Position on the proposal for a Cyber Resilience Act

Call for a realistic implementation approach

The CRA is the right approach, but it needs the right "transition strategy" to work

In the light of the proliferation of a fragmented regulatory landscape regarding cybersecurity, the ZVEI is a strong long-time proponent for a horizontal cybersecurity regulation for products within the proven new legislative framework (NLF). Therefore, we welcome in principle the coherent proposal of the CRA, as it follows the logic of the NLF and only adds some needed limited requirements in the life cycle, especially the establishment of a vulnerability management process, in a considerate manner.

Positions of the German Electro and Digital Industry:

- **Make the CRA the central reference point for product cybersecurity requirements and align the interplay with other regulations**, including those of the new machinery regulation (esp. reg. Annex III, section 1.1.9), the GPSR and the AI-Act. Also include the repeal of the delegated act under article 3 (3) d,e,f of the radio equipment directive (RED) in the text of the CRA to avoid double regulation.
- **Ensure a realistic transitional period and transition strategy**, potentially through a staggered approach, for a successful implementation through the cascade (comp. fig), including the development of hEN, their fast assessment and listing.
- **Clarify the definitions & scope of the regulation:** Focus on products, which are really able to exchange data (bidirectionally); Add an exemption regarding spare parts to allow for the continuous use of long living goods. Add missing definitions and streamline and clarify the content of the regulation to **ensure unambiguity** for the development of the harmonized standards (hEN) as well as for the economic actors concerned.
- **Choose a more differentiated approach to critical products with digital elements by amending the too broad classification in annex III** and differentiate between components and systems. Delete art. 6 (5) and encompass "highly critical products" in the third-party conformity assessment procedures acc. to art. 24 (3).
- **Optimize the connection of the obligations to the manufacturer and essential requirements for an effective and efficient implementation.** Especially amend essential cybersecurity requirement 1 (2) in annex I to reference the vulnerability handling requirements and not to address hypothetical vulnerabilities of products during transit, which will be fixed by the process requirements, e.g., through initial security updates
- **Conformity assessment – strengthen the consistent NLF-Approach of the CRA;** other means of showing conformity, like common specifications and CSA-Schemes, should undergo similar obligations and quality safeguards as hEN. Allow for the prudent (re)-use of established international standards like IEC 62443 in the development of the hEN.
- Mitigate possible additional challenges through the CRA in already strained supply chains, by taking into account the **incomplete character of most components**, especially in regard to their conformity assessment and testing and through the introduction of a lower limit for components, which pose only minimal risk.
- **Align the reporting obligations for incidents and vulnerabilities with the NIS-2-directive** and limit those requirements to significant incidents having a significant impact and actively exploited vulnerabilities. Refer to already established international reference points and scoring systems like the MITRE reference-method for "common vulnerabilities and exposures" (CVE) and the CISA "known exploited vulnerabilities catalog" (KEV).

The CRA is the right approach, but it needs the right “transition strategy” to work

The current situation

The German electrical and digital industry welcomes in principle the coherent and consistent proposal of the Cyber Resilience Act with the intention to simplify the complex regulatory landscape and to counter the further proliferation of piecemeal cybersecurity requirements.

The most important task at hand is now to ensure a practicable horizontal regulation that allows the industry to get into the practical implementation. There is little time for the experts in the companies as well as for other stakeholders like notified bodies and the European Standardization Organizations (ESO): The harmonized standards (hEN) must be developed by the ESO in time; Cybersecurity expertise and staff in companies must be expanded, processes must be amended or established; products have to be redesigned or in some cases designed from scratch and these tasks are spread over the whole supply chain. Often with one actor waiting and depending on the tasks and work the actor before him in the chain has to do.

The CRA is a coherent proposal, because it follows the logic of the NLF and therefore differentiates itself positively from the CSA, which only contains some NLF-elements and wording and therefore is no fitting way to place products onto the market. Only some needed limited requirements in the life cycle, especially the establishment of a vulnerability management process were added in a considerate manner. Otherwise, the CRA follows the common framework laid down in decision no. 768/2008/EC.

