KAN Brief

3/23

Kommission Arbeitsschutz und Normung

INFORMATIONS-SICHERHEIT

Information security

La sécurité informatique

Inhalt

© a_korn - stock.adobe.com

Titel

Themen

© GordonGrand - stock.adobe.com

© KAN

Immer auf dem neuesten Stand:

www_kan_de

Kommission Arbeitsschutz und Normung (KAN)

KAN_Arbeitsschutz_Normung

KAN – Kommission Arbeitsschutz und Normung

Benjamin Pfalz
Vorsitzender der KAN
IG Metall

Cybersecurity: eine regulative und betriebliche Herausforderung

Unternehmen müssen sich mehr denn je vor Cyberangriffen schützen. Dabei handelt es sich längst auch um eine Frage des Arbeitsschutzes. Durch die Interaktion zwischen Mensch und Maschine, aufgrund ferngesteuerter Arbeitsmittel, vernetzter Produktionsanlagen und des zunehmenden Einsatzes von maschinellem Lernen muss Cybersicherheit immer öfter auch im Rahmen der betrieblichen Gefährdungsbeurteilung berücksichtigt werden. Grundsätzlich spielen Maßnahmen zur Produktsicherheit eine besondere Rolle.

Die Regelsetzung hat diese Aspekte zunehmend aufgenommen. Für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen beispielsweise konkretisiert die TRBS 1115 die Betriebssicherheitsverordnung bezüglich der Ermittlung und Festlegung erforderlicher Cybersicherheitsmaßnahmen. Gleichzeitig behandeln die neue EU Maschinen- und die kommende KI-Verordnung das Thema. Der sogenannte Cyber Resilience Act ist auf den Weg gebracht, um das Inverkehrbringen von Produkten und Vorprodukten mit digitalen Elementen zu regeln.

Die Normung muss die Verordnungsebene nun angemessen untersetzen. Der Normungsauftrag zum KI-Verordnungsentwurf adressiert das Thema Cybersecurity deutlich. Die europäischen Normungsorganisationen reagieren darauf bereits mit der Überprüfung des vorhandenen Normenwerks und der Zuschreibung des Themas innerhalb ihrer Strukturen.

Die Stimme des Arbeitsschutzes darf dabei keinesfalls fehlen! Die KAN widmet sich dem Thema daher auf allen Ebenen, beispielsweise durch ein Fachgespräch zur arbeitsschutzrelevanten Normung im Kontext der KI-Verordnung noch im laufenden Jahr. «

EU-Verordnung: Die vernetzte Geräte- und Maschinenwelt soll sicherer werden

Hersteller von Produkten „mit digitalen Elementen“ müssen die Cybersicherheit künftig während des ganzen Lebenszyklus gewährleisten, plant die EU-Kommission mit dem Cyber Resilience Act.

Die EU-Kommission macht angesichts anhaltender Online-Angriffe etwa mit Verschlüsselungstrojanern weiter Druck beim Absichern von IT-Sicherheitslücken. Nach Gesetzen wie dem 2019 beschlossenen Cybersecurity Act, mit dem die Basis für ein EU-weites Zertifizierungsschema für die IT-Sicherheit vernetzter Geräte, Systeme und Dienste steht, oder der jüngsten Novelle der Richtlinie über die Netzwerk- und Informationssicherheit (NIS2) hat sie im September 2022 einen Entwurf für einen Cyber Resilience Act (CRA)[1] auf den Weg gebracht. Laut der geplanten Verordnung zur Cyber-Widerstandsfähigkeit sollen Produkte „mit digitalen Elementen“ wie Hard- und Software künftig „mit weniger Schwachstellen auf den Markt kommen“.

Breit ist der Geltungsbereich des Entwurfs. Die Kommission will etwa „jedes Software- oder Hardware-Produkt und dessen Ferndatenverarbeitungslösungen“ einschließlich zugehöriger Komponenten erfassen, selbst wenn sie getrennt in Verkehr gebracht werden. Ein Schwerpunkt dürfte auf dem Internet der Dinge liegen oder auf privaten Kleinroutern („Plaste-Routern“), die aufgrund vieler eingebauter Sicherheitslücken bislang häufig einfach angreifbar sind. Außen vor bleiben sollen Produkte, „die ausschließlich für die nationale Sicherheit oder für militärische Zwecke entwickelt wurden“, oder die speziell für die Verarbeitung von Verschlusssachen bestimmt sind. Auch Sektoren wie die Luftfahrt, Medizinprodukte oder Kfz sind nicht betroffen, da für sie schon eigene einschlägige Anforderungen gelten.

Erfasste Hersteller müssen dem Vorhaben zufolge künftig grundlegende Cybersicherheitsanforderungen für das Design, die Entwicklung und den Fertigungsprozess erfüllen, bevor sie ein Gerät auf den Markt bringen. Sie sollen angehalten werden, Schwachstellen während des gesamten Lebenszyklus des Geräts zu überwachen und durch automatische und kostenlose Updates zu beheben. Dazu kommt eine Pflicht für die Hersteller, der EU-Agentur für Cybersicherheit ENISA binnen knapp bemessener 24 Stunden jeden Vorfall zu melden, der sich auf die Sicherheit einer Hard- und Software auswirkt. Generell soll eine koordinierte Linie zur Offenlegung von Schwachstellen eingeführt werden.

Angriffsflächen bei den einbezogenen Geräten müssten laut dem CRA begrenzt, die Auswirkungen von Zwischenfällen minimiert werden. Die erfassten Produkte sollen die Vertraulichkeit der Daten etwa durch Verschlüsselung sicherstellen. Pflicht werden soll der Schutz der Integrität und Verarbeitung von Informationen und Messwerten, die für das Funktionieren eines Artikels unbedingt erforderlich sind.

Über diese Basisauflagen hinaus hat die Brüsseler Regierungsinstitution besonders kritische Hochrisikobereiche ausgemacht. Die entsprechenden Produkte teilt sie in zwei Klassen, für die ein unterschiedliches Konformitätsverfahren eingeführt werden soll. Zur Kategorie I gehören Identitätsmanagementsysteme, Browser, Passwortmanager, Antiviren-Programme, Firewalls, virtuelle private Netzwerke (VPNs), Netzwerkmanagement, umfassende IT-Systeme, physische Netzwerkschnittstellen, Router und Chips. Dazu kommen Betriebssysteme etwa für Smartphones oder Desktop-Rechner, Mikroprozessoren und das Internet of Things (IoT) in Unternehmen, die nicht als besonders empfindlich gelten.

Die höhere Risikoklasse II beinhaltet Desktop- und Mobilgeräte, virtualisierte und etwa in Maschinen eingebaute Betriebssysteme, Aussteller digitaler Zertifikate, Allzweck-Mikroprozessoren, Kartenlesegeräte, Robotersensoren und intelligente Messgeräte. Ferner sollen darunter IoT-Geräte, Router und Firewalls für den industriellen Einsatz fallen, der generell als „sensible Umgebung“ gilt. Denn IT-Sicherheitslücken haben längst auch massive Auswirkungen auf Maschinen und Anlagen, die zunehmend vernetzt und nicht mehr nur innerhalb des Betriebsgeländes erreichbar sind, und so auch auf den Arbeitsschutz.

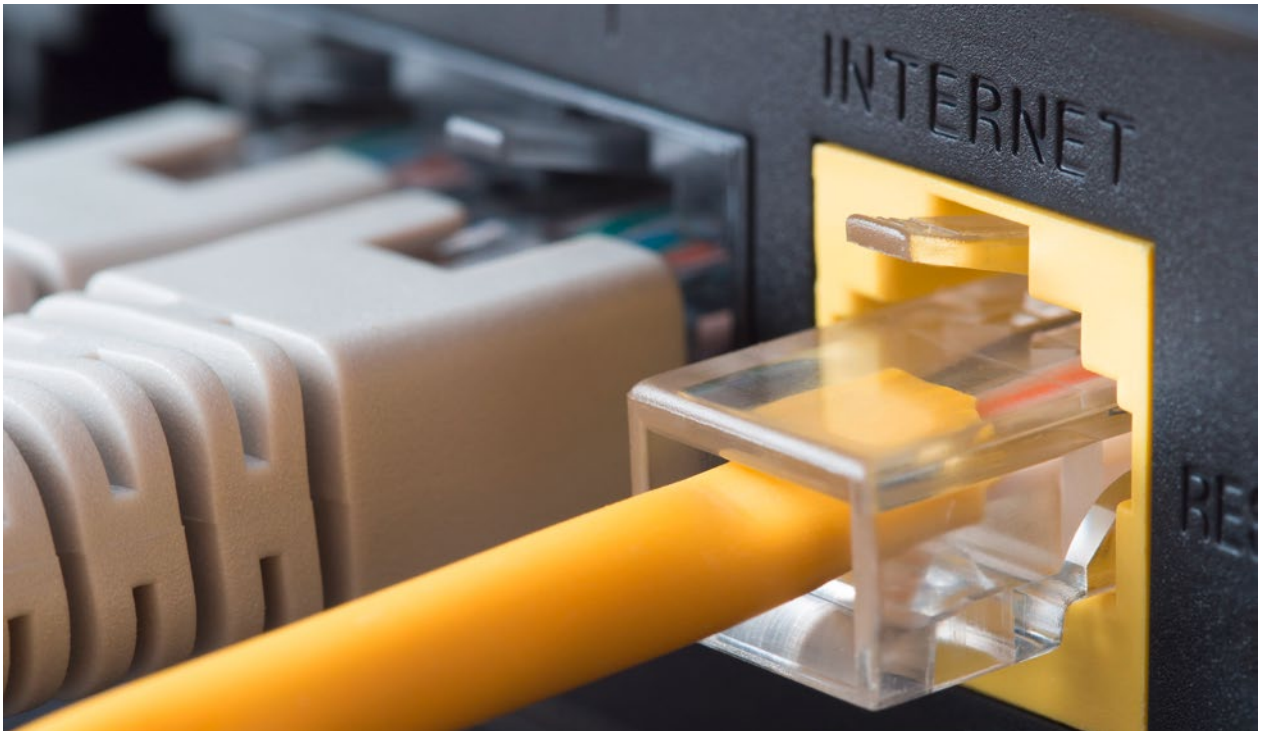
Hersteller sollen Konformitätsbewertungen ihrer Produkte über ein internes Verfahren oder eine Prüfung durch anerkannte Stellen durchführen. Wenn der Produzent auf harmonisierte Normen setzt oder bereits ein Zertifikat im Rahmen eines europäischen Zertifizierungssystems für Cybersicherheit erhalten hat, ist davon auszugehen, dass die entsprechende Hard- oder Software mit der Verordnung übereinstimmt. Importeure und Händler werden verpflichtet, die Einhaltung der einschlägigen Verfahren durch den Produzenten und die CE-Kennzeichnung des Geräts zu überprüfen. Für wenig kritische Produkte dürften Hersteller selbst eine Konformitätserklärung erstellen. In der Risikoklasse II soll eine Bewertung durch Dritte nötig sein.

Die Kommission sieht Handlungsbedarf, da die verstärkte Cyberkriminalität schon bis 2021 zu geschätzten jährlichen Kosten in Höhe von 5,5 Billionen Euro geführt habe. In einem vernetzten Umfeld könne ein Cybersicherheitsvorfall bei einem Produkt ein ganzes Unternehmen oder eine ganze Lieferkette in Mitleidenschaft ziehen und sich oft innerhalb weniger Minuten über die Grenzen des Binnenmarktes hinweg ausbreiten, wie etwa im Falle des Computerschädlings WannaCry. Wirtschaftliche und soziale Aktivitäten würden so unterbrochen, sogar Leben bedroht.

Kritik am Verordnungsentwurf

Die Deutsche Gesetzliche Unfallversicherung (DGUV) kritisiert in einer Stellungnahme[2], dass bereits der Kernbegriff Cyber-Security nicht klar definiert sei. Darunter werde in verschiedenen Normen und Verordnungen wechselweise ein Zustand, eine Tätigkeit oder ein Produkt verstanden. Problematisch seien generell Wörter, die aus „Cyber“ zusammengesetzt, aber nicht genau umrissen würden. So würden – je nach Quelle – Angriffe per Funk oder USB-Schnittstellen mit dem Begriff Cyber-Security nicht betrachtet.

