Cyber Resilience Act – recommendations for the trilogue

Executive summary

The currently discussed Cyber Resilience Act (CRA) will have far reaching consequences. We are convinced that the aim of the CRA to increase the overall cyber-resilience level in Europe is a very valid goal. The German Electro and Digital industry therefore supports the CRA, especially since this approach of a horizontal product regulation on cybersecurity uses the well-known and proven legal framework for placing products on the market, the New Legislative Framework.

However, we are very concerned that individual elements of the proposed regulation could have a massive negative impact on supply chains, the availability of products, components and spare parts, and thus also on the operation of essential infrastructures and industries. The very broad scope of application of the draft and also of the positions of the Council and Parliament would cover a large proportion of the products on the internal market, resulting in a huge impact. In our view, every article and aspect of the CRA should be worded so that implementation in practice is feasible. Only if efficient and effective action are derived from the finished legal text, the common effort to significantly rise the resilience level will be achieved.

To keep our recommendations efficient as well, we have organized them into two groups, the order within those does not reflect any prioritization.

Within the highest category, we see especially the following five aspects as critical for the German Electro and Digital industry:

- We support the new classification logic of the council for critical products with digital elements in Art. 6.
- We support the concept introduced by the Parliament, that manufacturers should transparently determine a support period for the product.
- We call for a more coherent establishment of the CRA as lex specialis for the cybersecurity of products.
- We urge the legislator to further specify the essential product requirement regarding known exploitable vulnerabilities.
- We are still convinced, that the CRA requires at least 48 months until the date of applicability for a successful implementation.

Table of contents

Our recommendations in detail

Recommendations with top priority

Recommendations with the top priority shall be considered, as they have the potential to significantly hinder the implementation of the CRA or could disrupt the single market and supply chains.

Issue: **Critical products with digital elements (classification logic)**

Recitals and articles: **Art. 6 & Recital 26**

Comment: The initial proposal of the European Commission lacked a focus on criticality and a clear methodology and therefore does not support legal clarity – for the CRA implementation as such – but also for the development of standards. Although the Parliament tried to improve the classification logic, its core problems prevailed. The focused approach introduced by the Council on the other hand offers a consistent and comprehensible new approach.

Recommendation for Council text: **The German electro- and digital industry strongly supports the Council's approach to establish easily understandable criteria to differentiate the classes of critical products with digital elements based on criticality.**

The chosen criteria in regard to the core functionality of a product of either a core cybersecurity function or a core network function for Annex III (1) or both for Annex III (2) is accurate as well as elegant in its minimalism. This logic of either a or b for class I, and simultaneously a and b for class II is easily comprehensible and gives clear criteria to differentiate the classes along the two core aspects along which risks and therefore criticality scale.

This recommendation also includes the changes in recitals 26 done by the Council, which further elaborate the proposed logic.

Issue: **Lists of critical products with digital elements**

Recitals and articles: **Annex III & Recital 27**

Comment: The Commission's and Parliament's lists of products in Annex III don't provide a clear view on the categorization of the different products because they are not based on a concrete methodology which focusses on criticality. Therefore, there is no clear separation of concerns and the Commission's, and Parliament's lists of products are a mixture of products, product categories, product types, features, functionalities and systems.

Recommendation for Council text: **ZVEI strongly recommends the product list of the Council in annex III, which is deducted from the classification logic, proposed by the Council.**

Especially since both other product lists by the Parliament and the Commission have the following issues: Whole product categories are addressed apart from differences in criticality within those groups, here the classification is just too broad. For example, products for the industrial internet of things, IACS and PLC in general, smart meters in general, robot sensing and actuator components and robot controllers and home automation systems are such broad categories that further differentiation would be urgently needed. In both lists systems and products are addressed interchangeably, when it comes to Industrial Automation & Control Systems (IACS), distributed control systems (DCS) and supervisory control and data acquisition systems (SCADA). Making such systems subject to mandatory third-party conformity assessment, when they are listed for class II, is unrealistic taking their nature into account. IACS and SCADA systems usually are complex systems and comprise of many different components and products, itself often having digital elements, fulfilling numerous tasks, and having different risk within the system as entirety. Also, the lists include products, where the criticality is already sufficiently covered by other regulations, like industrial robots by the new machinery directive.