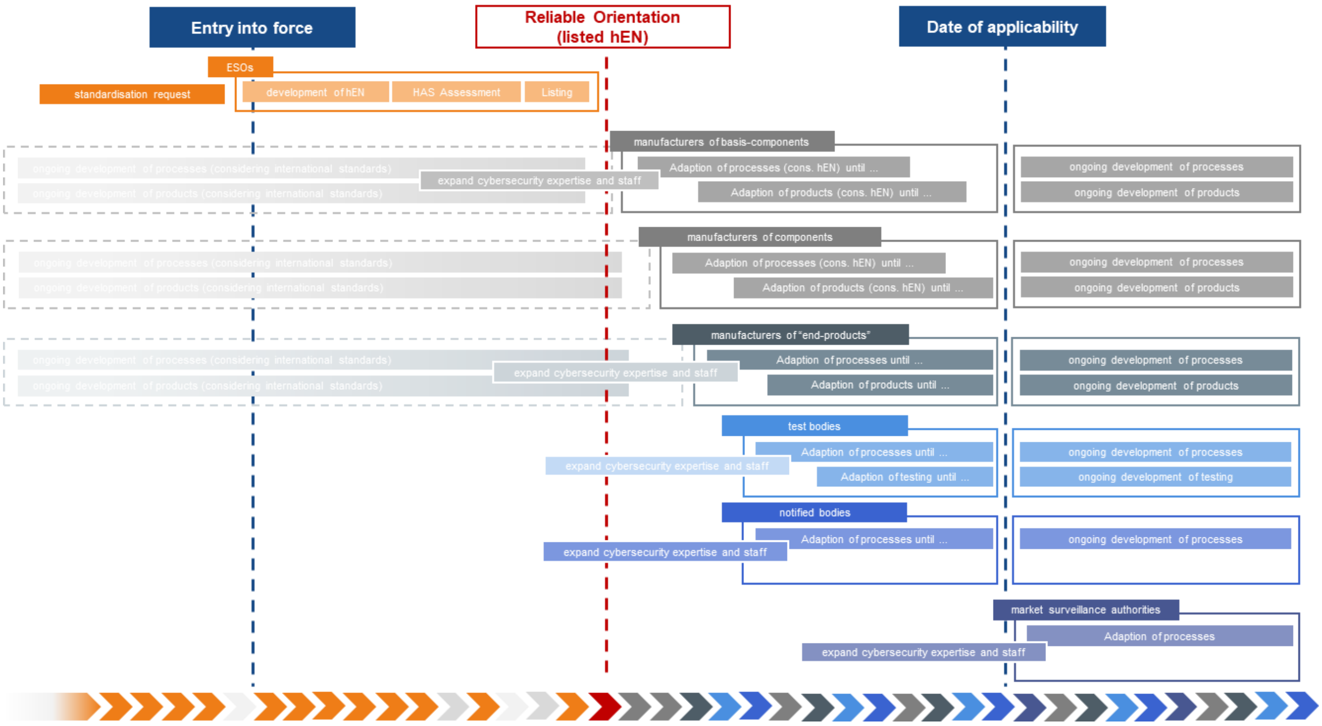
This way the CRA allows for the use of already known procedures and uses the strengths of the NLF:

- Technological neutral requirements
- Risk based requirements according to a risk assessement in consideration of the intended use and intended operational environment of a product
- Use of proven NLF conformity assessment procedures; especially the internal control procedure based on module A; which allow for a stringent assessement of a large number of products without creating bottlenecks

The tasks at hand – making the CRA work

In the understanding of the German Electrical and digital industry, two issues are of crucial importance: **(1) A clear, understandable, consistent, and unambiguous proposal,** which shows what tasks are at hand at an early stage. The CRA is already in most parts a very good proposal, but in some parts, we see need for improvement and clarification. Especially regarding which effort has to be made for which products in regard to their real criticality. **(2) A realistic timeframe for the technical implementation is needed.** As explained shortly not every affected entity can start with all needed implementing steps at the same time. Therefore, a staggered approach regarding the timeframe could be prudent, which is oriented at the position of components and products in the supply chain and the real criticality of a product. The limitation of resources, especially the shortage of qualified personnel, require the most effective and efficient approach, as all stakeholders, from manufacturers, to notified bodies as well as market surveillance authorities are facing the same resource issues in order to address the regulatory obligations. It can be expected that especially small and medium sized organizations likely will be facing bigger challenges to meet procedural and technical requirements of the CRA.

A core issue, to understand the challenges which will arise, is that ideally the requirements stemming from annex I of the CRA would be implemented in a cascade. Every stakeholder is to some extent dependent on the work of the stakeholder before him in the cascade: The manufacturers need the hEN for the use of module A at least as a reliable orientation, as do the testing bodies and notified bodies for information and orientation. Then there are dependencies between manufacturers of products and (basis)-components as well. All of these connections (as shown in the image below) have to be considered in a realistic timeframe resp. transition period.



Entry into force
Reliable Orientation (listed hEN)
Date of applicability
ESOs
standardisation request
development of hEN
HAS Assessment
Listing
manufacturers of basis-components
ongoing development of processes (considering international standards)
ongoing development of products (considering international standards)
expand cybersecurity expertise and staff
Adaption of processes (cons. hEN) until ...
Adaption of products (cons. hEN) until ...
ongoing development of processes
ongoing development of products
manufacturers of components
ongoing development of processes (considering international standards)
ongoing development of products (considering international standards)
Adaption of processes (cons. hEN) until ...
Adaption of products (cons. hEN) until ...
ongoing development of processes
ongoing development of products
manufacturers of "end-products"
ongoing development of processes (considering international standards)
ongoing development of products (considering international standards)
expand cybersecurity expertise and staff
Adaption of processes until ...
Adaption of products until ...
ongoing development of processes
ongoing development of products
test bodies
expand cybersecurity expertise and staff
Adaption of processes until ...
Adaption of testing until ...
ongoing development of processes
ongoing development of testing
notified bodies
expand cybersecurity expertise and staff
Adaption of processes until ...
ongoing development of processes
market surveillance authorities
expand cybersecurity expertise and staff
Adaption of processes

Definitions & scope

The chosen scope of the CRA is wide considering the addressed products and the connected definition of “products with digital elements”. But at the current state the scope also possesses a significant depth, as the definition in article 3 (1) also explicitly addresses “software or hardware components”. Uncertainties remain around the question which combination of software and hardware solutions fall into the scope, and which do not.