Kritisch sieht die DGUV auch die Pflicht für Hersteller, binnen 24 Stunden umfangreiche Details zu einer Sicherheitslücke zu melden. In dieser kurzen Zeit sei eine Prüfung in vielen Fällen nicht realistisch. Gleichzeitig sei die Weiterleitung von



© a_korn - stock.adobe.com

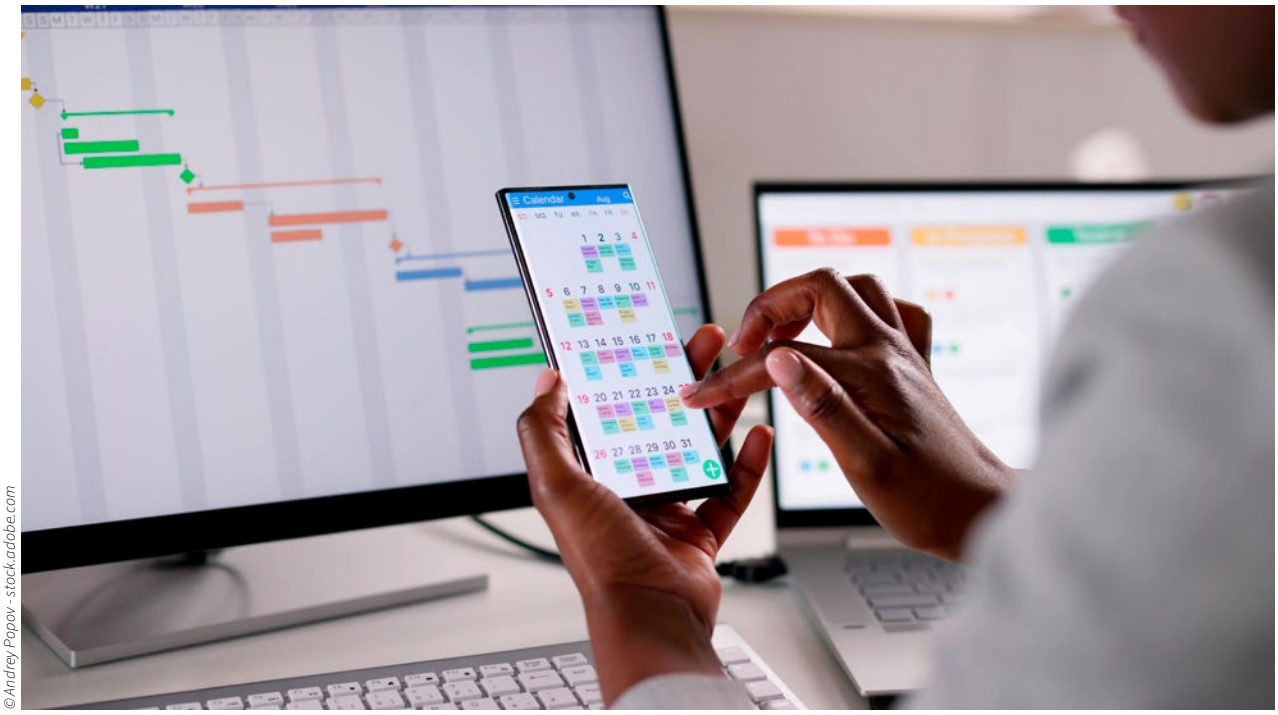
Details, die für Angriffe genutzt werden können, nicht unbedingt notwendig. In ihrer Stellungnahme plädiert die DGUV dafür, nur Daten zu übermitteln, die die Behörden wirklich benötigen, etwa zur Produktwarnung oder zur Abschätzung der Auswirkungen einer Schwachstelle. Auch das vorgesehene Zeitfenster von zwei Jahren, um sich auf die neuen Anforderungen einzustellen, hält die Gesetzliche Unfallversicherung für Hersteller zu knapp bemessen, die von anderen Produkten abhängig sind und etwa auf eine Konformitätsbewertung warten müssen.

Betriebssysteme könnten nicht sinnvoll geprüft werden, da sie sich ständig weiterentwickelten, moniert Jonas Stein, Leiter des Arbeitskreises Security der DGUV, ferner. Oft seien sie zudem – etwa bei Linux – von Open Source abhängig. Bei freier Software gebe es aber nicht einen einzelnen Hersteller, der für das Konformitätsverfahren zuständig wäre. Die Open-Source-Szene selbst befürchtet, in die Haftungsfalle zu tappen, da viele einzelne Entwickler zu Gemeinschaftswerken beitrügen und alle für potenzielle Lücken geradestehen müssten. Die Free Software Foundation Europe (FSFE) beklagt: „Aufgrund des Mangels an Finanzmitteln und Ressourcen, um die vorgeschlagenen Verfahren zur CE-Konformität zu durchlaufen, müssen einige dieser Projekte möglicherweise vollständig eingestellt werden."

Der EU-Ministerrat und der federführende Industrieausschuss des Europäischen Parlaments haben Mitte Juli zu dem Kommissionsvorschlag Position bezogen, sodass bald die Verhandlungen über einen finalen Kompromiss starten können. Die Mitgliedsstaaten plädieren etwa für eine vereinfachte Konformitätserklärung, mehr Unterstützung für kleine Unternehmen sowie eine Klarstellung der erwarteten Produktlebensdauer durch die Hersteller. Ausgenutzte Schwachstellen oder Sicherheitsvorfälle sollen zudem nicht an die ENISA, sondern an die zuständigen nationalen Behörden gemeldet werden müssen. Die Abgeordneten wiederum fordern präzisere Definitionen, praktikable Zeitpläne und eine gerechtere Verteilung der Verantwortlichkeiten. Andererseits drängen sie darauf, etwa auch Geräte fürs intelligente Heim, Smartwatches und private Sicherheitskameras in die Hochrisikokategorie aufzunehmen.

Dr. Stefan Krempl
Freier Journalist
sk@nexttext.de

1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454
2 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Gesetz-uber-Cyberresilienz-neue-Cybersicherheitsvorschriften-fur-digitale-Produkte-und-Nebendienstleistungen/F3376532_de



Bewährtes Wissen in neuen Spezifikationen zu Industrial Security

Komponenten der funktionalen Sicherheit schützen das Leben und die Gesundheit von Personen, etwa indem sie den Zugang zu gefährlichen Bereichen von Maschinen und Anlagen verhindern. Wichtig ist, dass auch Manipulationen von außen die Sicherheit nicht beeinträchtigen. Dazu muss der Stand der Technik konsequent umgesetzt werden und Hersteller und Betreiber müssen im Falle von Sicherheitslücken angemessen darauf reagieren.

Damit Sicherheitsfunktionen von Steuerungen zuverlässig funktionieren können, muss auch die Steuerung selbst sicher sein – geschützt also vor Ausfall und Manipulation. Die steigende Frequenz neuer Katastrophenmeldungen im Bereich Industrial Security wirkt erschreckend. Doch es gibt Grund zur Hoffnung, denn fast alle Sicherheitslücken können nach dem Stand der Technik eigentlich sehr leicht vermieden werden, wie folgendes typische Beispiel zeigt.

Bereits 1883 stellte Auguste Kerckhoffs sechs Grundvoraussetzungen für eine vertrauliche Kommunikation auf. Die zweite lautete „Das System darf keine Geheimhaltung erfordern und muss ohne Nachteil in die Hände des Feindes fallen können“. Diese Schrift kannte Guglielmo Marconi offensichtlich nicht. Seine Telegraphie zur vertraulichen Kommunikation erforderte, dass niemand in Besitz eines der Geräte kommt oder eines nachbaut und auf die gleiche Frequenz einstellt. Nevil Maskelyne machte 1903 auf das Problem aufmerksam, indem er während Marconis Vorführung unflätige Nachrichten dazwischen morste, und gilt dadurch als einer der ersten Hacker. Obschon die sichere Verschlüsselung mit kryptographischen Methoden lange bekannt ist, findet sich der gleiche Designfehler auch heute noch etwa in Funksteuerungen für Ampelsysteme[1] oder Industriekranen[2].

Es fehlt an einheitlicher Definition der Begriffe

Der Navigator für Normen mit Bezug zu Security von der Universität Bremen[3] hat aktuell rund 800 Normen und über 2000 Treffer zu Rechtsvorschriften in einer Datenbank erfasst. Problematisch ist, dass die Dokumente unterschiedliche Begriffe verwenden und zum Teil nicht eindeutig definieren. Während manche Dokumente umfassend von Security oder Informationssicherheit handeln, erfinden andere neue Begriffe als Kofferwort aus „Cyber“ und einem weiteren Wort. Diese neu geschaffenen Wörter müssen im Dokument genau definiert werden, da sie für sich keine eindeutige Bedeutung haben. Mal ist „Cybersicherheit“ eine Tätigkeit, mal ist es eine Maßnahme gegen Angriffe aus dem Internet, ein anderes Mal ein Zustand, bei dem das Produkt vor Angriffen über Funk geschützt ist.

Besser als neue Wörter zu erzeugen ist es, mit den eindeutigen Begriffen Informationssicherheit oder Security zu arbeiten. Muss der Bedeutungsumfang etwa auf Angriffe über Funk reduziert werden, sollte die Einschränkung klar benannt werden. Einen anderen sehr eleganten Weg hat die EU-Maschinenverordnung gewählt, indem sie in Anhang III 1.1.9 einen „Schutz gegen Korrumpierung“ fordert und in diesem Punkt auch deutlicher ist als die bisherige EU-Maschinenrichtlinie. Dabei fokussiert sie sich auf das Schutzziel, dass etwa bei Fernzugriff keine gefährlichen Situationen entstehen dürfen und lässt offen, wodurch die Korrumpierung im Detail hervorgerufen wird.

Schnelle Kommunikation ist entscheidend

Eine schnelle und effektive Kommunikation ist der Schlüssel zur angemessenen Reaktion auf Sicherheitslücken. Wie schlecht es jedoch um die Kommunikation bestellt ist, zeigte sich im Dezember 2021, als eine Sicherheitslücke in der Softwarebibliothek Log4J Schlagzeilen machte. Diese Softwarebibliothek ist nicht nur Bestandteil vieler Serverdienste, sondern auch vieler Industriekomponenten. Während einerseits Vorwürfe laut wurden, dass die Bibliothek falsch eingesetzt wurde und die Sicherheitsprobleme durch Lesen der Dokumentation verhindert worden wären, rätselten gleichzeitig viele Hersteller, ob sie von Sicherheitslücken betroffen sind. Nicht selten brauchten Hersteller viele Monate, bis sie wussten, ob ihre Produkte betroffen sind.

Zusammengefasst fehlte es an

- einem Notfallkontakt für Security innerhalb des Unternehmens,
- einem einheitlichen Format für Handlungsempfehlungen und
- einem Standard, nach dem Hersteller auch mitteilen können, dass ein bestimmtes Produkt nicht von einer Sicherheitslücke betroffen ist.

Der Mangel an einheitlichen Informationen und Schnittstellen wird durch einen Satz offener Spezifikationen behoben, die von verschiedenen Zusammenschlüssen von Unternehmen, Behörden und Organisationen erarbeitet wurden und die jedes Unternehmen ab sofort umsetzen kann (siehe Tabelle). Ein Notfallkontakt nach der IETF-Spezifikation RFC 9116 wird in einer einfachen security.txt-Datei auf der Webseite hinterlegt[4]. Darin kann ein Hersteller auch auf seine Liste der Handlungsempfehlungen (CSAF) verweisen. Jedes Hardware- und Softwareprodukt bekommt eine weltweit eindeutige Identifikation (CPE), damit die Internationalen Warnmeldungen (CVE) automatisch den exakten Produkten und Versionen zugeordnet werden können. Die Kritikalität der Sicherheitslücke wird durch einen weltweit einheitlichen Index (CVSS) so gut es eben geht eingestuft. Anhand der offenen Spezifikation SPDX kann zu jedem Projekt maschinenlesbar dokumentiert werden, welche Bibliotheken verwendet wurden. Auf Betreiberseite kann dann ein Programm zu allen Produkten regelmäßig abfragen, ob Sicherheitswarnungen vorliegen und die Handlungsempfehlungen anzeigen.

Einige große Unternehmen setzen bereits auf diese Spezifikationen. Entscheidend ist nun, dass auch alle anderen Unternehmen schnell folgen, damit die Information zu Sicherheitsproblemen schnell und kostensparend erfolgt.

