ZVEI-Position:

Recommendations for the Standardisation Request to the Cyber Resilience Act (CRA)

Executive Summary

ZVEI – the German Electro and Digital Industry Association calls in general for an effective and efficient approach to harmonised standards (hEN) for cybersecurity, which makes use of existing standardisation work. Ambitious cybersecurity regulation goals clash with limited resources, especially in regard to cybersecurity experts, who are qualified and mainly contribute on a voluntary basis to the critical standardisation work. The efficient and effective involvement of these experts is of utmost importance.
To ensure this ZVEI calls to adhere to the following principles:

- **Base the work on hEN for new or revised regulations, on existing and established European or international standards**
- **Ensure realistic timelines for the development of standards**
- **Foster coordination and alignment between regulations and standardisation projects**
- **Allow for a flexible, agile, and market-driven standardisation approach**
- **Focus on sectoral needs and avoid a one-size fits all approach that unnecessarily duplicates standardisation work**
- **Set commonly accepted rules for the conformity assessment of products, addressing the cybersecurity specific challenges**

As the Cyber Resilience Act is currently progressing in the legislative process, stakeholders are becoming increasingly familiar with the details, the interplay and special aspects of importance. Additionally, challenges in the coming implementation are becoming clearer and the framework gets more comprehensive. In this context the importance of harmonised standards (hENs) listed in the Official Journal of the EU (OJEU) as one way of showing compliance cannot be overstated.

With the already active standardisation process for the Delegated Regulation (EU) 2022/30 under Art. 3(3) d,e,f of the Radio Equipment Directive (RED) important lessons have been learned and open issues been identified regarding the development of harmonised standards for cybersecurity.

Additionally, the first draft standardisation request has been made available in August 2023, in preparation of the final standardisation request under the CRA, aiming to advance the development work towards harmonised standards before the final regulation text is agreed upon. The German Electro and Digital Industry welcomes this proactive step by the commission, which aims at minimising delays, but for this approach to work some important aspects have to be considered. Therefore, ZVEI would like to share the following attention points to contribute to a successful implementation of the upcoming formal standardisation request.

Identified issues and challenges

Current activities in standardisation committees

- Various standardisation activities are currently in progress in support of the regulatory frameworks on cybersecurity. These are in particular,
  - … the work in CEN-CLC/JTC 13/WG 8 on the hENs for the Delegated Regulation (EU) 2022/30 (RED),
  - … the preparations in CEN-CLC/JTC 13/WG 9 and ETSI TC Cyber for the hENs under the EU Cyber Resilience Act (CRA),
  - … the preparations for the EU CRA in sectoral technical committees, like CLC/TC 65X/WG 3 (cybersecurity in industrial automation) and other diverse domains (smart meters, household appliances, railways, toys, etc.), and
  - … the work of CLC/TC 44X (safety of machinery) to address the cybersecurity requirements in the Machinery Regulation (EU) 2023/1230, stemming from the essential health and safety requirements (EHSR) 1.1.9 and 1.2.1.
- Multiple parallel hEN-projects are putting a strain on the limited pool of available experts and pose challenges in terms of alignment.

Ambitious targets, complex work, challenging timelines

- Those current standardisation activities are further complicated by the level of detail of the corresponding standardisation requests and the constraints on the structure of the standardisation work.
- The extensive standardisation request[1] in support of (EU) 2022/30 called for the development of new generic hENs, as common denominator to all impacted sectors and technologies (from toys to 5G network equipment), with a multitude of common overarching requirements. Despite the very constrained and stringent work schedule, a consensus has been found within CEN-CLC/JTC 13/WG 8 on the draft hENs (formal enquiry phase until November 2023). Nevertheless, so far, the European Commission has not provided any feedback regarding the acceptability of the overall approach. This puts the standardisation activities at high risk. The aim of the standardisation activities is to develop harmonised standards that are listed in the OJEU, to facilitate legal certainty for all stakeholders through presumption of conformity. Moreover it is still unclear, even with the recent extension of the deadline for adoption of harmonised standards to the 30th of June 2024, if the harmonised standards will be available and listed in the OJEU on time.
  - … Similar concerns arise from the draft standardisation request for the CRA. It foresees the development of generic (“product-agnostic”) standards that need to be complemented by May 2025 and 31 “product-specific” standards by May 2026. Looking at the respective deadlines of roughly 1,5 years from now for the generic standards and an additional 12 months for the product-specific standards the expectation could be deducted, to (again) develop a new generic framework from scratch, on which new product-specific standards will be built.
- The Machinery Regulation (EU) 2023/1230 foresees a transition period of 42 months for a protection target that is well established within standardisation. On the other hand the EU CRA foresees a substantially shorter transition period of 24 months (proposal by the EU Commission), which is a brand new regulation addressing a new protection target for which no harmonised standards exist.