CRA article 3 „ (1) ‘product with digital elements’ means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately; “

Focus on products, which are really able to exchange data

To **prevent a further unintended extension**, we deem it important to specify a common understanding of

> *“products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network”* in article 2 (1).

This could be solved by amending the text of article 2(1) in the following way, so that

> *“This regulation applies to products with digital elements whose intended or reasonably foreseeable use includes a logical or physical **bidirectional** data connection to a device or network”,*

or at least by clarifying the understanding in a recital. In any case should a “data connection” not be misunderstood as any connection, for example: products that are connected to other products exclusively via switched inputs or outputs shouldn’t be seen under the scope of the CRA, as those products are only capable to perform simple signal processing.

Adding missing definitions & clarify

To further clarify the understanding of the proposal there should also be some **missing definitions** added in article 3, like “device”, “network”, “free-software” and “open-source software”.[1] Also article 3 (35) has counterpart in the NIS-2, as there are several mentions of “cybersecurity risk”, but there is no definition of the term “cybersecurity risk” in the (nearly) final text – only of the more generic term “risk” in article 6 (9) of the NIS 2. The term “incident” should also be added in article 3, at least in reference to its definition in NIS 2. Also, it would be helpful to explain the difference between “incident”, “vulnerability” and “actively exploited vulnerability” in a recital in regard to article 11 of the CRA. Additionally, some other definitions should be further aligned to clarify the respective issues addressed, e.g., regarding products like “secure elements” and “hardware security modules” the language should be further aligned with the eIDAS-regulation 910/2014[2] its amending regulation and the connected standards.

Exemption for spare parts

Another problem regarding the scope is the issue of **spare parts**. The CRA shouldn’t disrupt the use of long living products, therefore there is a strong need for **a provision for spare parts.** Spare parts which are part of the maintenance operation (and are not covered by the obligation of Article 10, Chapter 6), especially for long living products, should be excluded from the scope. This would be in line with Chapter 2.1 of the “Blue Guide” (OJEU, 2022/C 247/01): *“Thus, maintenance operations are basically excluded from the scope of the Union harmonization legislation*”. A spare part has to be a direct fit, in result the cyber resilience level of the product will not change and would remain the same. Therefore, the provision of a spare part shouldn’t constitute a new placing on the market under the Cyber Resilience Act.

Proposed amendment:

New paragraph in article 2 (6):

> *This Regulation does not apply to products and components that are intended to be used as spare parts to replace products or components during repair operations.*

[1] Comp. recital 10 of the CRA.

[2] EUR-Lex - 32014R0910 - EN - EUR-Lex (europa.eu)

New definition of “spare parts” in article 3 (x):

> *’spare parts’ means products and components that are intended solely to repair or replace defect products or components in order to restore their functionality.*

Challenges in the supply chain – components

Components according to the CRA should be defined more in detail: The limited aspects of components which are developed for further use in products have to be considered, as those components itself should be considered as incomplete. Especially, regarding the limited capabilities of a component itself and the question how requirements of such an item could be correctly assessed.
Therefore, the definition of components in article 3 (8) *(‘component’ means software or hardware intended for integration into an electronic information system;*) should be amended:

> *(8) ‘component’ means an item with digital elements (software or hardware) which contributes functionality to a product, is intended for integration into another product with digital elements; and possesses more than minimal risk*

Also, a lower limit for components has to be considered, as there are currently components, e. g. analogue switches or real-time-clock-chips (RTC), in the scope of the CRA with extremely limited functionalities and capabilities. To limit the burden for manufacturers and other stakeholders like notified bodies, such components, which are on the one hand lacking the functionalities and capabilities to address the cybersecurity requirements of the CRA and on the other hand pose only minimal risk (benign products/components), should be excluded from the scope of the CRA.

This does not necessarily result in a higher risk for more complex products. Basically, any part, component or subsystem of a product potentially imposes a cybersecurity risk on the networked product, and any such part placed on market by a third party, may contribute some risk. Thus, a product may require additional security measures, usually derived and determined based on a threat and risk analysis, conducted during the design process. The lower limit of consideration is determined by those parts, components or sub-systems that do not impose a security risk on the networked product. Where risk-freeness cannot be concluded, counter measures for security-by-design of the networked product are required. In any way, for making an informed decision, the relevant information, even of “benign” products will be needed.

The German electrical and digital industry welcomes the clarification in recital (27)[3], that the use of critical components of class I and II in a product does not constitute that the whole product should adhere to the requirements regarding the conformity assessment which refer to critical products.

Interplay with other regulations – making the CRA a truly horizontal product regulation

As much as the German electrical and digital Industry welcomes the CRA as a full-fledged coherent NLF-regulation, we unfortunately see also some missed opportunity in the current proposal, as it isn’t ambitious enough with regard to the interaction with other regulations.
Although Article 7 (on the GPSR), Article 8 (on the AI Act) and Article 9 (on the Machinery Regulation) attempt to develop these relationships, the mentioned articles are too complex and the CRA is not sufficiently enough positioned as a central reference point in the sense of an idea of a horizontal product regulation. We therefore would favor an amendment of article 2 (4), to give the CRA priority over other regulations regarding the essential cybersecurity requirements of products with digital elements. In our understanding only products, which are listed in article 2 (2) and (3) should be exempt in such a way, as article 2 (4) is currently drafted.

