement cet exemple, afin que l'information sur les problèmes de sécurité se fasse rapidement et à moindres frais.

La première mesure à prendre par les entreprises consisterait tout au moins à veiller à être joignables en cas d'incident de sécurité informatique, et d'indiquer qui contacter en cas d'urgence. En suivant les instructions données sous https://cert.dguv.de, cette mesure peut être mise en place en quelques minutes.

Jonas Stein

Responsable du laboratoire de sécurité informatique industrielle et du groupe de travail Security de la DGUV

Jonas.Stein@dguv.de

Spécifications ouvertes pour la sécurité informatique

Information d'entrée	Suivi par	Spécification
Propre contact d'urgence	Fabricant, exploitant	„security.txt" RFC 9116
Identification / ID du produit (nom du fabricant, du produit, version, version linguistique…)	Fabricant	CPE
Liste des logiciels (Software Bill of Materials - SBOM)	Fabricant	SPDX
Alerte sur une faille de sécurité	Autorités de numérotation CVE	CVE
Security Advisory (recommandation d'action sur la CVE)	Fabricant	CSAF
Caractéristiques permettant d'évaluer la criticité	Fabricant	CVSS

Ensemble de spécifications ouvertes qui contribueront de manière décisive à améliorer la sécurité informatique industrielle. Elles permettront, dans les années à venir, d'accélérer la communication sur les failles de sécurité, et d'atteindre une rapidité qui fait cruellement défaut.

1 Reportage TV (chaîne ARD) « Quand les feux de circulation passent au vert par piratage informatique » 2021 (en allemand), https://ardmediathek.de Hacker Ampeln
2 Andersen et al, 2019 « A Security Analysis of Radio Remote Controllers for Industrial Applications » https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf
3 https://cybersecurity-navigator.de
4 Des failles critiques de sécurité sur machines et installations et security.txt https://cert.dguv.de

Le nouveau règlement sur les machines – ses conséquences pour les normes harmonisées

Dans aucun autre secteur industriel, ou presque, les normes ont autant d'importance que dans la construction mécanique. Le nouveau règlement européen sur les machines confronte les comités de normalisation à une mission de taille : vérifier que les normes sont conformes au nouveau cadre légal et, le cas échéant, prendre les mesures nécessaires pour les adapter.

Au fil des ans, le besoin élevé de sécurité des utilisateurs de machines – auquel s'ajoute la diversité des types de machines – a débouché sur le nombre impressionnant de plus de 800 normes harmonisées relevant de la directive européenne Machines. Leurs utilisateurs peuvent partir du principe que les solutions et mesures qu'elles contiennent sont propres à satisfaire aux exigences légales des règlements et directives pour lesquels elles ont été élaborées. Sur ces quelque 800 normes, une centaine appelées « normes B » traitent de certains aspects de sécurité ou de dispositifs de protection qui s'appliquent à une multitude de machines. Plus de 700 normes décrivent des exigences et solutions techniques pour des types concrets de machines (normes C). Au fil des ans, la symbiose entre la directive Machines et les normes harmonisées a engendré un système éprouvé et solidement établi, qui garantit pour les machines un niveau de sécurité élevé reconnu au niveau international.

La normalisation confrontée à une tâche gigantesque

Avec le nouveau règlement (UE) 2023/1230 sur les machines, publié le 29 juin 2023 au Journal officiel de l'UE, la Commission européenne a ouvert un nouveau chapitre législatif. Le nouveau règlement, qui abroge la directive Machines 2006/42/CE encore valable, sera applicable à partir d'une date fixée au 20 janvier 2027, et donc sans période de transition. Outre de nombreux ajustements de la forme et du fond du texte juridique, des modifications substantielles ont été apportées à l'Annexe I de l'ancienne directive, où sont décrites les exigences essentielles de sécurité et de santé. Dans le nouveau règlement, ces exigences se trouvent dans la nouvelle Annexe III. Concrétiser ces exigences est le principal objet des normes harmonisées. Les modifications apportées soulèvent inévitablement les questions suivantes :

Quel est l'impact direct des exigences de sécurité et de santé nouvelles et modifiées sur le contenu des normes harmonisées actuelles ? Et les normes harmonisées relevant de la directive Machines peuvent-elles continuer à être utilisées sous le nouveau règlement, et conservent-elles leur présomption de conformité ?