Recommendation: The standardisation request should leave the approach for the development of relevant hENs to the experts within the ESOs. Similar to other hEN related standardisation activities it should be left to the expertise within the ESOs to decide, whether the EU CRA hENs should be based on existing, modified, or newly developed standards.

Broad scope of regulation and high number of addressed domains, special importance of hEN for critical products of class 1

- Due to the very broad scope of the EU CRA a high number of standards (generic, product-specific) need to be developed. Harmonised standards are of importance, because with their availability they often are the base for product development, conformity assessment, and testing done by notified bodies. In case of their unavailability, according to EU CRA Art. 24(2) (Class 1 products) the involvement of notified bodies for the conformity assessment of the respective products is mandatory. Considering the limited resources, also at the notified bodies, and the challenging timeframe, ZVEI supports the focussed approach as currently proposed in the position of the EU Council. Since the legislative process is still open, such a focussed approach, based on the critical cybersecurity functionality or the critical network functionality of a product would have a positive impact on the standardisation activities: It would not only significantly reduce the number of

[1] Implementing Decision C(2022) 5637 from 05/08/2022.

necessary standards, but it would also increase legal certainty, and keep the definition and the list of critical products much more stable in the long run.
- Due to the expected criticality, the development of harmonised standards for critical products should be of priority. Because they lead to comparable conformity assessment results, regardless of whether the manufacturer carries it out himself under own responsibility or whether a notified body is involved.

Recommendation: The standardisation request should only set the boundaries in order for the ESOs to be able to develop the necessary framework. The standardisation request should prioritize activities, meaning that in a first step generic and cited hENs should be developed to support the presumption of conformity for all products. In a second step and where deemed necessary/appropriate, more specific product group/product specific cited hENs should be developed.

Challenges specific to cybersecurity

- For all standardisation projects, it should be noted that cybersecurity poses special challenges with regard to objectively verifiable and reproducible test/assessment criteria for the verification of the respective cybersecurity requirements. This can only be achieved for certain requirements, because for many requirements it is nearly impossible to specify quantifiable test/assessment criteria. Adequate security controls must be derived from the outcome of a cybersecurity risk assessment that is based on a rapidly evolving threat landscape. Experiences, views, and different mitigation strategies as well as the intended use of the product and specifics of the foreseen environment of use can vary significantly and change over time. It is therefore challenging and might even be impossible to define objectively verifiable and reproducible test criteria to demonstrate whether a requirement has been fulfilled in a way that is applicable and appropriate.
  The requirement to specify verifiable, objective and reproducible test criteria may even harm the overall resilience level, as new and innovative ways to ensure adequate resilience could be limited by such a narrowed view, e.g. like the use of AI for threat prevention and detection.

Recommendation: Considering the lessons learned and pending open issues from the standardisation activities in support of the RED DR (EU) 2022/30 the described issues relating to assessment and test criteria must be solved before starting the EU CRA related standardisation activities to ensure the citation of the hENs in the OJEU.