[3] “(27) The categories of critical products with digital elements referred to in Annex III of this Regulation should be understood as the products which have the core functionality of the type that is listed in Annex III to this Regulation. For example, Annex III to this Regulation lists products which are defined by their core functionality as general purpose microprocessors in class II. As a result, general purpose microprocessors are subject to mandatory third-party conformity assessment. **This is not the case for other products not explicitly referred to in Annex III to this Regulation which may integrate a general purpose microprocessor.** The Commission should adopt delegated acts [by 12 months since the entry into force of this Regulation] to specify the definitions of the product categories covered under class I and class II as set out in Annex III.”

Such an amendment could be drafted in similar way like it is currently seen in article 9 regarding the machinery regulation proposal:

> *Products under the scope of an EU regulation which are products with digital elements within the meaning of this Regulation [the Cyber Resilience Act] and for which an EU declaration of conformity has been issued on the basis of this Regulation [the Cyber Resilience Act] shall be deemed to be in conformity with any essential requirements of an EU regulation which compliance is based on the adherence of security requirements set out in Annex I of this regulation [the Cyber Resilience Act], as long as the requirements are based on the same cyber risks, which are addressed by the Cyber Resilience Act.*

Concluding, article 7 and article 8 should be amended accordingly.

Improve alignment of the CRA and the new machinery regulation

Furthermore article 9 also should be further specified, because only some of the requirements set out in Annex III, Section 1.2.1 of the new machinery regulation relate to cybersecurity. Consequently, not all requirements of Section 1.2.1, but only the cybersecurity-related requirements in Section 1.2.1 can be covered by complying with the CRA requirements. We therefore propose the following amendment to better reflect this issue, including additional line brakes to enhance the readability of the article:

Current text of Article 9 of the CRA:

„Machinery products

Machinery products under the scope of Regulation [Machinery Regulation proposal] which are products with digital elements within the meaning of this Regulation and for which an EU declaration of conformity has been issued on the basis of this Regulation shall be deemed to be in conformity with the essential health and safety requirements set out in Annex [Annex III, Sections 1.1.9 and 1.2.1] to Regulation [Machinery Regulation proposal], as regards protection against corruption and safety and reliability of control systems, and in so far as the achievement of the level of protection required by those requirements is demonstrated in the EU declaration of conformity issued under this Regulation.“

Proposed amendment:

Machinery products under the scope of Regulation [Machinery Regulation proposal] which are

- *products with digital elements within the meaning of this Regulation and*
- *for which an EU declaration of conformity has been issued on the basis of this Regulation*

shall be deemed to be in conformity with the essential health and safety requirements set out in

- *Annex [Annex III, Section~~s~~ 1.1.9 ~~and 1.2.1~~] to Regulation [Machinery Regulation proposal], as regards protection against corruption ~~and safety and reliability of control systems~~, and*
- *Annex [Annex III, Section 1.2.1] to Regulation [Machinery Regulation proposal], as regards safety and reliability of control systems* to the extent they relate to cybersecurity, and

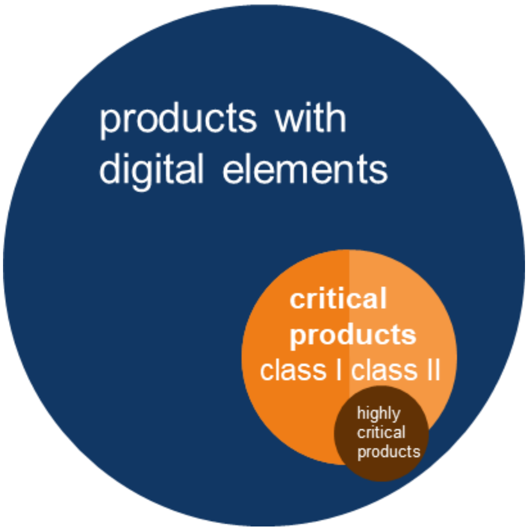
in so far as the achievement of the level of protection required by those requirements is demonstrated in the EU declaration of conformity issued under this Regulation.

Clarify relation of to the delegated act under Article 3 (3) d,e,f of the Radio Equipment Directive and the CRA

In addition, the relationship to the delegated act under Article 3 (3) d,e,f of the Radio Equipment Directive, which is currently the most prominent and most advanced attempt to establish sectoral cybersecurity requirements for products, is only mentioned in a non-binding recital. Its relation should be part of the legal text of the CRA: As a repeal would be the most favorable option, to prevent double regulation it would be prudent to lay down the process of the repeal, the transition period, and the relation regarding the compliance under the respective regulation in a new paragraph in article 2 or as a new Article 7a (similar to the solutions for Machinery and AI).

