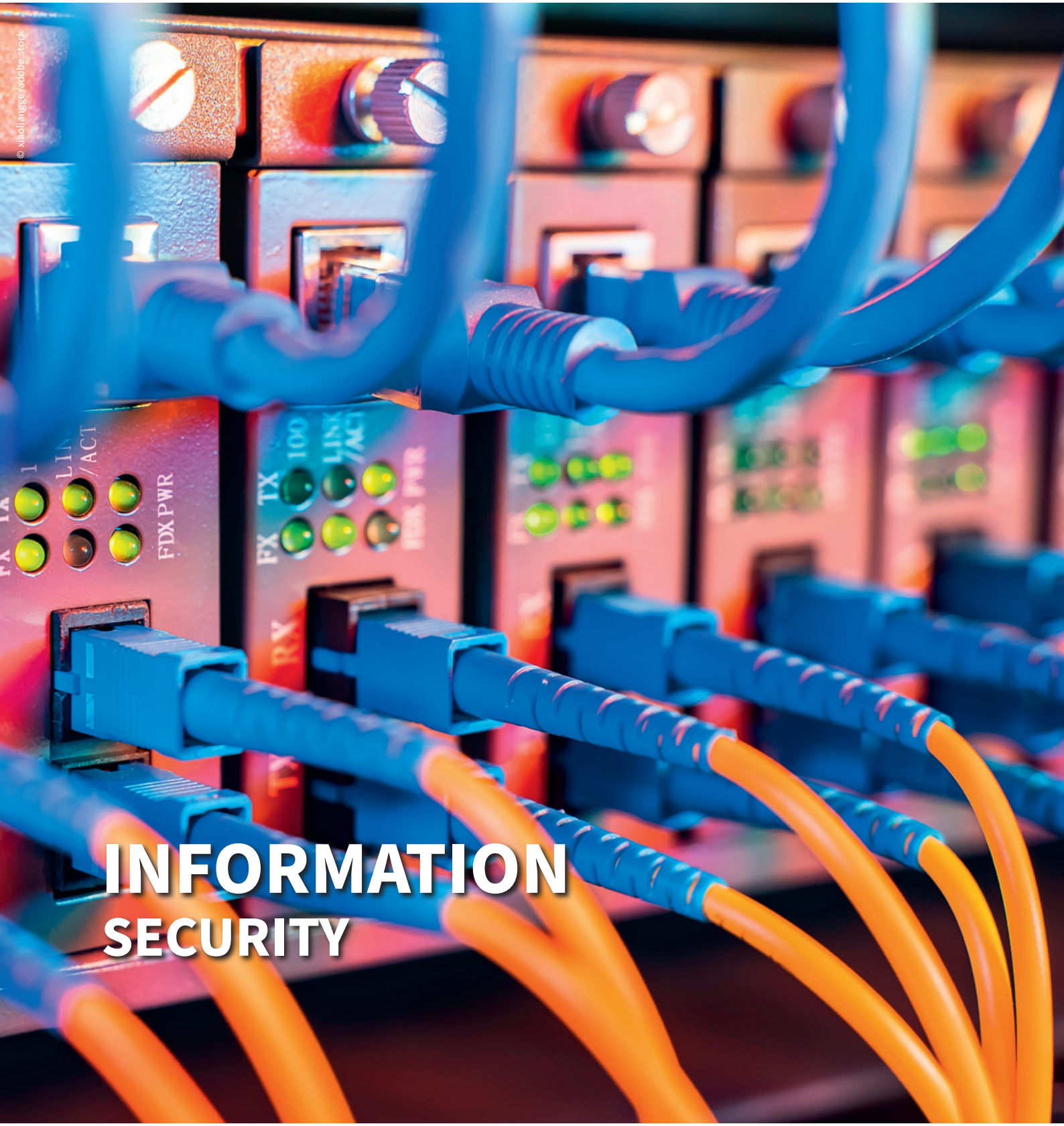
KAN Brief
3/23
Kommission Arbeitsschutz und Normung



INFORMATION SECURITY

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-online.com. 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.

Events

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
https://www.aplusa-online.com

25.10.23 » Online

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

25.-27.10.23 » Dresden

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

26.10.23 » Düsseldorf

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

02.11.23 » Berlin

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

13.11.23 – 18.01.24 » Dresden/Online

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

15.11.23 » Online

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

27.-28.11.23 » Bonn

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

29.11.-01.12.23 » Dresden

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

04.-07.12.23 » Sankt Augustin

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

Ordering

www.kan.de/en » Publications » KANBrief » KANBrief subscription (free of charge)

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

Impressum

Publisher
Verein zur Förderung der Arbeitssicherheit in Europa e.V. (VFA)
with the financial support of the German Federal Ministry of Labour and Social Affairs

Editorial team
Commission for Occupational Safety and Health and Standardization (KAN), Secretariat
Sonja Miesner, Michael Robert
Tel. +49 2241 231 3450 · www.kan.de · info@kan.de

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

Translation
Marc Prior

Publication
published quarterly

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