Als ersten Schritt sollten Unternehmen jetzt zumindest die Erreichbarkeit bei Sicherheitsvorfällen sicherstellen und einen Notfallkontakt bekannt machen. Mit der Anleitung auf https://cert.dguv.de kann das in wenigen Minuten umgesetzt werden.

Jonas Stein

Leiter des Prüflabors für Industrial Security und Leiter des Arbeitskreises Security der DGUV

Jonas.Stein@dguv.de

Offene Spezifikationen zur Informationssicherheit

Eingangsinformation	Gepflegt durch	Spezifikation
Eigener Notfallkontakt	Hersteller, Betreiber	„security.txt“ RFC 9116
Produktkennung / ID (Herstellername, Produktname, Version, Sprachausführung, ...)	Hersteller	CPE
Softwareliste (Software Bill of Materials – SBOM)	Hersteller	SPDX
Warnmeldung zur Sicherheitslücke	CVE-Nummerierungsstellen	CVE
Security Advisory (Handlungsempfehlung zur CVE)	Hersteller	CSAF
Eigenschaften zur Bewertung der Kritikalität	Hersteller	CVSS

Satz offener Spezifikationen, die gemeinsam einen entscheidenden Beitrag zur Industrial Security liefern werden. Sie werden die Kommunikation zu Sicherheitslücken in den kommenden Jahren auf die dringend erforderliche Geschwindigkeit beschleunigen.

1 ARD-Reportage 2021, https://ardmediathek.de „Hacker schalten Ampeln in Hannover auf Grün“
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 Kritische Sicherheitslücken an Maschinen und Anlagen und Kontaktstandard security.txt; https://cert.dguv.de

Die neue Maschinenverordnung – Konsequenzen für die harmonisierte Normung

In wohl kaum einem anderen Industriesektor haben Normen eine ähnlich hohe Bedeutung wie im Maschinenbau. Die neue EU-Maschinenverordnung stellt die Normenausschüsse vor die große Aufgabe, die Normen auf ihre Konformität mit der neuen gesetzlichen Grundlage zu überprüfen und ggf. Maßnahmen zu ihrer Anpassung vorzunehmen.

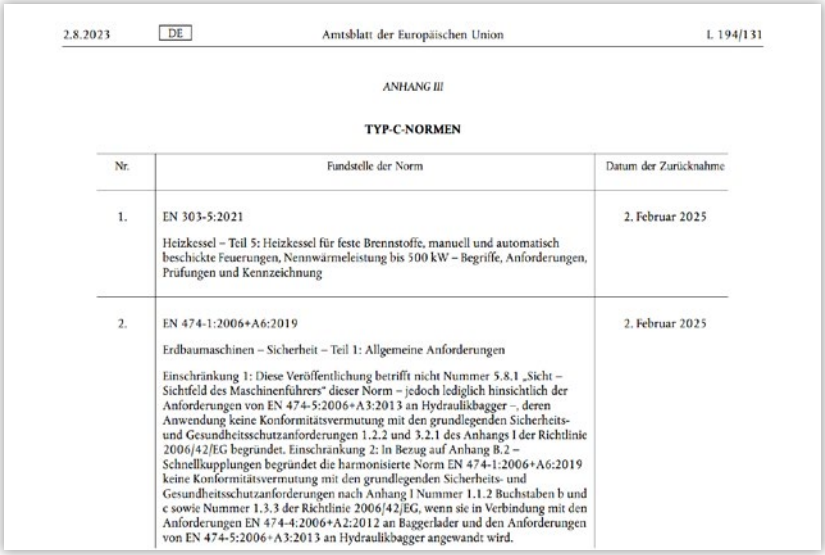
Das hohe Sicherheitsbedürfnis der Anwender beim Umgang mit Maschinen – in Kombination mit der Vielfalt an Maschinentypen – hat über die Jahre zu der erstaunlich großen Anzahl von mehr als 800 harmonisierten Normen unter der europäischen Maschinenrichtlinie geführt. Ihre Anwender dürfen davon ausgehen, dass die darin enthaltenen Lösungen und Maßnahmen geeignet sind, die gesetzlichen Anforderungen der Verordnungen oder Richtlinien zu erfüllen, für welche sie erarbeitet wurden. Von diesen über 800 Normen befassen sich etwa 100 sogenannte B-Normen mit bestimmten Sicherheitsaspekten oder Schutzeinrichtungen, die eine Vielzahl von Maschinen betreffen. Mehr als 700 Normen beschreiben Anforderungen und technische Lösungen für konkrete Maschinentypen (C-Normen). Im Zusammenspiel zwischen Maschinenrichtlinie und harmonisierten Normen hat sich über die Jahre ein bewährtes System etabliert, welches für Maschinenprodukte ein weltweit anerkanntes hohes Sicherheitsniveau gewährleistet.

Normung steht vor einer Mammutaufgabe

Mit der am 29. Juni 2023 im Amtsblatt der EU veröffentlichten neuen Verordnung (EU) 2023/1230 über Maschinen (MaschVO) hat die EU-Kommission nun ein neues gesetzliches Kapitel aufgeschlagen. Die Maschinenverordnung löst zum 20. Januar 2027 per Stichtagsregelung – also ohne Übergangsfrist – die aktuell noch gültige Maschinenrichtlinie 2006/42/EG (MRL) ab. Neben zahlreichen formellen und konzeptionellen Anpassungen des Rechtstexts wurden auch im Anhang I der MRL, der die wesentlichen Sicherheitsanforderungen (EHSR – Essential Health and Safety Requirements) beschreibt, signifikante Änderungen vorgenommen. In der MaschVO finden sich die EHSR im neuen Anhang III. Die Erfüllung dieser Sicherheitsanforderungen ist die Hauptaufgabe der harmonisierten Normen. Durch die Änderungen stellen sich unweigerlich folgende Fragen:

Welche unmittelbaren Auswirkungen haben die neuen und veränderten EHSR auf die Inhalte der heutigen harmonisierten Normen? Und können die unter der MRL harmonisierten Normen unter der MaschVO weiterverwendet werden und behalten sie ihre Konformitätsvermutung?

Die Beantwortung der ersten Frage ist nicht trivial, denn die praktische bzw. normative Umsetzung der neuen EHSR „Schutz gegen Korrumpierung“, „Überwa-



2.8.2023 DE Amtsblatt der Europäischen Union L 194/131

ANHANG III

TYP-C-NORMEN

Nr.	Fundstelle der Norm	Datum der Zurücknahme
1.	EN 303-5:2021 Heizkessel – Teil 5: Heizkessel für feste Brennstoffe, manuell und automatisch beschickte Feuerungen, Nennwärmeleistung bis 500 kW – Begriffe, Anforderungen, Prüfungen und Kennzeichnung	2. Februar 2025
2.	EN 474-1:2006+A6:2019 Erdbaumaschinen – Sicherheit – Teil 1: Allgemeine Anforderungen Einschränkung 1: Diese Veröffentlichung betrifft nicht Nummer 5.8.1 „Sicht – Sichtfeld des Maschinenführers“ dieser Norm – jedoch lediglich hinsichtlich der Anforderungen von EN 474-5:2006+A3:2013 an Hydraulikbagger –, deren Anwendung keine Konformitätsvermutung mit den grundlegenden Sicherheits- und Gesundheitsschutzanforderungen 1.2.2 und 3.2.1 des Anhangs I der Richtlinie 2006/42/EG begründet. Einschränkung 2: In Bezug auf Anhang B.2 – Schnellkupplungen begründet die harmonisierte Norm EN 474-1:2006+A6:2019 keine Konformitätsvermutung mit den grundlegenden Sicherheits- und Gesundheitsschutzanforderungen nach Anhang I Nummer 1.1.2 Buchstaben b und c sowie Nummer 1.3.3 der Richtlinie 2006/42/EG, wenn sie in Verbindung mit den Anforderungen EN 474-4:2006+A2:2012 an Baggerlader und den Anforderungen von EN 474-5:2006+A3:2013 an Hydraulikbagger angewandt wird.	2. Februar 2025

Mögliche Lösung für harmonisierte Normen unter der EU-Maschinenverordnung: Listung im Amtsblatt mit Einschränkung der Vermutungswirkung, ähnlich wie bei formellen Einwänden

chungsfunktion bei autonomen mobilen Maschinen“ oder „Vermeidung des Risikos des Kontakts mit stromführenden Freileitungen“ wird im Detail noch intensiv diskutiert.

Ein grober Überblick über die Geltungsbereiche der Normen zeigt aber: Kaum eine Maschinengattung dürfte von den neuen oder stark veränderten EHSR komplett unberührt bleiben. Es müssten also sämtliche harmonisierten Normen auf die Relevanz der neuen EHSR überprüft und im Falle ihrer Betroffenheit sowohl inhaltlich als auch formell gemäß den Verfahrensregeln der EU-Kommission (tabellarischer Anhang ZA, datierte Verweise) angepasst werden. Dazu wäre theoretisch eine Überarbeitung nahezu aller rund 800 harmonisierten Normen erforderlich – jeweils einschließlich der umfangreichen Assessments durch die HAS-Consultants. Eine Aufgabe, die in den verbleibenden dreieinhalb Jahren bis zur verbindlichen Anwendung der MaschVO völlig unrealistisch ist.

Eingeschränkte Listung als mögliche Zwischenlösung

Daher plant die EU-Kommission – Stand August 2023 – in einer außerordentlichen Aktion, sämtliche europäischen Normen (sowohl EN als auch EN ISO), die zu einem noch zu bestimmenden Zeitpunkt in der ersten Jahreshälfte 2026 unter der MRL harmonisiert sind, en bloc als harmonisierte Normen unter die neue MaschVO zu transferieren. Einzige Einschränkung: Diese Normen können natürlich nur für jene EHSR eine Harmonisierung gewährleisten, die sie auch schon unter der MRL adressieren. Um dies bei der Listung im Amtsblatt für Normennutzer kenntlich zu machen, wird es unerlässlich sein, dass die verantwortlichen Technischen Komitees (TCs) ihr jeweils gesamtes Normenportfolio einer Überprüfung (NICHT notwendigerweise einer Überarbeitung) unterziehen, um die jeweiligen Lücken zur neuen MaschVO zu identifizieren. Gleichzeitig werden bei CEN und CENELEC Arbeiten gestartet, um normative Lösungen zu den neuen bzw. signifikant modifizierten EHSR zu erstellen, so dass die identifizierten Lücken geschlossen werden können.

Derzeit wird mithilfe des koordinierenden CEN/CENELEC-Sektorforums „Machinery“ eine Handlungsanleitung erstellt, um den TCs Hilfestellung bei dieser sehr ambitionierten Aufgabe zu geben. Die Anleitung soll spätestens gegen Ende 2023 verfügbar sein.

Natürlich ist es bereits heute möglich und ratsam, bei anstehenden Normrevisionen oder neuen Projekten die Konformität mit der neuen MaschVO anzustreben. Somit ist zu hoffen, dass bis Anfang 2027 tatsächlich ein gewisser Anteil von Normen an die neue MaschVO angepasst ist. Für das Gros der harmonisierten Normen wird dies aber erst möglich sein, wenn die MaschVO bereits angewendet werden muss.

Ein genauerer Zeitrahmen zu zukünftigen Normenrevisionen wird mit dem neuen Normungsauftrag der Europäischen Kommission zur MaschVO erwartet, der im kommenden Jahr verfügbar sein soll. Im Gegensatz zu den früheren Mandaten ist dieser Normungsauftrag zeitlich begrenzt (vermutlich zwischen 5 und 10 Jahren). Er bildet die juristische Basis, auf deren Grundlage harmonisierte Normen unter der neuen MaschVO erstellt werden dürfen. Seit Ende Juni ist ein erster Entwurf des Normungsauftrags veröffentlicht. Die Kommentare der interessierten Kreise werden voraussichtlich im Herbst in den zuständigen Kommissionsgremien diskutiert.

Als weitere Maßnahme soll schließlich der Übergang der harmonisierten Normen von der MRL zur MaschVO für Normanwender erleichtert werden. Normen, welche von 2024 bis zur 1. Hälfte 2026 veröffentlicht werden, sollen mit zwei Anhängen ZA ausgestattet werden – je einem für die MRL und einem für die MaschVO – aus denen hervorgeht, welche Abschnitte der Norm welche Rechtsvorschriften abdecken. Auch hierzu werden die betroffenen Normen-TCs zeitnah informiert.