Issue: **Mandatory use of CSA-schemes for certain products**

Recitals and articles: **Art. 6 (5), Art. 6a (EC) & Recital 27a (EC)**

Comment: In our principle understanding, there is no need for the category or a new class of highly critical products with digital elements, 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. For products with special national security interest there is also already to possibility to make the use of CSA-schemes mandatory for those products under article 24 of the NIS-2-directive (EU 2022/2555).

Recommendation for deletion: **We recommend the deletion of Art. 6 (5) as proposed by the Commission and the Parliament or Art. 6a as proposed by the council.**

If there is a need for category of highly critical products the respective list in the annex should only contain products, for which certification schemes covering the CRA essential requirements are available. The currently developed EUCC-scheme based on common criteria and the EUCS for cloud services are only useable for a very small and limited set of products. So, we see the annex IIIa of the Council at least as positive in the way, that it only focusses on products, where common criteria could be applicable. Therefore, we also understand the logic described in recital 27a of the Council, including the products identified for Annex IIIa, but we still not see the need for a separate category to be make use of CSA-certification-schemes as this would already be possible.

Issue: **Period of security support**

Recitals and articles: **Art. 10 (6) & Recitals 2 (EP), 32a (EP)**

Comment: The existing concepts of product lifetime, like currently discussed in the ESPR, focus mainly on physical aspects of a product, often in regard to its physical composition. Digital elements introduce a completely new aspect, which shouldn't be mixed up with the current discussion of product lifetime in the ESPR. Complex assumptions, with a lot of unknown variables, have to be drawn to identify the lifetime of a digital element, which could differ from the product wherein the digital element is integrated. Therefore, the concept chosen in the CRA for a mandatory period of security support shall reflect this challenge and should strike a fair balance between, what manufacturers are able to predict and what users could expect.

Recommendation for Parliament text: **We strongly support the concept introduced by the Parliament, that manufacturers should determine a support period for the product.**

We also want to highlight the importance of the context of the product, as it is recognized by the Parliament. We agree that such a support period should be *"proportionate to the expected product lifetime as well as taking duly into account in line with the nature of the product and users expectations, the availability of the operating environment and, where applicable, the support period of the main components integrated into the product with digital elements."* It is important to understand that a product and the digital element within has to be assessed according to its intended use and its intended use environment, as this will lead to differences in requirements, expectations and also different limits of a product. Due to the ever changing threat landscape and newly identified vulnerabilities it must be understood that from a technical perspective, products cannot be supported for an indefinite timeline and new vulnerabilities cannot necessarily be resolved by software updates. We also think it is crucial for such a concept, that this support period is communicated in a transparent way, including the possibility to use digital means.

Issue: **Missing exemption for spare parts**

Recitals and articles: **Art. 2 (4a) (EC & EP) & Recitals 14a (EP)**

Comment: It is already significant progress, that the positions of the European Council (EC) as well as the European Parliament (EP) foresee an exemption for spare parts, but further improvements seem necessary, because the exemption should address products and components and should focus on the supply not the manufacturing.

Recommendation for adjusted Parliament text: The proposal of the Parliament seems to more on point by referring in general to “spare parts”, which includes products and components, but the wording could still be optimized the following way:

> *Art. 2 (4a.) This Regulation does not apply to spare parts that are **intended to be used** exclusively ~~manufactured~~ to replace identical parts and are supplied **or specified** by the manufacturer of the original products with digital elements.*

The Council proposal uses the term “component” which in this respect can be misleading and therefore the term “spare part” is deemed appropriate and should ideally be specified in Art. 3.
Recital 14a of the Parliament is also welcomed, as it describes the needed twofold application of the exemption, for products placed on the market before and under the CRA.

Issue: **Open-source software (OSS)**

Recitals and articles: **Recital 9a (EP), 10, 10a (EP)**

Comment: A thriving open source software (OSS) community is essential for innovation and research. Unfortunately, in all existing positions, there is no explicit regulation that ensures the free development of OSS in a binding way. We therefore recommend explicitly excluding the development of OSS ('upstream') from the regulatory requirements of the CRA and instead restricting the application of the CRA exclusively to the commercial use of OSS in digital products ('downstream'). As the current text of the Parliament is the most comprehensive in addressing the issue.