A differentiated approach to critical products with digital elements

Critical products with digital elements

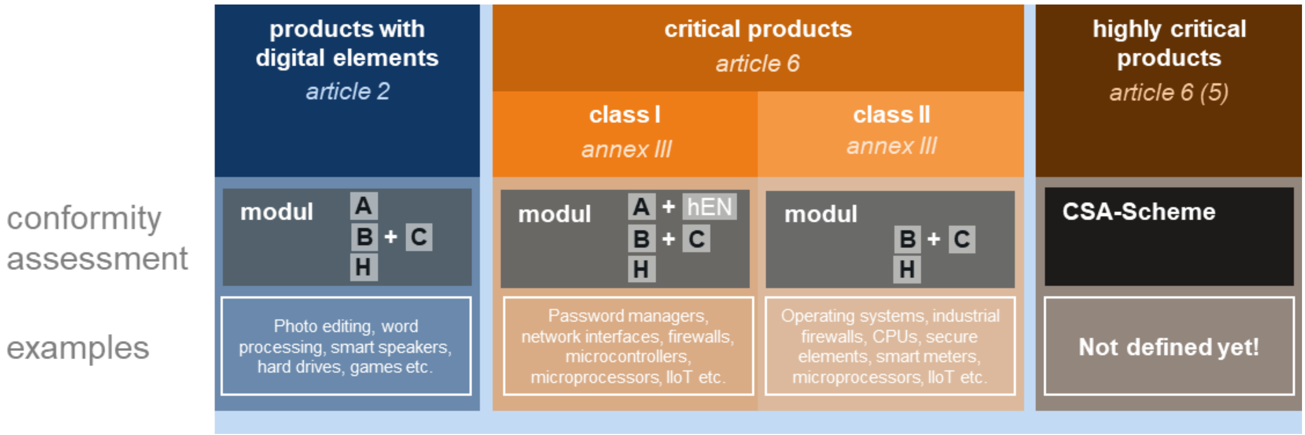


Currently the CRA references 4 classes. Within the default class of products with digital elements (PDE), there are two classes of “critical products” (class I and class II) plus a potential class of “highly critical products”. For the first three classes different conformity assessment procedures are assigned in article 24 of the CRA (cf. graph x).

By article 6 (2) the commission is also empowered to amend annex III by including new categories or removing existing ones through the adoption of a delegated act. For those delegated acts the criteria listed in article 6 (2) (a) to (e) shall be considered and at least one of those criteria has to apply. In our understanding only one criterion isn’t a sufficient threshold, so we propose that at least two of the criteria have to be applicable to justify the adoption of a category to the list. Also 6.2 should be extended with a criterium “(x) Exposure to internal and external networks”.

Furthermore article 6(2) should be amended in such a way, that the adoption process only could be started if proven evidence shows the need of such an adoption through a delegated act, like it is the regulated in the comparable process requirement of the new machinery regulation.

Finally, it is important to note, that high technical requirements can be implemented with all the conformity assessment procedures foreseen in the CRA, so there is no need for annex III to be so extensive as it currently is.



	products with digital elements *article 2*	critical products *article 6*		highly critical products *article 6 (5)*
		class I *annex III*	class II *annex III*	
conformity assessment	modul A B + C H	modul A + hEN B + C H	modul B + C H	CSA-Scheme
examples	Photo editing, word processing, smart speakers, hard drives, games etc.	Password managers, network interfaces, firewalls, microcontrollers, microprocessors, IIoT etc.	Operating systems, industrial firewalls, CPUs, secure elements, smart meters, microprocessors, IIoT etc.	Not defined yet!

Mandatory CSA-Schemes through article 6 (5)

Furthermore, with article 6 (5) the commission is empowered to adopt delegated acts to make CSA-schemes for highly critical products mandatory, creating a yet to be defined theoretical fourth class of “highly critical products”.

In our understanding, there is no need for a fourth class, which is circumventing the otherwise coherent NLF-approach of the CRA, as there is already a mandatory third-party involvement for all “critical products” of class II. The only reason, we could see to implement article 6 (5) in the way it was done, is in connection to article 24 (1) of the NIS-2 directive, as article 24 (1) in NIS-2 gives member states the possibility to “*may require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881.”* Article 24 (2) of the NIS-2 then follows an empowerment of the Commission, to specify the categories of essential and important entities, which are to be required to use those particular certified ICT products, ICT services and ICT processes. Article 6 (5) seems to be the respective link in the CRA regarding products for this issue. But there is no real need for this counterpart in the CRA, as article 18 (3 &4) of the CRA would already allow for the use of CSA-Schemes to show compliance, this would include products for which article 24 (2) of the NIS-2 would have been activated.

We would therefore favor to delete article 6 (5) and explain the above-described connection in a recital. If the co-legislators do not deem this possible, article 6 (5) of the CRA should at least be further aligned with article 24 (2) of NIS-2; as the activation of article 6 (5) should only be made possible for products, which are in use in essential entities for which an delegated act according to article 24 (2) of the NIS-2 directive has been adopted and an impact assessment and consultation has been carried out, which also considered the products in question. In conclusion, it would therefore only be logical to move article 6 (5) to a new article 7 addressing the relation between the CRA and NIS-2.

Too broad classification of critical products of class I and II

Regarding the categorization of class I and II "critical products" in annex III we see further need to address those products more accurately, as the current classification of products is too broad and unspecific. The following classifications therefore should be reworked.