La réponse à la première question n'est pas anodine, car les détails de la mise en œuvre pratique et normative des nouvelles exigences que sont la « protection contre la corruption », la « fonction de supervision pour les machines mobiles autonomes », ou le fait d'éviter le « risque de contact avec les lignes électriques aériennes sous tension » fait encore l'objet de discussions intensives.

Mais il suffit de jeter un regard sur les domaines d'application des normes pour constater qu'aucune catégorie de machines, ou presque, ne devrait être totalement épargnée par la création ou la modification notable des exigences de sécurité et de santé induites par le nouveau règlement. Cela signifie que les normes harmonisées devront toutes être contrôlées du point de vue de leur pertinence avec les nouvelles exigences et, le cas échéant, être adaptées, tant sur la forme que sur le fond, conformément aux règles de procédure de la Commission européenne (Annexe ZA sous forme de tableau, références datées). Or, cela impliquerait théoriquement une révision de la quasi-totalité des 800 normes harmonisées, avec, pour chacune d'entre elles, les évaluations circonstanciées des consultants HAS. Une tâche dont la réalisation semble totalement irréaliste durant les trois années qui restent jusqu'à la mise en œuvre définitive du nouveau règlement.

Un référencement restreint, solution transitoire possible

C'est pourquoi, selon l'état des discussions en août 2023, la Commission européenne prévoit, dans le cadre d'une action extraordinaire, de convertir en bloc, en tant que normes harmonisées relevant du nouveau règlement sur les machines, toutes les normes européennes (EN et EN ISO) recensées, à une date restant à déterminer située durant la première moitié de 2026, en tant que normes harmonisées sous la directive Machines. Seule restriction : ces normes ne peuvent évidemment garantir une harmo-

nisation que pour les exigences de sécurité et de santé qu'elles visaient déjà sous la directive Machines. Pour que cette restriction soit reconnaissable par les utilisateurs des normes dans les listes publiées au Journal officiel de l'UE, il sera indispensable que les Comités techniques (TC) responsables soumettent l'ensemble de leur portefeuille de normes à une vérification (MAIS PAS nécessairement à une révision), afin d'identifier les différentes lacunes par rapport au nouveau règlement. Parallèlement, des travaux sont lancés par le CEN et le CENELEC pour élaborer des solutions normatives répondant aux exigences de santé et sécurité nouvelles et/ou notablement modifiées, ce qui permettra de combler les lacunes identifiées. Un guide d'action est actuellement en cours de rédaction, avec le concours du forum sectoriel de coordination « Machinery » du CEN/CENELEC, afin d'aider les TC dans cette tâche très ambitieuse. Ce guide devrait être disponible au plus tard vers la fin de 2023.

Il est bien entendu déjà possible et conseillé de viser la conformité avec le nouveau règlement lors de révisions prévues ou de nouveaux projets de normalisation. On peut donc espérer que, d'ici le début de 2027, bon nombre de normes seront, de fait, déjà adaptées au nouveau règlement. Pour la majeure partie des normes harmonisées, ce ne sera toutefois possible qu'après le moment où celui-ci entrera en application.

Un calendrier plus précis des futures révisions de normes est attendu avec le nouveau mandat de normalisation de la Commission européenne pour le règlement sur les machines, mandat qui devrait être disponible l'année prochaine. Contrairement aux mandats précédents, il sera limité dans le temps (probablement entre 5 et 10 ans). Il constitue la base juridique sur laquelle pourront être élaborées les normes harmonisées relevant du nouveau règlement. Un premier projet de ce mandat de normalisation a été publié fin juin. Les commentaires des parties prenantes seront discutés au sein des organes compétents de la Commission, probablement à l'automne.

Et enfin, une autre mesure vise à faciliter, pour les utilisateurs des normes, le passage des normes harmonisées de la directive Machines au nouveau règlement sur les machines. Les normes publiées entre 2024 et la première moitié de 2026 seront dotées de deux annexes ZA – l'une pour la directive et l'autre pour le règlement – d'où il ressortira quelles sections de la norme couvrent telles ou telles dispositions légales. Ici aussi, les TC de normalisation concernés seront informés en temps utile.