All diese beschriebenen Maßnahmen tragen dazu bei, einen möglichst reibungslosen Übergang der harmonisierten Normen von der alten MRL zur neuen MaschVO zu erreichen.

Dr. Frank Wohnsland

VDMA

Vorsitzender des CEN/CENELEC-Sektorforums „Machinery“

frank.wohnsland@vdma.org

Digitale Ergonomie: KAN-Projekt gibt Überblick zum Forschungsstand

Die BioMath GmbH hat im Auftrag der KAN untersucht, wo die Forschung zu Schnittstellen und Datenformaten bei digitalen Menschmodellen und Systemen zur Bewegungserfassung steht.

Im Arbeitsschutz werden digitale Modelle und Methoden zur Planung und Beurteilung von Produkten und Prozessen genutzt. Digitale Menschmodelle simulieren physische Aspekte der Arbeit. Zudem gibt es Systeme, die anhand von Koordinaten der menschlichen Gelenke im dreidimensionalen Raum Bewegungen erfassen. Diese Daten können dann in ein digitales Menschmodell eingespeist werden. Fachleute leiten daraus Maßnahmen für die sichere und gesundheitsgerechte Gestaltung von Arbeitsplätzen ab.

Sowohl Forschungseinrichtungen als auch Unternehmen verfügen über Methoden und Werkzeuge zur Analyse, Beurteilung und Darstellung der Daten aus digitalen Menschmodellen und Systemen zur Bewegungserfassung. Häufig handelt es sich aber um Insellösungen, die aufgrund unterschiedlicher Datenformate untereinander nicht kompatibel sind. Seit den 1960er Jahren wurden rund 150 unterschiedliche digitale Menschmodelle für verschiedene Zwecke entwickelt (die jedoch nicht mehr alle genutzt werden).

Eine Standardisierung der Schnittstellen

- zwischen digitalen Menschmodellen untereinander,
- zwischen Systemen zur Bewegungserfassung untereinander und
- zwischen digitalen Menschmodellen und Systemen zur Bewegungserfassung

wäre für den Arbeitsschutz hilfreich, da eine belastbarere Datengrundlage zur Ableitung von Maßnahmen für die menschengerechte Arbeitsgestaltung geschaffen werden könnte. Mit Hilfe einheitlicher Schnittstellen und Datenformate könnten Bewegungsdaten aus verschiedenen Quellen zusammengefügt und für übergreifende Auswertungen genutzt werden.

KAN-Projekt zeigt Vielfalt der Modelle auf

Im Rahmen eines KAN-Projektes hat die BioMath GmbH wissenschaftliche Publikationen zur digitalen Ergonomie erfasst und ausgewertet. Es galt dabei auch herauszustellen, welche arbeitswissenschaftlichen Erkenntnisse in Bezug auf digitale Menschmodelle und die digitale Erfassung, Bewertung und Darstellung von Bewegungsdaten als gesichert anzusehen sind.

Der Bericht[1] gibt einen Überblick über digitale Menschmodelle und deren Eigenschaften und Möglichkeiten. Die Studie zeigt, dass digitale Menschmodelle auf anthropometrische Maße aus unterschiedlichen Datenbanken zurückgreifen, die verschiedene Bevölkerungsgruppen abbilden. Zudem sind die Daten teils sehr unterschiedlich gruppiert und/oder aufgeschlüsselt. Die Qualität der Daten bestimmt auch die Qualität der digitalen Menschmodelle.

Außerdem wurde analysiert, welche Systeme zur Bewegungserfassung bereits in Studien untersucht wurden. Dabei ging es vorrangig um Möglichkeiten zum Datenaustausch. Hier zeigte die Recherche, dass es bislang kein einheitliches Vorgehen gibt.

In zukünftigen Forschungsprojekten sollten daher u.a. folgende Punkte näher beleuchtet werden:

- Für den Austausch von Daten zwischen digitalen Menschmodellen wäre es sinnvoll, ein herstellerneutrales, gut dokumentiertes, standardisiertes Format zu haben.

- Begriffsdefinitionen und mögliche Detailgrade z.B. für bestimmte Teile eines digitalen Menschmodells sollten festgelegt werden.

- Da es für die Eigenschaften und Konfiguration von Menschmodellen verschiedene Ansätze gibt, wären Festlegungen zur Struktur der Modelle wichtig, die die Vergleichbarkeit fördern.

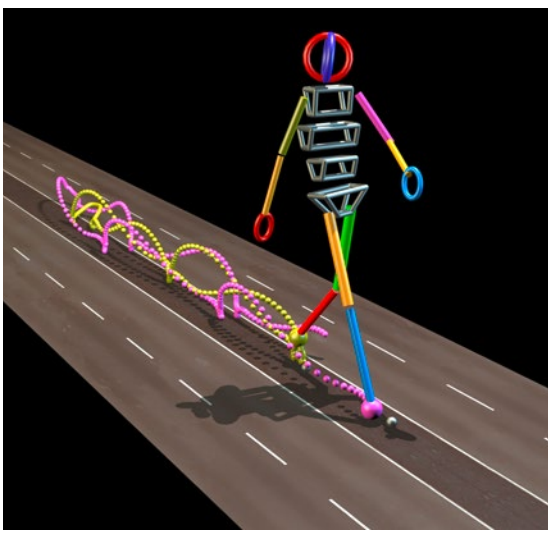
Wie geht es weiter?

Die Projektnehmerin hat die Ergebnisse der Recherche in einem Bericht zusammengefasst, in dem die derzeitige Ausgangslage und Ansätze zur Harmonisierung einheitlicher Schnittstellen und Datenformate beschrieben werden. Die Inhalte dieses Berichts sollen in Form eines technischen Reports (DIN/TR) verfügbar gemacht werden. Dazu wird die KAN den Text aufbereiten und einen Antrag bei DIN stellen. Langfristiges Ziel ist es, grundlegende Normen für digitale Menschmodelle, Schnittstellen und Datenformate zu schaffen. Eine vollständige Harmonisierung der Anforderungen ist aus Sicht der KAN jedoch aktuell noch nicht möglich.

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



Der ASGA – ein neuer Ausschuss für übergreifende Arbeitsschutzthemen

Der staatliche Ausschuss für Sicherheit und Gesundheit bei der Arbeit (ASGA) kam 2021 zu den bestehenden Arbeitsschutzausschüssen beim Bundesministerium für Arbeit und Soziales (BMAS) hinzu. Was sind seine Aufgaben und was war der Anlass für seine Gründung?

Die staatlichen Ausschüsse[1] sind in Deutschland dafür zuständig, (technische) Regeln zu erarbeiten, die die allgemeinen Schutzziele der Einzelverordnungen unter dem Arbeitsschutzgesetz konkretisieren. Koordiniert von der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) behandeln sie potentielle Gefährdungsfaktoren des Arbeitssystems wie Gefahrstoffe, Biostoffe, Arbeitsstätten und Betriebsmittel. Die Regeln stellen Arbeitgebern prozess- und gestaltungsbezogene Anforderungen bereit, mit deren Einhaltung die Inhalte der Einzelverordnungen zum Arbeitsschutzgesetz erfüllt werden (Vermutungswirkung).

Durch die Diversifizierung der Arbeitsformen, die Digitalisierung und klimabedingte Einflüsse auf die Arbeitsumgebung ist die bisher konsequent vertikal ausgerichtete Vorgehensweise der Regelsetzung nicht mehr ausreichend, um die aktuellen und zukünftigen Einwirkungen auf die Beschäftigten umfassend zu beurteilen und geeignete Maßnahmen abzuleiten. Auch bei klassischen Themen wie der Gefährdungsbeurteilung und der Unterweisung sind die Anforderungen unabhängig von einzelnen Gefährdungsfaktoren und sollten damit auch aus mehreren Perspektiven (horizontal) betrachtet werden.

Während der Corona-Krise und den damit einhergehenden neuen Herausforderungen an den betrieblichen Arbeits- und Gesundheitsschutz wurde dieser Bedarf besonders offensichtlich. Die SARS-CoV-Regel war die erste Regel, die gezielt faktorenübergreifend ausgelegt wurde. Der erfolgreiche betriebliche Einsatz dieser Regel machte deutlich, dass es sinnvoll ist zu prüfen, für welche weiteren Themenbereiche die Erarbeitung horizontaler Regeln für den betrieblichen Arbeits- und Gesundheitsschutz zielführend ist.

Aus diesem Grund verankerte die im Dezember 2020 veröffentlichte Ergänzung des § 24 a den ASGA[2] direkt im Arbeitsschutzgesetz. Zu den Aufgaben des neuen Ausschusses gehört es unter anderem – soweit kein anderer staatlicher Ausschuss zuständig ist – Regeln und Erkenntnisse zu erarbeiten, wie die im Arbeitsschutzgesetz gestellten Anforderungen erfüllt werden können.

Ein zweiter Anlass zur Etablierung des neuen Ausschusses ist der Mangel an Kohärenz im bestehenden Regelwerk, der mit der streng vertikalen Ausrichtung der etablierten Ausschüsse zusammenhängt. Bereits im Jahr 2011 formulierte das „Leitlinienpapier zur Neuordnung des Vorschriften- und Regelwerks im Arbeitsschutz“ das Anliegen, das autonome Satzungsrecht der Unfallversicherungsträger und das staatliche Regelwerk inhaltlich besser abzustimmen – sowohl miteinander als auch innerhalb der beiden Regelungsbereiche. Der Weg dahin ist in zentralen Handlungsfeldern, wie z. B. der Gefährdungsbeurteilung, immer noch nahezu unbetreten. Es besteht Konsens innerhalb des ASGA, dieses Anliegen konsequent in den Blick zu nehmen.

Zusammensetzung und Arbeitsweise

Die Zusammensetzung des ASGA unterscheidet sich nicht von jener anderer Arbeitsschutzausschüsse. Im Ausschuss sind vom BMAS berufene Fachleute der öffentlichen und privaten Arbeitgeber, der Gewerkschaften, der Landesbehörden, der gesetzlichen Unfallversicherung und der Wissenschaft vertreten. Dem Ausschuss gehören 15 Mitglieder und 15 stellvertretende Mitglieder an.

Die Ausschussvorsitzende koordiniert neben der Leitung des ASGA auch die Zusammenarbeit aller Arbeitsschutzausschüsse in einem Steuerkreis. Dieses Gremium übernimmt eine zentrale Funktion bei der Erarbeitung fachübergreifender, horizontaler Regeln. Die Ausschüsse bringen ihre fachbezogene Expertise über mandatierte Personen direkt in die jeweiligen Projektgruppen ein. Sie sind so von der Erarbeitung der Projektskizze bis zur Verabschiedung der neuen Regel unmittelbar eingebunden. Das ist ein Novum.

Der ASGA tagt zwei Mal im Jahr. Der Steuerkreis fasst seine Argumente und Voten in entsprechende Empfehlungen und legt diese dem ASGA-Koordinierungskreis vor. Der Koordinierungskreis sondiert die aktuellen Themen und Aufgaben und bereitet die Beschlussvorlagen für die ASGA-Sitzungen vor.

Projekte und Schwerpunkte

Der ASGA hat sich – wie alle anderen Ausschüsse auch – ein Arbeitsprogramm für die aktuelle Berufungsperiode gegeben. Kernthemen sind die Gefährdungsbeurteilung, psychische Belastungen, effiziente und zeitgemäße Unterweisungen, ortsflexible Bildschirmarbeit außerhalb von Arbeitsstätten und Auswirkungen des Klimawandels auf Sicherheit und Gesundheitsschutz bei der Arbeit. Ziel ist die Entwicklung von staatlichen Regeln, die sich kohärent in das bestehende Regelwerk einfügen.

Herausforderungen gibt es aktuell zahlreiche, denn Veränderungsprozesse laufen nie ganz reibungslos ab. Ziel ist es, den richtigen Weg in eine gute, wertschätzende Ausschusskultur zu finden, um im Konsens das ambitionierte Arbeitsprogramm zu erfüllen. Der ASGA-Vorsitz muss zudem die Entwicklung geeigneter und transparenter Prozesse und Handlungshilfen vorantreiben, die diese Kulturentwicklung unterstützen.