In annex III of the CRA, Industrial Automation & Control Systems (IACS) are listed in category class I and class II including distributed control systems (DCS) and supervisory control and data acquisition systems (SCADA). It therefore seems as if the CRA considers these systems in its entirety as products with digital elements. Especially in case of class II, such systems would be subject to mandatory third-party conformity assessment which seems unrealistic taking their nature into account. That is, IACS and SCADA systems usually are complex systems and comprise many different components and products, itself often having digital elements, fulfilling numerous tasks, and having different risk within the system as entirety. For example, some sub-products used for process control can be considered high risk and should therefore belong to class II, while sub-products not being used for any critical tasks can be categorized either class I or even no class at all. It is therefore suggested for the CRA to consider this complex relationship of products with digital elements in the context of an IACS, DCS, SCADA or any other system by changing Annex III as follows:

Proposed amendment:

Class I

22. Industrial Automation & Control Systems (IACS) not covered by class II, ~~*such as*~~ that are *programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC)* ~~*and*~~ or that are products intended for use in *supervisory control and data acquisition systems (SCADA);*

Class II

12. Industrial Automation & Control Systems (IACS) intended for the use in critical applications *by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)],* ~~*such as*~~ that are *programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC)* ~~*and*~~ or that are products intended for use in *supervisory control and data acquisition systems (SCADA);*

Such a change would also reflect the real world conditions better, as SCADA systems normally enter into operation in three main ways, of which only one would be addressable through the CRA, if the whole system is addressed: A SCADA system could either be bought as once, like it is chosen from a catalogue, or it is individually built and projected from different products by an external contractor, or a company builds their own SCADA system from scratch using different products. Only the first way of procurement is addressable as a whole by the CRA, so the focus on products as described above would also solve this issue and is therefore favorable.

In link to the above in article 6 (2) proposed criterium "(x) Exposure to internal and external networks" it also has to be noted, that the risk of many products in an industrial setting is mitigated by an defence-in-depth approach. Therefore, Annex III should not address almost all networkable industrial products. Currently, especially the categories "Industrial Automation & Control Systems (IACS)" and "Industrial Internet of Things" could be understood in such a much too broad way. For example, sensors and actuators are only connected to an internal bus/network in a machine behind a PLC that acts as gateway and should be understood as being less critical, even if being used in an industrial setting. Therefore annex III class I no. 23 and class III no. 13 have to be amended:

Proposed amendment:

Class I

> *23 Industrial Internet of Things devices, not covered by class II.*, which pose a high risk and which are intended for data connection from the internet.

Class II

> *13 Industrial Internet of Things devices* which pose a high risk and which are *intended for the use* in critical applications *by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];*

As third amendment we propose the deletion of class II 14. "Robot sensing and actuator components and robot controllers" because the strict assessment procedures of the Machinery Regulation will already apply to safety components under the Machinery Regulation. The criticality is thus sufficiently covered as most of the safety critical functions are strongly regulated by the machinery regulation and their supporting standards for many robot controllers. On the other hand are robots outside the context of the Machinery Regulation (e.g., vacuum cleaner robots) not critical and do not justify the highest criticality level for their components

Components as critical products in annex III

We understand that additionally there might be some products or especially some components which importance stems from their universal application in high numbers and not necessarily from their direct use in essential or important entities after NIS-2. However, careful deliberation is necessary: (1) For some products security functionalities of components are chosen and shaped through a communication between the manufacturer of the component and the manufacturer of the (end)-product in regard to its intended use and functionality. For those cases solutions could be found on a component or a product level or in a mixed form. (2) For other (end)-products, manufacturers take shelf ready components, which either already have some security functionalities which are used without any modification or, (3) manufacturers use "bare" components for implementing their own security functionalities on a product level. In any case it must be possible to clearly describe and differentiate the above-described (three) uses of a component and to guarantee that it is possible to use it in way, which allows for conformity with the CRA and without unnecessary burdens regarding the conformity assessment procedures described in article 24 of the CRA.

Additionally, to underline the importance to amend the categories in annex III, they have to be compared to the seemingly deliberate omission of some products that are relevant for critical business processes and products that are providing services on the Internet:

As other important product categories are seen as fit to be assessed without the assignment of specific conformity assessment procedures it should be strongly considered to use the same approach for other products categories on the two lists in annex III as well.

Optimize the connection of the obligations to the manufacturer and essential requirements for an effective and efficient implementation

Improve the fit between article 10 and annex 1 sec. 1 (2)

Currently annex 1 sec. 1 (2) states *"Products with digital elements shall be delivered without any known exploitable vulnerabilities"*. This proposes an unrealistic requirement as the transport and storage of product constitutes a time, during which the vulnerability handling process could not be ensured. On the other hand possible "fictional vulnerabilities", which one could even coin Schrödinger's vulnerabilities, as long a product is in transit, have no effect, if they are directly addressed during the first usage of a product. Therefore we call to amend essential cybersecurity requirement 1 (2) to reference the vulnerability handling requirements and not to address hypothetical vulnerabilities of products, which are in storage or in transit, which will be fixed by the process requirements, e.g. through initial security updates. Otherwise manufactures could hypothetically be seen as non-compliant, although they fulfil all requirements of annex I to keep the product secure and the product itself poses no risk, because it stays dormant.