Toutes les mesures décrites ci-dessus contribueront à ce que le passage des normes harmonisées de l'ancienne directive vers le nouveau règlement s'effectue le plus aisément possible.

Dr Frank Wohnsland

VDMA (Fédération allemande de la construction mécanique)

Président du Forum sectoriel « Machinery » du CEN/CENELEC

frank.wohnsland@vdma.org

Ergonomie numérique : un projet de la KAN fait le point sur l'état de la recherche

Mandatée par la KAN, la Sté BioMath a examiné où en est la recherche sur les interfaces et les formats de données des modèles humains numériques, et sur les systèmes de capture de mouvements.

Le secteur de la SST a recours à des modèles et méthodes numériques pour planifier et évaluer des produits et processus. Les modèles humains numériques simulent les aspects physiques du travail. Il existe en outre des systèmes capables de saisir les mouvements à partir des coordonnées des articulations humaines dans un espace tridimensionnel. Les données ainsi obtenues peuvent être alors importées dans un modèle humain numérique, à partir duquel les spécialistes définissent des actions permettant de concevoir des postes de travail sûrs et sains.

Tant les instituts de recherche que les entreprises disposent de méthodes et outils permettant l'analyse, l'évaluation et la visualisation des données provenant de modèles humains numériques et de systèmes de capture de mouvements. Il s'agit toutefois souvent de solutions isolées qui ne sont pas compatibles entre elles en raison de formats de données différents. Depuis les années 1960, quelque 150 modèles humains numériques différents ont été mis au point pour divers usages (mais ils ne sont plus tous utilisés).

Une standardisation des interfaces

- entre différents modèles humains numériques,
- entre différents systèmes de capture de mouvements et
- entre les modèles humains numériques et les systèmes de capture de mouvements

s'avèrerait utile pour la SST, car elle permettrait de créer une base de données plus fiable dont pourraient être déduites des mesures visant à une organisation du travail à dimension humaine. Des interfaces et formats de données standardisés permettraient de combiner des données de mouvements provenant de différentes sources et de les utiliser pour des évaluations générales.

Le projet de la KAN met en évidence la diversité des modèles

Dans le cadre d'un projet initié par la KAN, la Sté BioMath GmbH a recensé et évalué les publications scientifiques concernant l'ergonomie numérique. L'un des enjeux consistait à déterminer lesquelles, parmi les avancées des sciences du travail, peuvent être considérées comme sûres concernant les modèles humains numériques et la saisie, l'évaluation et la représentation numériques des données biomécaniques.

Le rapport[1] donne un aperçu des modèles humains numériques, de leurs caractéristiques et de leurs possibilités. L'étude révèle que les modèles humains numériques font appel à des mesures anthropométriques provenant de différentes bases de données, qui représentent des groupes de population différents. De plus, les données peuvent être regroupées et/ou ventilées très différemment d'une base de données à l'autre. La qualité des données détermine également la qualité des modèles humains numériques.

Il a été également examiné quels systèmes de capture de mouvements ont déjà fait l'objet d'études, le principal enjeu étant d'étudier les possibilités d'échange de données. Comme l'a révélé l'étude, il n'existe pas à ce jour de manière uniforme de procéder.

Dans les futurs projets de recherche, il conviendra donc d'examiner de plus près notamment les aspects suivants :

- Pour l'échange de données entre les modèles humains numériques, il serait utile de disposer d'un format standardisé, bien documenté et non lié à tel ou tel fabricant.
- Il serait bon de s'accorder sur la définition de termes donnés et sur les degrés de détails, par exemple pour certaines parties d'un modèle humain numérique.
- Étant donné qu'il existe différentes approches concernant les caractéristiques et la configuration de modèles humains, il serait important de définir pour les modèles une structure qui en favorise la comparabilité.

Et maintenant ?

L'exécutant du projet a synthétisé les résultats de l'étude dans un rapport qui décrit la situation actuelle et les approches visant à harmoniser les interfaces et formats de données uniformes. Il est prévu de mettre à disposition les contenus de ce rapport sous forme de rapport technique (DIN/TR). À cet effet, la KAN préparera le texte et introduira une demande auprès du DIN. L'objectif à long terme est de créer des normes fondamentales pour les modèles humains numériques, les interfaces et les formats de données. La KAN estime toutefois qu'une harmonisation complète des exigences n'est actuellement pas encore possible.