Our position

- The development of the work program is the responsibility of the ESOs and therefore the ESOs need appropriate flexibility to find the best approach for identifying and developing the necessary hENs. The standardisation request should only set the boundaries in order for the ESOs to be able to develop the necessary framework.
- Lessons learned and results from the standardisation activities under the Delegated Regulation (EU) 2022/30 must be taken into account, especially with regard to assessment and test criteria.
- Foster available and widely applied European/international cybersecurity standards for the development of hENs by amending them where necessary.
- Within the industrial domain and the area of industrial security the EN IEC 62443 series is recognized as an accepted and appropriate series of standards to safeguard the protective target of cybersecurity. Therefore the ESOs should be empowered to reuse existing standards, specifically the EN IEC 62443 series and ETSI EN 303 645 (for consumer products) and implement necessary amendments and additions.
- Requirements for specific European Standards handling vulnerabilities for products with digital elements and to prepare for effective vulnerability handling norms are also vividly welcome, as these allow an approach based on established industry norms and processes and avoid gaps in continuously ensuring product cyber protections. Here too it is indicated to adhere to exiting International Standards as ISO 30111 and ISO 29147, which have already received transposition into ENs.
- Ensure realistic timelines in accordance with the respective standardisation target. To base the standardisation activities on existing standards increases the likelihood of timely availability of harmonised standard. The work of the HAS consultant and the time needed by the Commission to cite the hENs in the OJEU also needs to be considered in the requested standardisation timelines. Additionally, enough resources for HAS consultants have to be ensured and prioritization in assessment and listing could be prudent.
- Although we appreciate the forward looking approach, it is important, that before a standardisation request for product specific standards is issued, the scope of the regulation including the classification of those products has to be clear.

- In a first step generic and cited hENs should be developed to support the presumption of conformity for all products. In a second step and where deemed necessary, more specific product group/product specific cited hENs should be developed.
- A focus on processes would be useful not only for standards on vulnerability-handling requirements, but also for standards relating to the properties of products. Therefore, we propose to focus CRA standardization more on sustainable, more generic cybersecurity processes rather than developing many, quickly outdated product-specific standards per product. For the essential requirements related to properties of products these processes could specify e. g, relevant aspects of a security risk analysis and how to determine applicability of essential requirements to a product, how to determine appropriateness of security measures and how to document these steps, etc. Here the focus should lay on the outcomes of those processes. Finding the right approach to derive sensible standards, which are considering all those aspects will take the ESOs time and they need enough leeway in the standardisation request to solve this complex challenge. Here too the recourse to existing sector standards, like the EN IEC 62443, could be very helpful, but to reach a comprehensive result, the work on the hENs under RED DR (EU) 2022/30 has to be considered as well. Legacy products must be considered as well when process standards are developed or reused. This could be solved by applying the respective processes based on a security risk analysis.
- A product might be covered by multiple different EU regulations, all covering the same protection objective of cybersecurity. Therefore, it must be ensured that the various standardisation activities are aligned to prevent inconsistencies in order to enable the reference of the hENs under these regulations. For example, the activities related to the development of cybersecurity specific standards to support e.g. the Machinery Regulation (EU) 2023/1230, the General Product Safety Regulation (EU) 2023/988, and the upcoming Artificial Intelligence Act must urgently be aligned with the EU CRA related standardisation activities.
- Further paralleling efforts in the cybersecurity domain should be avoided, this includes the future work on CSA-Schemes e.g. for IoT or IACS: Here too the efforts should be based on the yet to develop hEN or the accepted and appropriate European and international standards, as it is intended in Art. 54 (1) (c) of the cybersecurity act (EU) 2019/881.
- The product must be designed to address the cybersecurity risks resulting from the intended use and its intended environment of use. Standards can only address the intended and reasonably foreseeable use and misuse of the product by the (end) user, but not the foreseeable misuse of the product by an attacker. Even in the risk assessment this can only be partly covered.
- In case of the unavailability of cited hENs a number of products, e.g. Class 1 products, will have to undergo a conformity assessment with the mandatory involvement of a notified body. Even though the notified bodies must have the competence to perform the conformity assessment even in the absence of harmonised standards (see 768/2008/EC Annex I Art. R17 and Art. R23) they alone cannot ensure the comparability of the conformity assessment results. In case of a mandatory involvement of the notified bodies, a lack of resources of the bodies to perform the conformity assessment is very likely.[2]

[2] For more details about the interworking between harmonised standards and third-party conformity assessment bodies compare the ZVEI-Position-Paper „Ensure adequate transition periods for a functioning EU Single Market“.