Proposed amendment of annex I 1.:

> (2) ensure that vulnerabilities are addressed by the vulnerability handling process of annex I 2. after the placing on the market of a product, so that vulnerabilities can be mitigated when the product is initially connected

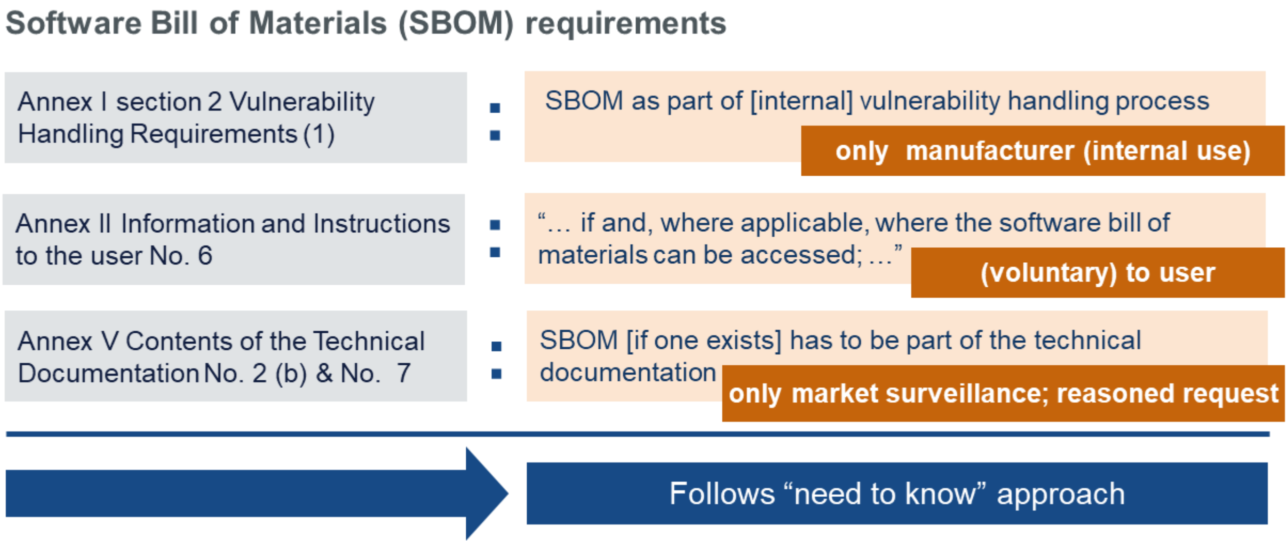
Realistic understanding of security support in context of the product type

The German electro and digital industry welcomes the prudent partial evolution which took place in form of the CRA, which allows an NLF-Regulation to address obligations in the life cycle after the placing on the market of the product. In its current form the introduction of process requirements in form of the mandatory establishment of an "vulnerability handling" process in accordance with article 10 and annex I section 2 is a clever and targeted extension, which addresses the relevant core issue in the life cycle.

Use of Software Bill of Material (SBOM) in regard to the obligations

The CRA introduces for the first time some requirements regarding the use of a software bill of material: To meet the vulnerability handling requirements of Annex 1 Section 2 manufacturers are required to establish a vulnerability handling process that includes the production of SBOM and their internal use. Additionally, in accordance with Annex II, No. 6 information from the internal SBOM could be issued on a voluntary basis.

Also, the technical documentation according to Annex V of the CRA requires per product, where applicable, SBOM for the product as part of the vulnerability handling process, which must be issued on a case-by-case basis in response to a justified request from the competent market surveillance authority.



Software Bill of Materials (SBOM) requirements

Annex I section 2 Vulnerability Handling Requirements (1)

SBOM as part of [internal] vulnerability handling process

only manufacturer (internal use)

Annex II Information and Instructions to the user No. 6

"… if and, where applicable, where the software bill of materials can be accessed; …"

(voluntary) to user

Annex V Contents of the Technical Documentation No. 2 (b) & No. 7

SBOM [if one exists] has to be part of the technical documentation

only market surveillance; reasoned request

Follows "need to know" approach

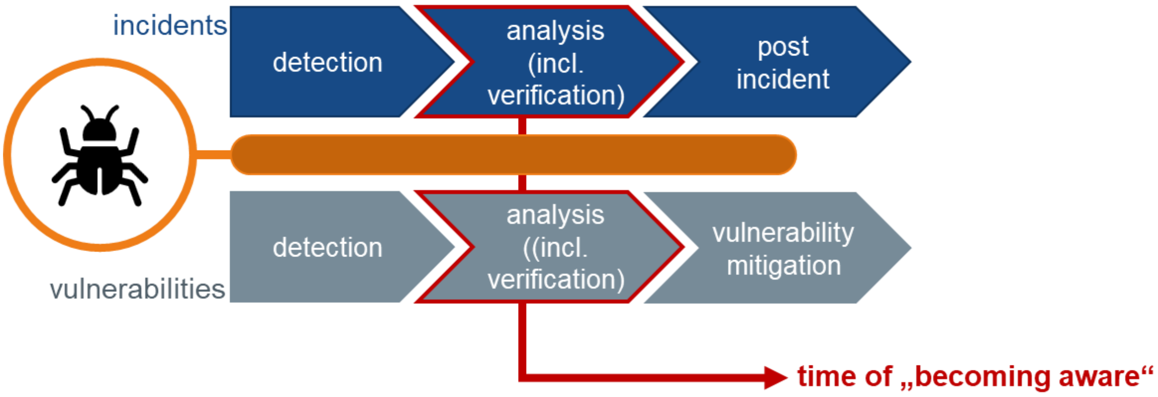
We agree that the use of SBOM will be important to fulfill the vulnerability handling requirements of Annex 1 Section 2, but **we strongly advise against specifying formats and elements of the software bill of materials** as it is described in recital 63. Those aspects should be defined and solved by the international standardization community, which is already working on three different standards on SBOM.