Katharina von Rymon Lipinski
vonrymonlipinski@kan.de

1 www.kan.de/fileadmin/Redaktion/Dokumente/KAN-Studie/de/2023_KAN-Projekt_Digitale_Ergonomie_bf_final.pdf

L'ASGA – une nouvelle commission pour des aspects transversaux de la SST

En 2021, la Commission d'État pour la sécurité et la santé au travail (ASGA) est venue compléter les commissions en charge de la SST qui existaient déjà au sein du Ministère fédéral du Travail et des Affaires sociales (BMAS). Quelle sont ses missions, et qu'est-ce qui a motivé sa création ?

En Allemagne, les commissions d'État[1] sont chargées d'élaborer des règles (techniques) qui concrétisent les objectifs généraux de protection des différentes ordonnances relevant de la loi sur la Sécurité et la santé au travail. Placées sous la coordination de l'Institut fédéral de la sécurité et de la santé au travail (BAuA), ces commissions sont dédiées aux facteurs de risque potentiels du système de travail, tels que les substances dangereuses, les agents biologiques, les lieux de travail et les équipements de travail. S'adressant aux employeurs, les règles définissent des exigences relatives aux processus et à la conception, exigences dont le respect permet d'être en conformité avec les contenus des différentes ordonnances relevant de la loi sur la SST (présomption de conformité).

Du fait de la diversification des formes de travail, de la numérisation et de l'impact de facteurs climatiques sur l'environnement de travail, l'approche d'une réglementation jusqu'alors systématiquement verticale ne suffit plus pour évaluer en profondeur les effets actuels et futurs sur les travailleurs, et en déduire les mesures appropriées. Même pour les sujets classiques, notamment l'évaluation des risques et la formation, les exigences ne dépendent pas des différents facteurs de risque, et devraient donc également être considérées (de manière horizontale) sous plusieurs perspectives.

Pendant la crise du covid et les défis nouveaux qu'elle a entraînés pour l'organisation de la SST dans les entreprises, ce besoin est devenu particulièrement évident. La règle relative au SARS-CoV a été la première à être conçue de manière ciblée pour couvrir plusieurs facteurs. Le succès de l'application de cette règle dans les entreprises a montré qu'il était judicieux d'examiner pour quels autres domaines thématiques l'élaboration de règles horizontales pour la SST en entreprise s'avérerait efficace.

C'est la raison pour laquelle, suite à l'amendement de l'article 24 a, publié en décembre 2020, l'ASGA[2] s'est trouvé directement ancrée dans la loi sur la SST. La nouvelle commission a notamment pour mission – pour autant qu'aucune autre commission d'État soit compétente pour le faire – d'élaborer des règles et des conclusions sur la manière dont les exigences définies dans la loi sur la SST peuvent être respectées.

Une deuxième raison qui a motivé la mise en place d'une nouvelle commission est le manque de cohérence dans le cadre réglementaire existant, qui s'explique par l'orientation strictement verticale des commissions existantes. Dès 2011, un document d'orientation sur la réorganisation des prescriptions et réglementations dans le domaine de la SST exprimait le souhait d'une meilleure harmonisation des contenus respectifs du droit statutaire autonome des organismes d'assurance accidents et des réglementations d'État, non seulement entre eux, mais aussi à l'intérieur des deux domaines de réglementation. Le chemin pour y parvenir est encore pratiquement

inexploré dans des domaines d'action majeurs, notamment l'évaluation des risques. Au sein de l'ASGA, tous s'accordent à vouloir s'attaquer systématiquement à cet enjeu.

Composition et mode de travail

La structure de l'ASGA ne diffère pas de celle des autres commissions dédiées à la SST. Elle se compose d'experts nommés par le BMAS, qui représentent les employeurs publics et privés, les syndicats, les autorités des Länder, l'assurance accidents légale et le monde de la recherche. La commission compte 15 membres et 15 membres suppléants.