Recommendation for adjusted Parliament text: **We recommend adjusting the text in the recitals 9a, 10 and 10a of the Parliament in the following way:**

> **Recital 9a (EP) […] To foster the development and deployment of free and open-source software, in particular by microenterprises and small, medium sized enterprises, including start-ups, and not-for-profit organisations, academic research and individuals, this Regulation should apply only to free and open-source software products in specific cases of ‘downstream’ use, to take into account the fact that different development models of software distributed and developed under public licences exist.**
>
> Recital 10 ~~In order not to hamper innovation or research,~~ ***Only*** free and open-source software ~~developed or supplied outside~~ ***made available on the market for commercial use in digital products ('downstream') in*** the course of a commercial activity should ~~not~~ be covered by this Regulation. ~~This is in particular the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable.~~ **The development of free and open-source software ('upstream') should explicitly be excluded from the regulatory requirements of the CRA.**
> ***Whether a free and opensource product has been made available as part of a commercial activity for commercial use in digital products should be assessed on a product-by-product basis~~, looking at both the development model and the supply phase of the free and open-source product with digital elements.~~***
>
> **Recital 10a (EP) For example, a fully decentralised development model, where no single commercial entity exercises control over what is accepted into the project’s code base, should be taken as an indication that the product has been developed in a non-commercial setting. On the other hand, where free and open-source software is developed by a single organisation or an asymmetric community, where a single organisation is generating revenues from related use in business relationships, ~~this~~ the commercial use in digital products should be considered to be a commercial activity. Similarly, where the main contributors to free and open-source projects are developers employed by commercial entities and when such developers or the employer can exercise control as to which modifications are accepted in the code base, the project should generally be considered to be of a commercial nature and the commercial use in digital products would fall under the CRA.**

With those additions a targeted distinction between “upstream"-development and (monetized) “downstream” use would be possible, allowing the use of the creative potential of the open-source-community without turning a blind eye to potential risks in products, which use open-source-software. But to effectively ensure the

implementation of this legislative solution, an exclusion of free and open-source software development should also be directly included in the legal provisions of the CRA.

Recommendation for an additional provision in consideration of the Parliament recitals: We also recommend adding a direct exclusion of free and open-source software development in a new article 2 (3a):

> *3a. This Regulation does not apply to free and open-source software including non-profit free and open-source software collaborative development platforms, hosting, or distribution unless it is offered as or incorporated in a "monetised" product or service by a manufacturer, distributor or importer.*

Issue: **Essential product requirements – known exploitable vulnerabilities**

Recitals and articles: **Annex I 1. (2) resp. annex I.1. (3aa), Art. 3 (38) (EC) & Recital 32**

Comment: The German Electro and Digital industry appreciates the change, that the requirement that products with digital elements shall "be placed [made available] on the market without any known exploitable vulnerabilities" on a risk assessment basis. But we still think that this is not sufficient to avoid problems in the implementation: The requirement still could lead to unrealistic assumptions, e.g. by market surveillance authorities, and does not reflect the widely established practice of installing new updates during the first use of a product.

Recommendation for Parliament and Council text: We recommend the move under annex I.1. (3) done by the Parliament and the Council, but further text is needed to focus the requirement only on the cases, where the security of a product in use maybe compromised. The addition of the Parliament in recital 32 already goes in the right direction focussing on the security of the product. But this should be included in the requirement in the annex as well:

> **Annex I.1. (3) […** **and where applicable, products with digital elements shall:] (aa) be placed on the market without any known exploitable vulnerabilities that might have an impact on the security of those products;**

A major improvement in this regard is the new definition by the Council of "exploitable vulnerability", which specifies, that a respective vulnerability must have the potential to be effectively used by an adversary under practical operational conditions. Although these practical operational conditions should in our opinion be described in more detail.

Recommendation for Council text: We recommend the new definition of "exploitable vulnerability" given by the Council and recommend specifying this definition further by the following additional text:

> Art. 3 (38a) 'exploitable vulnerability' means a vulnerability as defined in Article 6, point (15), of Directive (EU) 2022/2555 that has the potential to be effectively used by an adversary under ~~practical operational conditions~~ **the condition that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen;**

Issue: **Reporting obligations and definition of "actively exploited vulnerability"**

Recitals and articles: **Art. 3 (39a) (EC), Art. 11 & Recital 19, 19a (EC & EP), 35a (EP & EC), 35b (EP &EC)**

Comment: It is already considerable progress, that the proposals of the Council and the Parliament partly aligned the reporting obligations of the CRA with those of the NIS-2-directive.