Reporting obligations and their consequences

Regarding the reporting obligations of article 11 the approach should be more proportionate, especially considering the already strained personnel resources and challenges especially SME will face to adhere to them. The **obligations should be further aligned with the NIS-2-directive and its wording**. Therefore, we call for an extension of the time limit for the reporting of incidents to 72 hours for incident notifications in general. If possible, warnings should be within 24 hours, but there should be an exemption from penalties as long as a warning was released within 72 hours. The reporting obligations to ENISA should also be limited to significant incidents having a significant impact in order to limit the burden on ENISA.

Accordingly, the reporting obligations regarding actively exploited vulnerabilities contained in the product with digital elements should also be further aligned with NIS-2 and should also be limited to significant exploited vulnerabilities to limit the burden on ENISA and the manufacturers in particular SME. Especially since it is to be expected, that the number of reported vulnerabilities will be higher, than those of incidents. Therefore, it would be also prudent to refer to already established international reference points and scoring systems like the MITRE reference-method for “common vulnerabilities and exposures” (CVE) and the CISA “known exploited vulnerabilities catalog” (KEV)[4].

Also, responsible disclosure should be ensured. Additionally, the reporting obligations should consider the usual respective incident and vulnerability handling process, which starts with detection, forwards to an analysis stage and subsequently to a post incident or in the case of vulnerabilities to a mitigation stage. Full awareness will only be reached after the analysis stage, therefore the time limit to notify enisa should start from the time of verification.



Conformity assessment – strengthen the consistent NLF-Approach of the CRA

Harmonized standards, common specifications and certifications schemes should all undergo the same level of evaluation procedure as foreseen for harmonized standards, in order to ensure consistency with the essential requirements. Otherwise, the burden would be higher for the development of harmonized standards through the involvement of the HAS consultant and the listing process etc. compared to the creation of common specifications and the rather closed shop approach of the development of certification schemes under the CSA Therefore the same obligations and quality safeguards are needed for hEN; CSA-Schemes and common specifications.

Realistic transitional periods for a successful implementation

As explained in the beginning of this position paper the implementation will follow different steps. This has to be considered in the transitional period. We therefore call for a transitional period of 48 months. This is even more relevant since there are currently not enough security specialists available on the market. They are needed for both the manufacturers and the conformity assessment bodies as well as for the operators concerning the broad scope of NIS-2-directive, which will have to be implemented by the essential and important entities Falling under NIS 2 in approximately the same time frame.

In the face of massive political pressure, which calls for unrealistic time frames, at least a staggered approach has to be considered, which could implement the following transitional periods for different categories of products:

As we understand the current sense of urgency regarding the cybersecurity of some products there could be some categories of products with a transitional period of 24 months. As critical products of class II are

[4] Known Exploited Vulnerabilities (nist.gov)

exceptionally relevant for essential entities of the NIS-2-directive and encompass important components, which are widely used, a transitional period of 24 months might be justifiable. But this only applies, if class II is limited to the most critical products, which is currently not the case.

Critical products of class I could build on the expertise from class II, as several similar categories, with less critical use environments are mentioned. Therefore, those products should have a transitional period of 36 months. However, class I currently also encompass too many general categorizations of products – including several similar broad categories with much less critical use environments.

For the remaining products with digital elements there is no heightened sense of urgency, as they possess a lower risk potential and a lot of those products will additionally be already covered by the delegated act under article 3(3) d,e,f of the radio equipment directive. Here we propose a transitional period of 48 months.

Closing remarks – how we all can contribute

As the CRA is moving along in the European legislative process there are already preparations in which different stakeholders could partake to prepare for a smooth implementation of the CRA and further actions, which could be done, when the CRA is published:

Manufactures have to be prepared on different levels: Internally they have to grow their resources regarding the cybersecurity of products, by developing internal expertise or by hiring additional (product)-security-experts, as far as those are even available. They also have to look at their processes and products (hardware and software), the currently available standards like the EN 303 645 and especially the IEC 62443 series are important reference points for this task. It would be also prudent to take part in the international standardization efforts, especially in those which will lead to the harmonised standards under the CRA:

The (national) cybersecurity agencies are also seen as key players in those standardization efforts, it is to be expected, that they could play an important role in the market surveillance for the CRA, so here preparation is needed.

The European standardization organisations play a key role as platform for expertise and especially in the process of the development of harmonized standards. It is important that preparations for the coming standardization request of the CRA begin as soon as possible. Therefore, the ESOs should enter in a close exchange especially with the international software-community, which is in large parts for the first time addressed by a European product regulation under the NLF. Also the lessons learned from the standardization work for the delegated act under article 3 (3) d,e,f of the RED in the CEN/CENELEC/JTC 13 WG 8 “Special working group RED Standardization Request” should be taken into account at an early stage.

The notified bodies also have to prepare in order to be able to fill their role foreseen in the CRA. This means a ramp-up of capacities and expert personnel, to prevent that they could become a bottleneck.

Those operators, which will fall under the requirements for essential and important entities under the NIS-2 could use CRA-compliant products, once those are available, to implement the state of the art.

As the lack of experts will be one of the greatest obstacles, the EU should focus on this problem and should address it through programs to support the building up of expertise and the education of (new) security experts as well as actions to improve the availability of experts.

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

Date: February 9th, 2023