Sa présidente a pour mission non seulement de diriger l'ASGA, mais aussi de coordonner la coopération de toutes les commissions dédiées à la SST, au sein d'un comité de pilotage. Cet organe assume une fonction centrale dans l'élaboration de règles pluridisciplinaires et horizontales. Les commissions font directement l'apport de leur expertise technique dans les différents groupes de projet, par le biais de personnes mandatées. Elles sont ainsi directement impliquées dans la rédaction des nouvelles règles, depuis l'élaboration de l'esquisse du projet jusqu'à leur adoption. C'est une nouveauté.

L'ASGA se réunit deux fois par an. Le comité de pilotage formule ses arguments et votes dans des recommandations, et les soumet au cercle de coordination de l'ASGA. Ce cercle de coordination examine les thèmes et missions d'actualité et prépare les projets de décision pour les réunions de l'ASGA.

Projets et enjeux prioritaires

Comme toutes les autres commissions, l'ASGA s'est fixé un programme de travail pour son mandat actuel. Les principaux sujets en sont l'évaluation des risques, le stress psychique, les formations efficaces et adaptées à notre époque, le travail mobile sur écran en dehors des lieux de travail, et l'impact du changement climatique sur la sécurité et la santé au travail. L'objectif est d'élaborer des règles gouvernementales qui s'intègrent de manière cohérente dans le cadre réglementaire existant.

Les défis sont actuellement nombreux, tout processus de changement se déroulant rarement sans heurts. L'objectif est de trouver le chemin adéquat pour parvenir à une culture de commission basée sur la qualité et le respect, afin de réaliser sur une base consensuelle l'ambitieux programme de travail. La présidence de l'ASGA doit en outre faire progresser les processus et instruments adéquats et transparents propres à soutenir cette évolution culturelle.

Le groupe de projet « Évaluation des risques » travaille déjà à la conception et à la définition du contenu d'une règle de l'ASGA. Le groupe de projet « Stress psychique » devrait commencer ses travaux avant la fin de l'année.

Pr Dr Anke Kahl

Chaire de la Sécurité au travail à l'Université de Wuppertal

Présidente de l'ASGA

1 www.bmas.de/DE/Arbeit/Arbeitsschutz/Arbeitsschutzausschuesse/arbeitsschutzausschuesse.html (en allemand)
2 www.baua.de/EN/Tasks/Committee-administration/ASGA/ASGA_node.html (en anglais)

Réforme de la législation européenne sur la responsabilité du fait des produits

À l'automne 2022, la Commission européenne a amorcé une modernisation des règles de l'UE concernant la responsabilité du fait des produits. Après qu'elle a publié des projets portant respectivement sur une révision de la directive sur la responsabilité du fait des produits et sur une nouvelle directive sur la responsabilité applicable à l'IA, ce sont maintenant le Conseil des ministres de l'UE et le Parlement qui examinent plus en détail la proposition.

Le passage à l'ère numérique implique un ajustement non seulement de la législation concernant la mise sur le marché, mais aussi du droit de la responsabilité civile. Vieille déjà de 1985, l'ancienne directive sur la responsabilité du fait des produits, qui a été transposée dans le droit allemand en 1989 avec l'adoption de la loi sur la responsabilité du fait des produits, n'est plus à même de couvrir tous les dommages causés par des produits. Il en résulte une incertitude juridique pour les entreprises, ainsi qu'un nombre croissant de produits pour lesquels le consommateur n'a droit à aucune compensation au titre des dommages qu'ils ont provoqués.[1] La directive doit être en outre alignée sur le règlement sur la sécurité générale des produits récemment actualisé, et sur le règlement sur la surveillance du marché.

Viser davantage de produits et de sinistres

On peut s'attendre à ce que la nouvelle directive s'applique à toutes sortes de produits, y compris à un certain nombre qui n'était pas couverts précédemment. Il s'agira notamment des produits intelligents, des mises à jour de logiciels, des systèmes d'IA et des services numériques, mais aussi des produits reconditionnés ou qui ont fait l'objet de modifications significatives. Les fabricants de l'économie circulaire ne seront toutefois pas tenus responsables des dommages provoqués par des parties non modifiées du produit.

Pour les produits provenant de pays tiers ou importés directement dans l'UE par les consommateurs, par exemple via le commerce en ligne, les droits de responsabilité seront élargis. Ils s'appliqueront dorénavant non seulement aux importateurs, qui sont actuellement responsables, mais aussi aux représentants des fabricants et aux autres acteurs, tels que les plateformes en ligne, basés dans l'UE.