Die Projektgruppe „Gefährdungsbeurteilung“ arbeitet bereits an der Konzeptionierung und inhaltlichen Ausgestaltung einer ASGA-Regel. Die Projektgruppe „Psychische Belastung“ wird voraussichtlich noch in diesem Jahr ihre Arbeit antreten.

Prof. Dr. Anke Kahl

Lehrstuhl für Arbeitssicherheit der Bergischen Universität Wuppertal

Vorsitzende des ASGA

1 www.bmas.de/DE/Arbeit/Arbeitsschutz/Arbeitsschutzausschuesse/arbeitsschutzausschuesse.html
2 www.baua.de/DE/Die-BAuA/Aufgaben/Geschaeftsfuehrung-von-Ausschuessen/ASGA/ASGA_node.html

Reform des EU-Produkthaftungsrechts

Die EU-Kommission hat im Herbst 2022 eine Modernisierung der EU-Produkthaftungsregelungen angestoßen. Nachdem sie Entwürfe für eine novellierte Produkthaftungsrichtlinie und eine neue KI-Haftungsrichtlinie veröffentlicht hat, beschäftigen sich EU-Ministerrat und Parlament damit nun intensiver.

Der Übergang in das digitale Zeitalter macht eine Anpassung nicht nur der Rechtsvorschriften für das Inverkehrbringen, sondern auch des Haftungsrechts erforderlich. Die alte Produkthaftungsrichtlinie, immerhin von 1985, die in Deutschland 1989 mit Erlass des Produkthaftungsgesetzes umgesetzt wurde, ist nicht mehr in der Lage, alle durch Produkte verursachten Schäden abzudecken. Resultat sind Rechtsunsicherheiten für Unternehmen und eine zunehmende Anzahl von Produkten, bei denen der Verbraucher keinen Rechtsanspruch auf Kompensationen für durch das Produkt verursachte Schäden hat.[1] Daneben soll die Richtlinie an die kürzlich aktualisierte Produktsicherheitsverordnung und an die Marktüberwachungsverordnung angeglichen werden.

Mehr Produkte und Schadensfälle im Fokus

Es ist davon auszugehen, dass die neue Produkthaftungsrichtlinie auf alle Arten von Produkten anwendbar sein wird – auch solche, die bisher nicht erfasst waren. Darunter fallen dann z.B. auch smarte Produkte, Softwareupdates, KI-Systeme und digitale Services, aber auch wiederaufbereitete Produkte und solche, die wesentlich modifiziert wurden. Hersteller der Kreislaufwirtschaft werden jedoch nicht für Schäden haften müssen, die durch nicht-modifizierte Teile des Produktes entstanden sind.

Bei Produkten aus Drittstaaten, die z.B. per Onlinehandel direkt von Verbrauchern in die EU importiert werden, werden Haftungsansprüche ausgeweitet. Zusätzlich zu den derzeit haftenden Importeuren gelten sie künftig für Herstellervertreter und weitere Akteure wie Online-Plattformen, die in der EU ansässig sind. Zudem sind prozessrechtliche Änderungen vorgesehen: Um die Informationsasymmetrie zwischen Hersteller und Verbraucher zu verringern, können die Wirtschaftsakteure zur Offenlegung von Beweismitteln verpflichtet werden. Insgesamt wird es eine deutliche Beweiserleichterung zu Gunsten der Geschädigten geben, jedoch ohne dass es zu einer Beweislastumkehr kommt. Die bisher vorgesehenen Grenzen zu Haftungshöchstbetrag und Selbstbeteiligung fallen im Entwurf weg.

Angepasste Haftungsregelungen

Ersatzansprüche auf Grundlage des Entwurfs der Produkthaftungsrichtlinie entstehen nur bei Personenschaden (einschließlich psychischer Gesundheitsschäden), Sachbeschädigung und Datenverlust. Es handelt sich um eine strenge Produkthaftung, die verschuldensunabhängig gegen den Hersteller und weitere Wirtschaftsakteure greift. Ansprüche können nur von natürlichen Personen geltend gemacht werden und auch nur, wenn das Produkt nicht ausschließlich für berufliche Zwecke genutzt wird.

Neue KI-Haftungsrichtlinie ergänzt den Rechtsrahmen

Begleitet werden soll die neue Produkthaftungsrichtlinie durch eine KI-Haftungsrichtlinie. Sie soll es Geschädigten im Falle von Schäden durch KI-Systeme deutlich erleichtern, ihre Ansprüche auf einer anderen Rechtsgrundlage als dem Produkthaftungsrecht geltend zu machen, z.B. bei Grundrechtsverletzungen oder zivilrechtlichen Haftungsregelungen.

Um eine Rechtzersplitterung zwischen den EU-Mitgliedsstaaten zu verhindern, soll ein harmonisierter Rechtsrahmen für die Haftung von Herstellern, Betreibern oder Nutzern von Künstlicher Intelligenz vorgegeben werden. Es ist vorgesehen, dass bei Schadensfällen die KI als verursachend angenommen wird. Geschädigte müssen dann nur noch zeigen, dass Anbieter, Betreiber oder Nutzer der KI eine relevante Verpflichtung schuldhaft nicht eingehalten haben und ein Kausalzusammenhang wahrscheinlich ist. Zudem sollen die Hersteller oder Zulieferer von Hochrisiko-KI verpflichtet werden, im Falle eines Prozesses alle relevanten Produktinformationen bereitzustellen.

Die KI-Haftungsrichtlinie allein bietet noch keine rechtlichen Schadenersatzansprüche, sondern sie ergänzt bestehende nationale verschuldensabhängige Haftungsregelungen bei Rechtsverletzungen durch KI. Die neuen, verschuldensabhängigen Haftungsregelungen erlauben eine vereinfachte Geltendmachung von Schadenersatzansprüchen, auf die sich alle natürlichen und juristischen Personen berufen können.

Verhandlung in den EU-Institutionen

Der EU-Ministerrat hat sich bereits mit dem Kommissionsentwurf der Produkthaftungsrichtlinie befasst und stimmt diesem weitgehend zu. Die Diskussion im Europäischen Parlament ist ebenfalls angelaufen, wird aber noch einige Monate in Anspruch nehmen. Die KI-Haftungsrichtlinie soll erst in einem zweiten Schritt verhandelt werden.

Freeric Meier

meier@kan.de

1 Evaluierungsstudie und Richtlinienvorschläge: https://ec.europa.eu/commission/presscorner/detail/de/ip_22_5807

UK verlängert Gültigkeit der CE-Kennzeichnung

Das Ministerium für Wirtschaft und Handel des Vereinigten Königreichs hat angekündigt, die Anerkennung der CE-Kennzeichnung für Produkte, die in Großbritannien (England, Schottland, Wales) auf den Markt gebracht werden, auf unbestimmte Zeit über Dezember 2024 hinaus zu verlängern. Für Nordirland war dies bereits zuvor der Fall. Die Regelung gilt für 18 Verordnungen im Zuständigkeitsbereich des Ministeriums, unter anderem für Maschinen, persönliche Schutzausrüstung, Druckgeräte, Niederspannungsgeräte, ATEX und Gasgeräte.

Ursprünglich sollte die Anerkennung der CE-Kennzeichnung in Großbritannien Ende 2024 auslaufen und durch eine verpflichtende UKCA-Kennzeichnung (UK Conformity Assessed) abgelöst werden. Mit der neuen Regelung können Unternehmen künftig zwischen beiden Kennzeichnungen wählen. Dies ist sowohl für Unternehmen in der EU als auch für britische Unternehmen von Vorteil, da sie ihre Produkte nicht doppelt zertifizieren lassen müssen, um sie in den jeweils anderen Wirtschaftsraum zu exportieren.

Weitere Informationen (auf Englisch): www.gov.uk/government/news/uk-government-announces-extension-of-ce-mark-recognition-for-businesses

Neue Kampagne der EU-OSHA

Die Europäische Agentur für Sicherheit und Gesundheit am Arbeitsplatz (EU-OSHA) startet im Oktober 2023 ihre zweijährige Kampagne „Sicher und gesund arbeiten in Zeiten der Digitalisierung“. Die EU-OSHA und ihre nationalen Kontaktpunkte organisieren eine Vielzahl von europäischen und nationalen Veranstaltungen, um bei Beschäftigten, Unternehmen, und politischen Entscheidungsträgern das Bewusstsein für Sicherheit und Gesundheit bei der Arbeit zu schärfen.

Inhaltliche Schwerpunkte der Kampagne sind die Arbeit auf digitalen Plattformen, Automatisierung von Aufgaben, mobiles und hybrides Arbeiten, Personalmanagement mit Hilfe künstlicher Intelligenz und intelligente digitale Systeme. Ziel ist es, zu diesen Themen Daten und Fakten zur Verfügung zu stellen, die die Entwicklung relevanter Rechtsvorschriften, Leitlinien, Sensibilisierungs- und Unterstützungsmaßnahmen sowie neuer Dienstleistungen und Produkte befördern können.

Informationen zur Kampagne: https://healthy-workplaces.osha.europa.eu/de

A+A 2023: Die KAN ist dabei!

Vom 24. bis 27. Oktober 2023 findet die Fachmesse A+A in Düsseldorf statt. Die KAN befindet sich auf dem Gemeinschaftsstand der DGUV, der sich in diesem Jahr zum ersten Mal in Messehalle 5, Stand 5C06 dem Publikum zeigt. Wir informieren Sie über unsere aktuellen Arbeitsgebiete wie fahrerlose selbstfahrende Maschinen, Infektionsschutzmasken oder Gasgrills, stellen Ihnen unsere Publikationen vor und beantworten gern Ihre Fragen rund um Arbeitsschutz und Normung.

„Genormter Mensch – Körpermaße im Wandel“ ist das KAN-Thema in der „Sprech-Stunde Sicherheit und Gesundheit“ am Donnerstag, 26. Oktober um 10 Uhr auf der Bühne des DGUV-Gemeinschaftsstandes.

Auf dem zeitgleich stattfindenden A+A-Kongress ist die KAN mit folgenden Vorträgen vertreten:

- 25. Oktober 2023: VISION ZERO versus Standardization: A Position Statement
- 26. Oktober 2023: Arbeitsschutzrelevante Managementnormen abseits der ISO 45001

Wir freuen uns auf Ihren Besuch!

Weitere Informationen zum Programm finden Sie unter www.aplusa.de.

Normungsarbeit im Arbeitsschutz – Grundlagen- und Aufbauseminar

In Zusammenarbeit mit dem Institut für Arbeit und Gesundheit der DGUV (IAG) bietet die KAN zwei Seminare zur Normungsarbeit im Arbeitsschutz an.

Das **Grundlagenseminar** richtet sich an aktive Mitglieder von Normungsgremien und an alle, die sich zum Nutzen von Sicherheit und Gesundheit mit der Normung befassen möchten. Sie lernen im Seminar die Abläufe der Normenerarbeitung und Ihre Einflussmöglichkeiten in den verschiedenen Phasen kennen. Tipps, Tricks und der Austausch untereinander unterstützen Sie bei der erfolgreichen Mitarbeit in der Normung. Das Grundlagenseminar findet vom 25. bis 27. Oktober 2023 in Dresden statt.

Sie kennen sich mit den Grundlagen der Normungsarbeit gut aus und wollen Ihre Kompetenzen erweitern? Im **Aufbausemi-nar** treffen Sie auf andere erfahrene Normungsexpertinnen und -experten und überlegen gemeinsam, mit welchen Strategien Sie Ihre (Mit)arbeit weiter optimieren können. Sie tauschen Erfahrungen über den Normungsprozess und die Möglichkeiten der Einflussnahme aus und erhalten aktuelle Informationen aus dem Bereich der Normung.

Die Präsenzphase des Aufbauseminars findet am 5. und 6. Dezember 2023 in Dresden statt. Die weiteren Seminarteile sind online oder als Selbstlernphase geplant.