Brief overview of the current state of regulation

- **Complex regulatory landscape regarding cybersecurity,** which can be divided in regulations, which address operations and in those, which address products. Concerning the cybersecurity of operations the current Network and Information Security directive (NIS) will be superseded by the overhauled NIS-2-directive. The NIS-2 has to be transposed by member states, the transpositions have to be applicable by the 18th of October 2024. The cybersecurity of products is partly addressed in different, mostly newly (re-)worked, sectoral regulations in context of other protection goals (new machinery regulation; general product safety regulation; AI Act; proposal of the new product liability directive and the radio equipment directive (RED)). The product regulations as well as the regulation for the operation side have connections to the voluntary certification framework of the 2019 cybersecurity act.
- The **delegated regulation 2022/30 under Art. 3(3) d,e,f of the RED plays a special role** as its date of application, 1st of august 2024; will precede the CRA and through this legal act the first cybersecurity requirements for products falling under the RED will be established.
- To simplify the complex regulatory landscape and to counter the further proliferation of piecemeal cybersecurity requirements, the European Commission has **proposed the Cyber Resilience Act** on the 15th of September 2022, which is currently under discussion by the European co-legislators and is planned to enter into force under the current commission.

Background: Numbers & Facts

- **Critical personnel gap**: Currently are already more than **100,000 cybersecurity professionals missing** for Germany alone. Other European member states have similar numbers, e.g. France and Spain with about 60,000 missing experts in relation to a **worldwide gap of 3,4 million cybersecurity workers**[3]. And the raised demand through NIS-2, the delegated act under the RED and the CRA is not fully considered yet.
- **Continuous proliferation of connected devices:** The number of IoT-devices will increase even more in the upcoming years, reaching a range of over 30 billion predicted IoT connections in 2028 from currently over 13 billion connections.[4]
- **Products falling under RED DR & CRA, effected markets:** Whereas the implications of the delegated act are somehow limited by the fact, that only products falling under the RED are addressed, this is only a small limitation as especially the number of wireless devices is increasing and outpaces those of wired devices.[5] Looking at the concerned products under the CRA, the broadness of its scope increases the number of concerned products and companies even further. This leads to a range for the turnover of the effected EU 27 hardware industries of 285 bn to 1220 billion in 2019 numbers[6] and up to a 172 bn turnover in 2019 for the also in major parts effected software development market.[7]

[3] (ISC)2 Cybersecurity Workforce Study, 2022; p. 3 & 8. The staff shortage does not seem to have fully reached the wages for this group in Europe, as the corresponding U.S. wage level is significantly higher (about 40%) than the European one. (ebd. p. 65).
[4] 13,2 billion total connections in 2022 to a forecast of 34,7 billion IoT connections in 2028 (combined number of wide, area, cellular and short range IoT connections); Ericsson Mobility Report, November 2022, p. 11.
[5] Worldwide, between 2016 and 2021 the increase in the number of wireless local area network (WLAN) connected devices far outperformed the increases in the number of wired connected devices with a rise from 8,36 bn to 22,2 bn devices in comparison to less than 4bn to 5,5 bn devices. Comp.: WLAN connected devices worldwide 2016-2021 | Statista; Wired connected devices worldwide 2016-2021 | Statista
[6] In the impact assessment (Annex p. 34ff) of the CRA (Impact assessement documents: Cyber Resilience act – new cybersecurity rules for digital products and ancillary services (europa.eu)) the ICT manufacturing sector – standard classification (ICT-SC), representing a sub- set of 3-digit NACE 2 activities of the manufacturing sector, was set as lower level of concerned hardware companies and the unofficial extended classification (ICT-EXC) was set as upper level. Considering the extensive scope of the current CRA proposal, a tendence towards the upper level could be expected. But it still has to be considered, that not all of the products produced by those manufactures are products with digital elements as defined in the CRA.
[7] Impact assessment (Annex p. 27-33), the used category is also a proxy used as an indicator built for the purpose of the impact assessment.

Contact

Marcel Hug • Manager Cyber Security & Strategy • Digital and Innovation Policy •
Tel.: +49 69 6302 432 • Mobil: +49 162 2664 941 • E-Mail: Marcel.Hug@zvei.org

ZVEI e. V. • Electro and Digital Industry Association • Lyoner Straße 9 • 60528 Frankfurt am Main • Germany
Lobbying Register ID.: R002101 • EU Transparency Register ID: 94770746469-09 • www.zvei.org

10/2023