Des modifications du droit procédural sont par ailleurs prévues : afin de mettre les fabricants et les consommateurs sur un pied d'égalité en termes d'informations, les acteurs économiques pourront être tenus de divulguer des éléments de preuve. D'une manière générale, la constitution de la preuve sera notablement allégée pour les victimes, sans toutefois qu'il y ait inversion de la charge de la preuve. Précédemment prévues, des limites concernant le plafond de la responsabilité et la franchise n'apparaissent plus dans le projet.

Un ajustement des règles en matière de responsabilité

Une indemnisation sur la base du projet de directive sur la responsabilité du fait des produits ne peut être revendiquée que dans le cas de dommages corporels (y compris d'atteintes à la santé psychique), de dommages matériels et de perte de données. Il s'agit d'une responsabilité stricte et objective du fait des produits, qui s'applique à l'encontre du fabricant et d'autres acteurs économiques. Seules les personnes physiques peuvent faire valoir des droits, et ce uniquement si le produit n'est pas utilisé exclusivement à des fins professionnelles.

Une nouvelle directive sur la responsabilité en matière d'IA complète le cadre juridique

La nouvelle directive sur la responsabilité du fait des produits sera accompagnée d'une directive sur la responsabilité en matière d'IA. En cas de dommages causés par des systèmes d'IA, elle devrait permettre aux victimes de faire valoir plus facilement leurs droits sur une base juridique différente de celle de la responsabilité du fait des produits, notamment en cas de violation des droits fondamentaux ou d'action civile en responsabilité.

Afin d'éviter une fragmentation juridique entre les États membres de l'UE, un cadre juridique harmonisé doit être défini pour la responsabilité des fabricants, des exploitants ou des utilisateurs de l'intelligence artificielle. Il est prévu que, en cas de dommage, l'IA soit présumée être à l'origine de ce dommage. Les victimes n'auront plus qu'à montrer que le fournisseur, l'exploitant ou l'utilisateur de l'IA n'a pas, par sa faute, respecté une obligation pertinente, et qu'un lien de causalité est probable. De plus, en cas de procès, les fabricants ou fournisseurs de systèmes d'IA à haut risque seront tenus de fournir toutes les informations pertinentes sur le produit.

La directive sur la responsabilité en matière d'IA ne permet pas à elle seule de faire valoir juridiquement des dommages et intérêts, mais elle complète les réglementations nationales existantes en matière de responsabilité pour faute en cas de violation de la loi par l'IA. Les nouvelles règles en matière de responsabilité pour faute permettent de simplifier les demandes d'indemnisation, et peuvent être invoquées par toute personne physique ou morale.

Des négociations dans les institutions de l'UE

Le Conseil des ministres de l'UE s'est déjà penché sur le projet de directive de la Commission sur la responsabilité du fait des produits, et l'approuve dans ses grandes lignes. La discussion au sein du Parlement européen a également été lancée, mais devrait prendre encore quelques mois. Les discussions concernant la directive sur la responsabilité en matière d'IA ne devraient intervenir que dans un deuxième temps.

Freeric Meier
meier@kan.de

1 Étude d'évaluation et propositions de directives : https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_5807

Le Royaume-Uni maintient la validité du marquage CE

Le ministère de l'Économie et du Commerce du Royaume-Uni a annoncé une prolongation indéfinie, au-delà de décembre 2024, de la validité du marquage CE pour les produits mis sur le marché en Grande-Bretagne (Angleterre, Écosse, Pays de Galles). Pour l'Irlande du Nord, c'était déjà le cas auparavant. Cette décision concerne 18 réglementations relevant de la compétence de ce ministère, concernant notamment les machines, les EPI, les équipements sous pression, les équipements basse tension, le matériel ATEX et les appareils à gaz.

Il était initialement prévu que, en Grande-Bretagne, la reconnaissance du marquage CE expire fin 2024, pour être obligatoirement remplacée par la marque UKCA (UK Conformity Assessed). La nouvelle réglementation permettra aux entreprises d'opter pour l'un ou l'autre marquage. Une solution avantageuse pour les entreprises, tant européennes que britanniques, car elles n'auront plus à faire certifier doublement leurs produits pour les exporter respectivement dans l'autre espace économique.