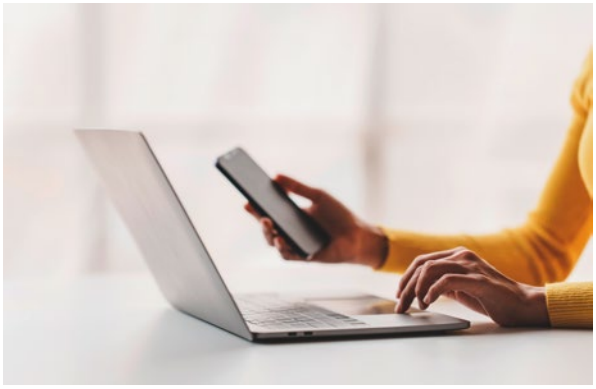
Informationen und Anmeldung: https://asp.veda.net/webgate_dguv_prod, Veranstaltungsnummer 570044 (Grundlagen) und 570139 (Aufbau)

Europäische Änderungen an IEC-Normen

Elektrotechnische Normen sollen nach dem Frankfurter Abkommen bevorzugt auf internationaler Ebene bei IEC erarbeitet und parallel von CENELEC als identische europäische Normen (EN IEC) übernommen werden. In manchen Fällen sind jedoch bei der Übernahme von IEC-Normen europäische Änderungen notwendig, um Anforderungen der Binnenmarktrichtlinien oder -verordnungen zu genügen.

Dass eine solche Abweichung vorliegt, ist daran erkennbar, dass CENELEC diese Normen dann nicht als **EN IEC** 6xxxx, sondern nur als **EN** 6xxxx herausgibt – jedoch mit der gleichen Nummer wie bei IEC.

Content



© Suphakant - stock.adobe.com

Lead topic

Themes

© Arto - stock.adobe.com

© M.Dörr & M.Frommherz - stock.adobe.com

Stay up to date:

www_kan_de

Kommission Arbeitsschutz und Normung (KAN)

KAN_Arbeitsschutz_Normung

KAN – Kommission Arbeitsschutz und Normung

Benjamin Pfalz
Chairman of KAN
German Metalworkers' Trade Union
(IG Metall)

Cybersecurity: a challenge for both regulators and companies

The need for companies to protect themselves against cyberattacks is greater than ever. The issue has long had implications for occupational safety and health. Owing to the interaction between human beings and machines, remote-controlled work equipment, networked production facilities and the increasing use of machine learning, cybersecurity must be considered more and more often in the course of risk assessments within companies. Product safety measures are a particular aspect here.

These aspects are increasingly being addressed in regulations and codes. For example, for measurement, control and regulation devices with a bearing on safety, the TRBS 1115 Technical Rule supports the German Ordinance on Industrial Safety and Health (BetrSichV) with regard to identification and specification of the required cybersecurity measures. The issue is also addressed by the new EU Machinery Regulation and the upcoming AI Regulation. The EU Cyber Resilience Act has been initiated to regulate the placing on the market of intermediate and end products employing digital elements.

It now falls to the standardization sector to provide appropriate support for the regulation level. The standardization mandate in support of the draft of the AI Regulation addresses the topic of cybersecurity clearly. The European standards organizations are already responding to this by reviewing the existing body of standards and how the topic can be addressed within their structures.

It is crucial that the voice of occupational safety and health be heard during this process. KAN is therefore addressing the topic at all levels. This includes holding an expert discussion on OSH-related standardization in the context of the AI Regulation before the end of the current year. **«**

EU Regulation: world of networked equipment and machinery to be made more secure

With the Cyber Resilience Act, the European Commission is planning to oblige manufacturers of products "with digital elements" to guarantee cybersecurity throughout their products' life cycle in the future.

Against a continued backdrop of online attacks, for example involving encryption trojans (ransomware), the European Commission is continuing to push for safeguards against IT security vulnerabilities. Following adoption of legislation such as the Cybersecurity Act (2019), which lays the groundwork for an EU-wide certification scheme for the IT security of networked equipment, systems and services, and the recent amendment of the Network and Information Security Directive (NIS2), the Commission published a draft of a Cyber Resilience Act (CRA)[1] in September 2022. According to the planned regulation, products "with digital elements" such as hardware and software should "be placed on the market with fewer vulnerabilities“ in the future.

The draft is broad in its scope. For example, the Commission intends it to cover "any software or hardware product and its remote data processing solutions", including associated components, even where they are placed on the market separately. One focus is likely to be on the Internet of Things, or small private routers which have often been vulnerable to attack owing to numerous inherent security vulnerabilities. Products "developed exclusively for national security or military purposes" or those specifically designed to process classified information are to be excluded from the act. Sectors such as aviation, medical devices and motor vehicles are also not affected, as requirements specifically governing them already exist.

The proposal foresees affected manufacturers being required to meet basic cybersecurity requirements for the design, development and manufacturing process before placing a device on the market. They must ensure that vulnerabilities are monitored throughout the device's entire life cycle and eliminated through updates made available automatically and at no cost. The proposal also includes an obligation for manufacturers to report any incident affecting the security of a piece of hardware or software to ENISA, the EU's cybersecurity agency, by a tight, 24-hour deadline. A coordinated policy on vulnerability disclosure is to be established.

Vulnerabilities on devices covered would have to be constrained in accordance with the CRA and the impact of incidents minimized. The products covered are to ensure the confidentiality of data, for example by means of encryption. Protection of the integrity and processing of information and measurement data that are essential for the functioning of an item is to become mandatory.

Beyond these basic requirements, the European Commission has identified particularly critical high-risk areas. It divides the products concerned into two classes, for each of which a different conformity procedure is to be introduced. Class I includes identity management systems, browsers, password managers, anti-virus programs, firewalls, virtual private networks (VPNs), network management, comprehensive IT systems, physical network interfaces, routers and chips. It further covers operating systems, for example for smartphones and desktop computers, microprocessors, and the Internet of Things (IoT) in companies that are not considered particularly vulnerable.

The higher risk class II includes desktop and mobile devices, operating systems that are virtualized or integrated for example into machines, digital certificate issuers, general purpose microprocessors, smartcard readers, robot sensing components and smart meters. It also covers IoT devices, routers and firewalls for industrial use, which is generally considered a "sensitive environment." The background to this is that IT security vulnerabilities have long had large-scale impacts on machinery and systems that, increasingly, are networked and can also be accessed from outside the company premises. As a result, the vulnerabilities also impact upon occupational safety and health.

Manufacturers are to conduct conformity assessments of their products by means of an internal procedure or testing by recognized bodies. Where the manufacturer has relied upon harmonized standards or has already obtained a certificate within a Euro-

pean cybersecurity certification framework, it can be assumed that the hardware or software concerned complies with the regulation. Importers and distributors have an obligation to verify the manufacturer's compliance with the relevant procedures and check the CE marking of the device. For less critical products, manufacturers may prepare a declaration of conformity themselves. In risk class II, assessment by third parties is to be necessary.

The Commission considers the need for action urgent, since by 2021, growing cybercrime had already resulted in estimated annual costs of 5.5 trillion euros. In a networked environment, a cybersecurity incident involving a single product may impact upon an entire company or supply chain, often spreading within minutes across the external borders of the Single Market, as was the case for example with the WannaCry computer malware. As a result, economic and social activities are interrupted, and lives possibly even threatened.

Criticism of the proposed regulation

In a statement[2], the German Social Accident Insurance (DGUV) criticizes that even the core term "cybersecurity" is not clearly defined. At different points in various standards and regulations, the term is used to mean a state, an activity or a product. The DGUV points out that compound terms including "cyber" but not precisely defined are often problematic. For example, depending on the source, attacks conducted across wireless or USB interfaces are not considered under the term "cyber security".

The DGUV is also critical of the obligation for manufacturers to report comprehensive details of a security vulnerability within 24 hours. In many cases, an investigation cannot realistically be conducted within such a short time. It also points out that there is not necessarily any need for details that could be exploited for attacks to be forwarded. In its statement, the DGUV advocates only communicating data actually needed by the

© Suphakant - stock.adobe.com

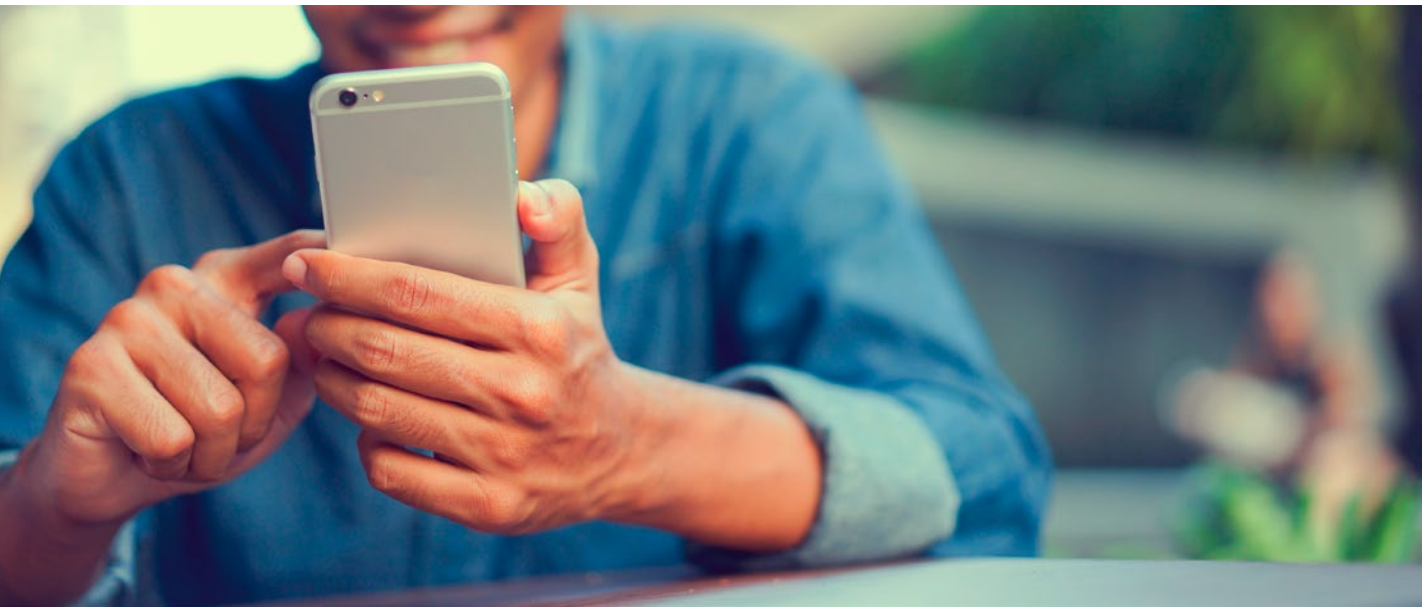
authorities, for example for the issuing of product warnings or assessing the impact of a vulnerability. The German Social Accident Insurance also considers the planned timeframe of two years for adjustment to the new requirements to be too short for manufacturers who are dependent on other products and must await a conformity assessment, for example.

Jonas Stein, head of the DGUV's Security Working Group, also criticizes that the continual, ongoing development of operating systems prevents their being tested in a meaningful way. Furthermore, they are often dependent on open-source software, as in the case of Linux. However, no single manufacturer is responsible for the conformity procedure for "software libre". The open-source community itself fears it may fall into the liability trap, as many individual developers contribute to collaborative works and would all bear liability for potential security gaps. The Free Software Foundation Europe (FSFE) laments that "due to the lack of funding and resources to go through these procedures, some of these projects might have to stop completely".

The EU Council of Ministers and the European Parliament's lead industry committee commented on the Commission's proposal in mid-July, thereby enabling negotiations on a final compromise to begin shortly. The Member States advocate, for example, a simplified declaration of conformity, greater support for small businesses, and clarification by manufacturers of expected product lifetimes. Moreover, exploited vulnerabilities or security incidents should be reported to the relevant national authorities rather than ENISA. For their part, MEPs are calling for more precise definitions, workable timeframes and a fairer distribution of responsibilities. At the same time, they are pushing for smart home devices, smartwatches and home security cameras to be included in the high-risk category.

Dr Stefan Krempl
Freelance journalist
sk@nexttext.de

1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454
2 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services/F3376532_en



© chinnarach - stock.adobe.com

Proven knowledge in new industrial security specifications

Functional safety components protect workers against hazards to their life and health, for example by preventing access to hazardous parts of machinery and systems. Manipulation from outside that could adversely affect safety must also be prevented. This requires thorough observance of generally accepted good practice, and an appropriate response by manufacturers and operators in the event of security exploits.

In order for the safety functions of control systems to be reliably assured, the control system itself must also be both secure, i.e. protected against failure and manipulation. The increasing frequency with which industrial security disasters are now being reported is alarming. There are however grounds for optimism, because almost all security vulnerabilities can in fact be avoided very easily by observance of current good practice, as the following pertinent example shows.