ENISA or the designated CSIRT as entity which will receive the early warnings and notifications for vulnerabilities and incidents, could be overwhelmed by an excess of notifications. Therefore the early warnings and notifications should be limited, at least in a first step, to only the relevant vulnerabilities and incidents, to ensure sufficient capacities are available to handle them properly

For vulnerabilities it is already a good starting point, that reporting is limited to "any actively exploited vulnerability contained in the product", especially with the added definition of "actively exploited vulnerability" in

Art 3(39) by the Commission, which highlights that there has to be „reliable evidence" for the attempted exploit. This definition should be further limited to successful attempts. We therefore see parts of the added text by the Council as critical, even though it is structured in a more coherent way.

Recommendation for combination of Commission and Council text: **We recommend, to combine the Commission and Council text of the definition 'actively exploited vulnerability' in Art. 3 (39) the following way, starting with Council text, and focus on successful exploits:**

> (39) 'actively exploited vulnerability' means a vulnerability **as defined in Article 6, point (15), of Directive (EU) 2022/2555** for which there is reliable evidence that ~~execution of~~ **it has been successfully exploited by a** malicious ~~code was performed by an actor on~~ **actor** ~~**has attempted to exploit it**~~ **in** a **product with digital elements** ~~system without permission of the system owner, irrespective of whether this attempt has been successful or not;~~

To make the reporting usable starting from the above described definition we also recommend to further limit the reporting of vulnerabilities according to article 11 (1) to the reporting of significant vulnerabilities. This could be done by referring to threshold based on a CVSS-Score. Also a limitation to critical products could be worthwhile in a first step, to limit reporting received once the CRA is applicable and to lessen the burden for the majority SMEs, as those are often in general less likely to produce critical products of annex III.

Recommendation for adjusted Parliament text: **We recommend the Parliaments proposal in Art. 11 (1) as it highlights the need for strict security protocols in cases, where no corrective or mitigating measures are available. It also should be adjusted in the following:**

> The manufacturer shall~~, without undue delay and in any event within 24 hours of becoming aware of it,~~ notify to ENISA any **significant** actively exploited vulnerability contained in ~~the~~ **a critical and highly critical** product**s** with digital elements ***in accordance with paragraph 1a of this Article***.

With this changes, the burden, especially for SMEs, could be changed significantly, because the ambitious reporting times of 24h for an early warning and 72h for a notification are particularly challenging in regard of the topic of vulnerabilities. Vulnerabilities are a concern of the product security departments, those are often not active 24/7, as many operational security departments may be, in particular not looking at SMEs, where product security is often also managed by the staff responsible for the product in general. There are just no capacities available to extend those departments to 24/7-shifts to be able to fulfil such reporting requirements and they also will not be available, looking at the shortage of product security experts.

Recommendation for Parliament text: **We recommend the Parliaments proposal for article 11 (2) as it focuses on the reporting of significant incident having impact on the security of the product with digital elements.**

We also welcome, that the Parliaments already included a definition of an "significant incident" in Art. 11 (2a), but we want to highlight that in particular Art. 11 (2a) point (b) should be understood in the context of incidents having impact on the security of the product with digital elements. Incidents directly affecting natural or legal persons by causing considerable material or non-material damage are not a regulatory subject of the CRA but of the NIS-2 directive.

Issue: **CRA as "lex specialis" – relation of the new Machinery Regulation and the CRA**

Recitals and articles: **Art. 2(4), Art. 9 & recital 30**

Comment: In the Council Text Article 9, which links the CRA to the essential health and safety requirements (ESHR) set out in Annex III, Section 1.1.9. and 1.2.1 of the new Machinery Regulation, has been deleted. This was done, because in its current form it would generate blind spots, especially in the reference to EHSR 1.2.1, as this EHSR goes beyond security requirements. Also, some requirements in the new machinery regulation, which are referring to cybersecurity, were sadly in some respects drafted in too much detail, which complicates the reference of the CRA.