Pour en savoir plus (en anglais) : www.gov.uk/government/news/uk-government-announces-extension-of-ce-mark-recognition-for-businesses

Nouvelle campagne de l'EU-OSHA

L'Agence européenne pour la sécurité et la santé au travail (EU-OSHA) lance en octobre 2023 sa campagne « La sécurité et la santé au travail à l'ère numérique », qui s'étendra sur deux ans. L'EU-OSHA et ses points focaux nationaux organisent, au niveau européen et national, une multitude d'activités dont le but est de sensibiliser les salariés, les entreprises et les décideurs politiques aux enjeux de la sécurité et de la santé au travail.

Le contenu de la campagne est principalement axé sur le travail sur les plateformes numériques, l'automatisation des tâches, le travail à distance et hybride, la gestion des ressources humaines à l'aide de l'intelligence artificielle et les systèmes numériques intelligents. L'objectif est de mettre à disposition, à propos de ces thèmes, des données et faits susceptibles de promouvoir l'élaboration de réglementations, de lignes directrices et de mesures de sensibilisation et de soutien, ainsi que de nouveaux services et produits.

Pour en savoir plus sur la campagne : https://healthy-workplaces.osha.europa.eu/fr

La KAN au salon A+A 2023

Du 24 au 27 octobre 2023, le salon professionnel A+A attend les visiteurs à Düsseldorf. Ils trouveront la KAN sur le stand collectif de la DGUV, qui se présente au public dans le hall 5 du Parc des expositions, stand 5C06. Nous vous informerons sur les domaines sur lesquels nous travaillons actuellement, notamment les machines automotrices sans conducteur, les masques de protection contre les infections ou les barbecues au gaz. Nous vous présenterons aussi nos publications et répondrons volontiers à vos questions sur la sécurité et la santé au travail et la normalisation.

« L'individu normalisé – les données anthropométriques en pleine évolution » est le thème de la discussion « Sprech-Stunde Sicherheit und Gesundheit » (Une heure pour parler de la SST) proposée par la KAN le jeudi 26 octobre à 10 heures sur le podium du stand collectif de la DGUV.

La KAN est également présente au congrès A+A avec les exposés suivants :

- 25/10/2023 : VISION ZERO versus Standardization : A Position Statement (en anglais)
- 26/10/2023 : Les normes de management pertinentes pour la SST autres que la norme ISO 45001 (en allemand)

Vous trouverez des informations plus détaillées sur le programme sous https://www.aplusa-online.com

Des séminaires sur le travail de normalisation dans le domaine de la SST

En collaboration avec l'Institut pour la Santé au travail de la DGUV (IAG), la KAN propose deux séminaires consacrés au travail de normalisation dans le domaine de la SST (en langue allemande).

Le **séminaire de base** s'adresse aux membres actifs des comités de normalisation et à tous ceux qui s'intéressent à la normalisation dans l'optique des enjeux de sécurité et de santé. Vous découvrirez durant ce séminaire les processus d'élaboration des normes, et l'influence que vous pourrez exercer aux différentes phases. Des conseils et astuces, ainsi que l'échange avec les autres participants vous aideront à prendre part avec succès dans le travail de normalisation. Le séminaire de base aura lieu du 25 au 27 octobre 2023 à Dresde.

Vous possédez les bases du travail de normalisation et souhaitez élargir vos compétences ? Lors du **séminaire de perfectionnement**, vous rencontrerez d'autres experts expérimentés dans le domaine de la normalisation, et réfléchirez avec eux aux stratégies qui vous permettront d'optimiser encore votre travail et collaboration. Vous échangerez vos expériences sur le processus de normalisation et sur les possibilités de l'influer, et recevrez des informations actuelles dans le domaine de la normalisation.

La phase en présentiel du séminaire de perfectionnement a lieu les 5 et 6 décembre 2023 à Dresde. Les phases suivantes du séminaire sont prévues sous forme de sessions en ligne ou de phase d'auto-apprentissage.