As long ago as 1883, Auguste Kerckhoffs set out six basic requirements for secure, i.e. confidential communication. The second of these requirements was that the system should not require secrecy, and if it were to fall into enemy hands, no adverse consequences should arise. Guglielmo Marconi was evidently not aware of Kerckhoffs' document: secure (confidential) communication by means of his wireless telegraph system depended upon other parties not taking possession of one of the devices or replicating one of them and tuning it to the same frequency. Nevil Maskelyne drew attention to the problem in 1903 by transmitting obscene Morse code messages during Marconi's demonstration, thereby making him one of the first ever hackers. Although secure cryptographic methods are not new, design flaws similar to Marconi's can still be found today, for example in radio controls for traffic light systems[1] or industrial cranes[2].

Harmonized definitions of concepts are lacking

The University of Bremen's navigator for security-related standards[3] includes a database of currently around 800 standards and over 2,000 search hits for legislation. One problem is that the documents use different terms, and do not always define them clearly. While some documents deal comprehensively with security, and specifically with information security, others invent new portmanteau terms beginning with "cyber". These newly created terms must be defined precisely in the document, as they do not have a unique inherent meaning. "Cybersecurity" may refer to an activity, or to a measure taken to protect against attacks from the Internet; at other times it refers to a state in which a product is protected against radio-based attacks.

A better alternative to creating new terms is to work with the unambiguous terms "security" or "information security". Where the term's scope must be limited to radio-based attacks, for example, this restriction should be stated clearly. The EU Machinery Directive has chosen another, very elegant solution by requiring "protection against corruption"[6] in Annex III 1.1.9, and is also clearer on this point than the previous EU Machinery Directive. With this approach, it focuses on the objective of protection, for example that remote access must not lead to a hazardous situation. It does not address in detail how such corruption may be caused.

Fast communication is crucial

Fast and effective communication is a crucial part of an appropriate response to security vulnerabilities. However, the poor state of communication was demonstrated in December 2021, when a security vulnerability in the Log4J software library made headlines. This software library forms part of many industrial components, as well as many server services. Whilst some were blaming incorrect use of the library and arguing that the security issues could have been prevented had the documentation been read, many manufacturers were left wondering whether they were affected by security vulnerabilities. In some cases, they were not able to establish whether their products were affected until several months later.

In summary, the following were lacking:

- An emergency contact point for security within the company
- A standardized format for recommendations for action

Jonas Stein

Head of the DGUV's industrial security laboratory and Head of the DGUV security working group

Jonas.Stein@dguv.de

• In addition, a standard procedure for manufacturers to communicate that a particular product is not affected by a security vulnerability

The lack of harmonized information and interfaces is addressed by a catalogue of open specifications, developed by various consortia of companies, public bodies and organizations, that can be implemented immediately by any company (see table). An emergency contact point according to IETF specification RFC 9116 is stored on the website in a simple security.txt file[4]. A manufacturer can also refer in this file to his list of recommended actions (CSAF). A globally unique identifier (CPE, common platform enumeration) is assigned to each hardware and software product. This enables the international alerts (CVE, common vulnerabilities and exposures) to be referenced automatically to the precise product and version. The criticality of the security vulnerability is classified as closely as possible against a globally standardized index (CVSS, common vulnerability scoring system). The SPDX open specification[9] can be used to document, in machine-readable form, what libraries were used for each project. A program used by the operator can then regularly query for all products whether any security alerts have been issued, and display the recommended actions.

Some large companies are already employing these specifications. It is now crucial that all other companies swiftly follow suit, so that information on security problems is delivered quickly and at low cost.

As a first step, companies should at least ensure that they can be contacted in the event of a security incident, and make an emergency contact public. Instructions are provided at https://cert.dguv.de by which this can be implemented in a matter of minutes.

Open specifications on information security

Input information	Maintained by	Specification
Emergency contact point	Manufacturer, operator	"security.txt" RFC 9116
Product identifier/ID (manufacturer's name, product name, version, language version, etc.)	Manufacturer	CPE
Software bill of materials (SBOM)	Manufacturer	SPDX
Security vulnerability alert	CVE numbering authorities	CVE
Security advisory (recommended action for CVE)	Manufacturer	CSAF
Properties for criticality evaluation	Manufacturer	CVSS

Catalogue of open specifications; together, these will substantially enhance industrial security. In the years ahead, they will step up the urgently needed communication of security vulnerabilities.

1 ARD TV report on hackers switching traffic lights in Hannover to green (2021), 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 Critical security vulnerabilities on machinery and installations, and the security.txt file: https://cert.dguv.de

The new Machinery Regulation and what it means for harmonized standards

In probably no other industrial sector are standards as important as in mechanical engineering. The new EU Machinery Regulation presents the standards committees with the major task of reviewing the standards for their conformity with the new statutory basis and, if necessary, taking measures to bring them into line with it.

The importance of the safety of machinery users and the wide diversity of machine types has led over the years to over 800 harmonized standards being created under the European Machinery Directive, an astonishingly large number. Users of these standards can assume that the solutions and measures described in them enable the legal requirements of the regulations or directives for which they were developed to be satisfied. Among these standards are some 100 "type B" standards, which address specific safety aspects or protective devices affecting a large number of machines. Over 700 standards describe requirements and technical solutions for specific machine types (type C standards). Over the years, the symbiosis between the Machinery Directive and harmonized standards has created a proven system that ensures a high level of safety, recognized worldwide, for machinery products.

Standardization now faces a mammoth task

With publication of the new Regulation (EU) 2023/1230 on machinery in the Official Journal of the EU on 29 June 2023, the European Commission has now opened a new legal chapter. The Machinery Regulation will replace the current Machinery Directive 2006/42/EC on the cut-off date of 20 January 2027, i.e. without a transition period. In addition to numerous formal and conceptual amendments to the legal text, significant changes have been made to Annex I of the Machinery Directive, which describes the essential health and safety requirements (EHSRs). The EHSRs are found in the new Annex III of the Machinery Regulation. Fulfilment of these safety requirements is the main purpose of the harmonized standards. The amendments inevitably raise the following questions:

What immediate consequences do the new and amended EHSRs have for the content of current harmonized standards? Can the standards harmonized under the Machinery Directive continue to be used under the Machinery Regulation, and do they still give rise to a presumption of conformity?

The answer to the first question is not trivial, because practical/normative implementation in detail of the new EHSRs of "Protection against corruption", "Supervisory function" (on autonomous mobile machinery) and "Risk of contact with live overhead power lines" is still the subject of intense discussion.

However, a broad overview of the standards' scope shows that hardly any category of machinery is likely to remain completely unaffected by the new or strongly amended EHSRs. All harmonized standards will therefore need to be reviewed for their relevance to the new EHSRs, and should they be affected, amended in both form and content in accordance with the procedural rules of the European Commission (table in Annex ZA, dated references). Theoretically, this would entail revision of almost all of the approximately 800 standards, including extensive assessments by the HAS Consultants in each case. Completion of this task in the three and a half years that are left before application of the Machinery Regulation becomes mandatory is in no way realistic.

A possible interim solution: conditional listing

For this reason, the European Commission is planning – as at August 2023 – the following exceptional step: all European standards (both EN and EN ISO) that are harmonized under the Machinery Directive at an as-yet unspecified point in time in the first half of 2026 are to be transferred en bloc as harmonized standards under the new Machinery Regulation. The only limitation will be that, obviously, these standards can ensure harmonization only for the EHSRs that they already address under the Machinery Directive. In order to make this clear to standards users when the standards are listed in the Official Journal, it will be essential for each responsible Technical Committee (TC) to subject its entire portfolio of standards to a review

(NOT necessarily a revision) in order to identify the gaps with respect to the new Machinery Regulation. At the same time, work will begin at CEN and CENELEC to produce normative solutions to the new or significantly modified EHSRs to enable the gaps identified to be addressed in normative provisions.

With the support of the coordinating CEN/CENELEC "Machinery" Sector Forum, a guidance document is currently being prepared to assist the TCs in this very ambitious task. The guidance document is to be made available by the end of 2023 at the latest.

It is of course already possible – and advisable – to make conformity with the new Machinery Regulation an objective during new projects or pending revisions of existing standards. It is therefore to be hoped that by the beginning of 2027, a part of the standards will already have been brought into line with the new Machinery Regulation. For the majority of harmonized standards, however, this will not be possible until application of the Machinery Regulation has already become mandatory.

A more precise timeframe on future standards revisions is anticipated with the European Commission's new standardization mandate for the Machinery Regulation, which is expected to be available in the coming year. Unlike previous mandates, the term of this standardization mandate will be limited (probably to between 5 and 10 years). It forms the legal basis by which harmonized standards may be developed under the new Machinery Regulation. The first draft of the standardization mandate was published at the end of June. Comments from stakeholders are expected to be discussed in the autumn in the relevant Commission committees.

Finally, as a further measure, transition of harmonized standards from the Machinery Directive to the Machinery Regulation is to be made easier for users of standards. For standards published between 2024 and the first half of 2026, two Annexes ZA are to be created: one for the Machinery Directive, the other for the Machinery Regulation, showing which sections of the standard cover which parts of the legislation. The affected standard TCs will also be provided with relevant information in due course.

The measures described all contribute to the transition of harmonized standards from the Machinery Directive to the new Machinery Regulation progressing as smoothly as possible.

Dr Frank Wohnsland

VDMA (German mechanical engineering association)

Chair of the CEN/CENELEC "Machinery" Sector Forum

frank.wohnsland@vdma.org

Digital ergonomics: KAN project provides an overview of the current progress of research

BioMath GmbH has been tasked by KAN with examining the current state of research into interfaces and data formats for digital human models and motion capture systems.

Digital models and methods are used in occupational safety and health to plan and assess products and processes. Digital human models simulate physical aspects of work. Systems also exist that use coordinates of human joints to record movements in three-dimensional space; these data can then be fed into a digital human model. Experts use this model to identify measures for safe and healthy workplace design.

Enterprises and research institutes alike possess methods and tools with which data from digital human models and motion capture systems can be analysed, assessed and presented. These are often standalone applications, incompatible with each other owing to their different data formats. Since the 1960s, some 150 different digital human models have been developed for various purposes. (Not all are still in use.)

Standardizing the interfaces would be advantageous for occupational safety and health, as it would enable a more robust body of data to be generated, from which measures for human-centric work design could be created. The interfaces concerned are:

- Between different digital human models
- Between different motion capture systems
- Between digital human models and motion capture systems

Standardized interfaces and data formats would facilitate the merging of kinematic data from multiple sources and their use for generic evaluations.

KAN project reveals diversity of the models

In the course of a KAN project, BioMath GmbH identified and reviewed research publications dealing with digital ergonomics. The aim was to highlight findings concerning human factors relating to digital human models and the digital capture, evaluation and presentation of kinematic data that can be considered validated.

© berCheck - stock.adobe.com

The report[1] provides an overview of digital human models and descriptions of their characteristics and capabilities. The study shows that digital human models retrieve anthropometric data from different databases representing different population groups. In some cases, the databases differ widely in how they group the data or break it down. The quality of the data is decisive for the quality of the digital human models.

The study also analysed what motion capture systems have already been examined in studies. The primary focus here lay on the scope for data interchange. The study revealed that no uniform procedure for this exists at present.

Points to be examined in greater detail by future research projects should therefore include the following:

- A standardized and well-documented non-proprietary format would be advantageous for the exchange of data between digital human models.
- Terminology and possible levels of detail, for example for specific parts of a digital human model, should be defined.
- Since multiple approaches exist for the properties of human models and their configuration, specifications for structuring the models in a way that facilitates comparability are important.

The next step

The project contractor has summarized the results of the survey in a report describing the current situation and approaches to harmonizing interfaces and data formats. The content of the report is to be published in the form of a DIN/TR technical report. For this purpose, KAN will prepare the text and submit an application to DIN. The long-term objective is to develop generic standards for digital human models, interfaces and data formats. In KAN's view, however, full harmonization of the requirements is not possible at the present time.

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

ASGA: a new committee for generic occupational safety and health topics

Germany's state committee for safety and health at work (ASGA) was added to the existing occupational safety and health committees at the Federal Ministry of Labour and Social Affairs (BMAS) in 2021. What are the ASGA's tasks, and why was it created?