Informations et inscription : https://asp.veda.net/webgate_dguv_prod, Numéro de l'événement : 570044 (base) et 570139 (perfectionnement)

Modifications européennes des normes CEI

Selon l'Accord de Francfort, les normes électrotechniques doivent être de préférence élaborées au niveau international par la CEI, et reprises parallèlement par le CENELEC à l'identique en tant que normes européennes (EN IEC). Or, lors de la reprise des normes CEI, il est nécessaire dans certains cas d'apporter des modifications européennes afin de répondre aux exigences des directives et règlements du Marché intérieur.

La présence d'une telle modification est reconnaissable au fait que le CENELEC publie ces normes non pas en tant que **EN IEC** 6xxxx, mais seulement en tant que **EN** 6xxxx, toutefois sous le même numéro que la norme CEI.

Agenda

18.-20.10.23 » Dresden

Seminar
Manipulation an Maschinen und Anlagen: Risiken erkennen, Maßnahmen ergreifen
IAG
https://asp.veda.net/webgate_dguv_prod
🔎 570089

19.10.23 » Bern

Tagung
Schweizerische Tagung für Arbeitssicherheit
SUVA
www.suva.ch 🔎 Tagung

24.-27.10.23 » Düsseldorf

Messe und Kongress / Trade fair and Congress
A+A 2023
Messe Düsseldorf
www.aplusa-online.com

25.10.23 » Online

Informationsveranstaltung
Dresdner Treffpunkt „Kollege Roboter – Mensch-Roboter Interaktion in der betrieblichen Praxis“
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
www.baua.de 🔎 Kollege Roboter

25.-27.10.23 » Dresden

Seminar
Grundlagen der Normungsarbeit im Arbeitsschutz
IAG/KAN
https://asp.veda.net/webgate_dguv_prod
🔎 570044

26.10.23 » Düsseldorf

Kongress
GfA-Herbstkongress 2023 „Nachhaltige Sicherheit und Gesundheit bei der Arbeit“
Gesellschaft für Arbeitswissenschaft (GfA)
www.gesellschaft-fuer-arbeitswissenschaft.de

02.11.23 » Berlin

Nationaler Kick-off der EU-OSHA-Kampagne 2023-25
Sicher und gesund arbeiten in Zeiten der Digitalisierung
BAuA/DGUV/EU-OSHA
www.baua.de 🔎 Nationaler Kick-off

13.11.23 – 18.01.24 » Dresden/Online

Seminar
Normungsarbeit im Arbeitsschutz weiterdenken – Aufbauseminar
IAG/KAN
https://asp.veda.net/webgate_dguv_prod 🔎 570139

15.11.23 » Online

Informationsveranstaltung
Dresdner Treffpunkt „Die neue europäische Maschinenverordnung“
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
www.baua.de 🔎 Maschinenverordnung

27.-28.11.23 » Bonn

Seminar
Maschinenanlagen/Technische Anlagen
MBT
www.maschinenbautage.eu/seminare/seminarmaschinenanlagen

29.11.-01.12.23 » Dresden

Seminar
Sicherer Einsatz von kollaborierenden Robotern
Institut für Arbeit und Gesundheit der DGUV (IAG)
https://asp.veda.net/webgate_dguv_prod
🔎 570164

04.-07.12.23 » Sankt Augustin

Seminar
Sicherheitstechnik von Maschinen
Institut für Arbeitsschutz der DGUV (IFA)
https://dguv.converia.de/frontend/index.php?sub=94

Commande

www.kan.de/fr » KANBrief (gratuit)

Gefördert durch: Bundesministerium für Arbeit und Soziales aufgrund eines Beschlusses des Deutschen Bundestages

Impressum

Éditeur
Verein zur Förderung der Arbeitssicherheit in Europa e.V. (VFA)
avec le soutien financier du Ministère fédéral allemand du Travail et des Affaires sociales

Rédaction
Commission pour la sécurité et santé au travail et la normalisation (KAN), Secrétariat
Sonja Miesner, Michael Robert
Tel. +49 2241 231 3450 · www.kan.de · info@kan.de

Responsable
Angela Janowitz, Alte Heerstr. 111, D – 53757 Sankt Augustin

Traduction
Odile Brogden

Publication
parution trimestrielle

ISSN: 2702-4024 (Print) · 2702-4032 (Online)