In Germany, the state committees[1] are responsible for drawing up technical rules supporting the general objectives of protection of the individual regulations under the German Occupational Health and Safety Act (ArbSchG). This work is coordinated by the German Federal Institute for Occupational Safety and Health (BAuA), and addresses potential hazard factors in the work system such as hazardous substances, biological substances, workplace premises and equipment. The rules describe process and design-related requirements to be met by employers in order for the provisions of the individual regulations under the ArbSchG to be satisfied (presumption of conformity).

Owing to the diversification of forms of work, the digital transformation and climate-related influences on the working environment, the existing, systematically vertical regulatory process is no longer adequate for comprehensive assessment of current and future impacts on employees and for the formulation of suitable measures. For familiar topics such as risk assessment and the provision of instruction, too, the requirements are independent of specific risk factors and should therefore also be considered from multiple perspectives (horizontally).

This need became particularly apparent during the Covid-19 crisis and the challenges it presented for the safety and health of workers at work. The SARS-CoV Rule was the first rule to be purposefully drawn up with consideration for all factors. The success with which this rule was applied in companies clearly demonstrated the benefit of considering other subject areas for which it would be expedient to develop horizontal rules for the safety and health of workers at work.

For this reason, the amendment to Section 24(a) of the ArbSchG published in December 2020 enshrined the ASGA[2] directly within the act. The new committee's tasks include formulating rules and observations by which the requirements set out in the ArbSchG can be met, except where they fall within the responsibility of another state committee.

A second reason for creation of the new committee is the lack of coherence in the existing regulatory framework. This failing is related to the strictly vertical orientation of the established committees. As early as 2011, the guideline paper on the reorganization of the body of occupational safety and health rules and regulations set out the intention of reconciling the content of the state body of rules and regulations and that of regulations under the German Social Accident Insurance Institutions' autonomous charter, both within each of the two regulatory spheres, and between them. In key areas of activity, such as risk assessment, virtually no progress has as yet been made in this area. A consensus exists within the ASGA that this objective should be pursued systematically.

Composition and operation of the ASGA

The composition of the ASGA resembles that of other German occupational safety and health committees. It includes experts appointed by the BMAS from public and private sector employers, the trade unions, the regional administrations, the German Social Accident Insurance and the research community. The committee comprises 15 members and 15 proxies.

Besides heading the ASGA, the committee Chair coordinates, in a steering committee, the work performed jointly by all the occupational safety and health committees. The steering committee assumes a key function in the development of interdisciplinary, horizontal rules. The individual occupational safety and health committees contribute their specialist expertise directly to the respective project groups through appointed representatives. They are thus involved directly, from

production of the project's draft through to the new rule's adoption. This approach is new.

The ASGA meets twice a year. The steering committee formulates its arguments and votes in the form of recommendations and presents them to the ASGA coordinating committee. The coordinating committee sounds out the topical issues and tasks and prepares draft resolutions for ASGA meetings.

Projects and key issues

Like the other committees, the ASGA has set itself a work programme for its current term. Core topics include risk assessment, mental stresses, efficient provision of up-to-date instruction, screen work at changing locations outside work premises, and the impact of climate change on occupational safety and health. The goal is to develop state rules that can be added cohesively to the existing body of regulations.

Since processes of change are never entirely smooth, numerous challenges exist at present. The aim is to create a positive committee culture based on mutual esteem, with which the ambitious work programme can be completed by consensus. The ASGA Chair must also promote the development of suitable and transparent processes and tools that support development of this culture.

The "Risk Assessment" project group is already working on the concept and content of an ASGA rule. The "Mental Stress" project group is expected to assume its work before the end of the year.

Professor Dr Anke Kahl

Department of occupational safety at the University of Wuppertal

Chair of the ASGA

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

Reform of EU product liability legislation

In the autumn of 2022, the European Commission began modernizing EU product liability legislation by publishing drafts for an amended Product Liability Directive and a new AI Liability Directive. The European Council of Ministers and Parliament are now addressing this legislation in greater detail.

© Dzmitry - stock.adobe.com

The transition to the digital age necessitates changes to the legislation governing liability, as well as that governing placing on the market. The existing Product Liability Directive, which dates back to 1985 and was transposed in Germany in 1989 with passing of the German Product Liability Act (ProdHaftG), no longer covers all damage potentially caused by products. This has given rise to legal uncertainty for companies and to a growing number of products in respect of which the consumer has no legal claim to compensation for damages caused by them.[1] In addition, the directive is to be brought into line with the recently updated General Product Safety Regulation and the Market Surveillance Regulation.

Focus on more products and claims

The new Product Liability Directive can be expected to apply to products of all types, including those not covered in the past. It therefore extends for example to smart products, software updates, AI systems and digital services, and also to products that have been refurbished or significantly modified. Manufacturers in the circular economy will, however, not be liable for harm caused by unmodified parts of the product.

Liability is extended to cover products from third countries that are imported into the EU by consumers themselves, for example through the online trade. In addition to importers who already face liability, it will apply in future to manufacturers' representatives and other economic operators such as online platforms that are based in the EU. Procedural changes are also planned: in order to reduce the information asymmetry favouring manufacturers to the detriment of consumers, economic operators can be obliged to disclose evidence. Altogether, the burden of proof will be eased significantly to the benefit of the injured party, but not reversed. The existing limits on liability and excess have been omitted from the draft.

Amended liability provisions

Claims for compensation arising from the new Product Liability Directive in its current draft form apply only in cases of personal injury (including harm to mental health), damage to property and loss of data. This is a strict product liability that applies against the manufacturer and other economic actors regardless of fault. Claims can be made only by natural persons and only where the product is not used exclusively for professional purposes.

New AI Liability Directive added to legal framework

The new Product Liability Directive is to be accompanied by an AI Liability Directive. Where harm is caused by AI systems, the AI Liability Directive is intended to make it substantially easier for injured parties to assert their claims on a legal basis other than product liability law, for example in the event of violations of fundamental rights, or cases falling under civil liability.

To prevent legal fragmentation of the EU Member States, a harmonized legal framework for the liability of manufacturers, operators and users of artificial intelligence is to be set out. It is envisaged that in the event of a claim, the AI will be assumed to have caused the damage. Injured parties need then demonstrate only that the provider, operator or user of the AI culpably failed to comply with a relevant obligation and that a causal link is probable. In addition, manufacturers or suppliers of high-risk AI are to be required to make all relevant product information available in the event of a lawsuit.

The AI Liability Directive does not make provision on its own for legal claims for damages, but complements existing national fault-based liability regimes in the event of legal infringements caused by AI. The new, fault-based liability regimes simplify the assertion of claims for damages for all natural and legal persons.

Negotiation in the EU institutions

The EU Council of Ministers has already considered the Commission's draft of the Product Liability Directive and has largely accepted it. Discussion in the European Parliament has also begun, but will last for several months. The AI Liability Directive is not to be negotiated until the second phase.

Freeric Meier

meier@kan.de

1 Evaluation study and proposals for the directives: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5807

UK extends validity of CE marking

The UK's Department of Business and Trade has announced that recognition of CE marking for products placed on the market in Great Britain (England, Scotland and Wales) is to be extended indefinitely, i.e. beyond December 2024. This was already the case for Northern Ireland. The arrangement applies to 18 regulations falling within the department's responsibility. The products concerned include, inter alia, machinery, personal protective equipment, pressure equipment, low-voltage electrical equipment, ATEX equipment and gas appliances.

Originally, recognition of CE marking in Great Britain was to expire at the end of 2024 and be replaced by mandatory UKCA (UK Conformity Assessed) marking. The new arrangement allows companies to choose between the two labels in the future. This is advantageous both for companies based in the EU and for British companies, as CE marking enables them to have their products certified only once for sale in both economic areas.

Further information: www.gov.uk/government/news/uk-government-announces-extension-of-ce-mark-recognition-for-businesses

New EU-OSHA campaign

In October 2023, the European Agency for Safety and Health at Work (EU-OSHA) will launch its two-year campaign on the subject of safe and healthy work in the context of the digital transformation. EU-OSHA and its national Contact Points are organizing numerous Europe-wide and national events to raise awareness for occupational safety and health among employees, companies and policymakers.

The campaign is focused upon work on digital platforms, automation of tasks, mobile and hybrid work, the use of artificial intelligence in personnel management, and smart digital systems. The goal is to provide data and facts on these topics that can inform the development of relevant legislation, guidelines, measures for support and raising of awareness, and new services and products.

For information on the campaign, visit: https://healthy-workplaces.osha.europa.eu/de

A+A 2023: KAN will be there

The A+A trade fair will be held in Düsseldorf from 24 to 27 October 2023. KAN will be exhibiting on the DGUV's joint stand, which this year will be stand 5C06, located for the first time in Hall 5. We will be there to provide information on our current areas of activity, such as driverless self-propelled machinery, infection protection masks and gas grills, to present our publications, and to answer any questions you may have concerning occupational safety and health and standardization.

"The standardized human being – how human body dimensions are changing" will be the KAN topic in the "Safety and health talks and discussion", which will be held on the stage of the DGUV's joint stand at 10 am on Thursday, 26 October.

KAN will also be present at the A+A Congress, which is taking place at the same time, where it will deliver the following papers:

- 25 October 2023: VISION ZERO versus Standardization: A Position Statement
- 26 October 2023: Management standards relevant to occupational safety and health and beyond ISO 45001

For more information on the programme, visit www.aplusa.de.

We are looking forward to seeing you there!

Seminars on standardization work in occupational safety and health

In conjunction with the Institute for Work and Health of the DGUV (IAG), KAN is running two seminars on standardization work in occupational safety and health (in German).

The **introductory seminar** is intended for active members of standards committees and any party interested in standardization in the interests of safety and health. In this seminar, participants acquire familiarity with the procedures for standards development and their opportunities to exert influence at the various phases. Guidance and dialogue are provided on becoming involved effectively in the standards development process. The introductory seminar will be held in Dresden from 25 to 27 October 2023.

Are you already familiar with the principles of standardization work, and would you now like to expand your skills? The **advanced seminar** offers you the opportunity to meet other experienced standardization experts and discuss with them the strategies for participating in standardization activity even more effectively. You will share the experience you have gained in the standardization process and the options available for exerting influence, and learn what is currently happening in the field of standardization.

The face-to-face phase of the advanced seminar will be held in Dresden on 5 and 6 December 2023. The other parts of the seminar will be held online or will take the form of independent learning.

Information and registration: https://asp.veda.net/webgate_dguv_prod, event Nos 570044 (introductory seminar) and 570139 (advanced seminar)

European amendments to IEC standards

In accordance with the Frankfurt Agreement, electrotechnical standards should preferably be drawn up at international level at IEC and adopted in parallel by CENELEC as identical European (EN IEC) standards. The adoption of IEC standards in Europe may, however, require amendments in order for the requirements of Single Market directives or regulations to be met.

The resulting deviation between the two standards is evident in that CENELEC then publishes these standards not as **EN IEC** 6xxxx, but only as **EN** 6xxxx – but with the same number as the corresponding IEC standard.

Sommaire

© Vector Tradition - stock.adobe.com

Dossier

Thèmes

© berCheck - stock.adobe.com

© momius - stock.adobe.com

43 En bref

44 Agenda

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-

©smshoot - stock.adobe.com

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

© picoStudio - stock.adobe.com

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 www.aplusa.de

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.

Termine / Events / 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.de

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/seminarmaschinen-anlagen

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

Bestellung / Ordering / Commande

www.kan.de » Publikationen » KANBrief » KANBrief-Bestellservice (kostenfrei)
www.kan.de/en » Publications » KANBrief » KANBrief subscription (free of charge)
www.kan.de/fr » Publications » KANBrief (gratuit)

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

Impressum

Herausgeber / publisher / éditeur
Verein zur Förderung der Arbeitssicherheit in Europa e.V. (VFA)
mit finanzieller Unterstützung des Bundesministeriums für Arbeit und Soziales

Redaktion / editorial team / rédaction
Kommission Arbeitsschutz und Normung (KAN), Geschäftsstelle
Sonja Miesner, Michael Robert
Tel. +49 2241 231 3450 · www.kan.de · info@kan.de

Verantwortlich / responsible / responsable
Angela Janowitz, Alte Heerstr. 111, D – 53757 Sankt Augustin

Übersetzung / translation / traduction
Odile Brogden, Marc Prior

Publikation
vierteljährlich / published quarterly / parution trimestrielle

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