The deletion of Art. 9 and the addition of explanatory language in recital 30 is one way of solving this issue, but it only shifts the problem to the level of standardization, where the precedence between the two regulations cannot be decided. We therefore understand the solution approach taken by the Council with the deletion of Art. 9 and the extension of Recital 30, but we are not entirely satisfied with this either.

This problem could be solved if the intention of the CRA would be followed more stringently, which was to create a simple, coherent, and effective legal framework that horizontally regulates the cybersecurity of all covered products when placed on the market. This has to be done in such a way, that existing, product-specific regulations are not taking precedence for the protection goal of cybersecurity, but it should not interfere with the protection goals, like those of the machinery directive, either. To follow this approach the CRA should be construed as a "lex specialis" (a total harmonisation legislation) and should thus replace the existing and upcoming cybersecurity-related harmonisation legislation ("CE directives"). Both proposals of the Parliament and the Commission aim in that direction. Even though, they are not enough to create a proper "lex specialis" framework. To do this, Article 2(4) of the draft CRA should be modified so that conformity with the CRA results in conformity with other existing and upcoming harmonisation legislation regulating cybersecurity as long as the requirements of those regulations are based on the same cyber risks, which are addressed by the Cyber Resilience Act.

Recommendation deletion: **We recommend the deletion of article 9 as long as article 2 (4) is adjusted.**

Recommendation for adjusted text: To allow the above described solution the following text would have to be added at the beginning of article 2 (4):

> *Art. 2(4) 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 essential requirements or the parts of the requirement of an EU regulation which compliance is based on the adherence to cybersecurity requirements as 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.*

Only by adjusting article 2(4) in the described logic, the issue of the CRA as lex specialis for cybersecurity could be solved coherently. Nonetheless, if the mentioned adjustments of article 2 (4) are not possible, at least recital 30 has to be adjusted. The starting point should be the version of the council, to ensure, that the CRA could be used to fulfil requirements of the machinery directive as long as those requirements depend on cybersecurity. At the minimum this should be done by the following addition to the Council version of recital 30:

> Recital 30 To the extent […] *keeping the proposed council text for this part* …] ~~*as regards protection against corruption and safety and reliability of control systems in so far*~~ ~~*as the compliance with those requirements is demonstrated by the EU declaration of*~~ ~~*conformity issued under this Regulation*~~. ***A manufacturer may identify such synergies during the risk assessment process as foreseen under*** ~~***the [Machinery***~~ ***Regulation*** ***(EU) 2023/1230***~~***proposal]***~~***. If during the risk assessment risks are identified, which are cybersecurity risks wholly or partly covered by this regulation [the CRA], the compliance under the CRA should show compliance in accordance with Art. 9 of Regulation (EU) 2023/1230 for those aspects of the essential health and safety requirements in sections 1.1.9 and 1.2.1 to the extent that they relate to cybersecurity.***
>
> ***Furthermore, the Commission and the European Standardisation Organisations should take into account this Regulation in the preparation and development of harmonised standards to facilitate the implementation of Regulation (EU) 2023/1230*** ~~***the [Machinery Regulation proposal]***~~ ***as regards in particular the cybersecurity aspects related to the protection against corruption and safety and reliability of control systems set out in Sections 1.1.9 and 1.2.1 of Annex III to that Regulation*** ~~***[Machinery Regulation proposal]***~~***.***

But we still would prefer to clearly position the Cyber Resilience Act as lex specialis for requirements, whose compliance rests on the compliance with cybersecurity requirements.

Issue: **Transitional provisions – no repeal of Delegated Regulation (EU) 2022/30**

Recitals and articles: Article 55 (3a) (EP) & recital 15

Comment: We strongly support the addition of the Parliament in Article 55 (3a) to repeal Delegated Regulation (EU) 2022/30. Only when such a repeal of the Delegated Regulation under Art. 3 (3) d,e,f of the Radio Equipment Directive (RED) is a direct part of the provisions of the CRA legal certainty is ensured.

Recommendation to adopt the Parliament text: We recommend adopting the Parliament amendment in Article 55 (3a) to repeal Delegated Regulation (EU) 2022/30 on the same date of application as the CRA.

We also appreciate the idea of the proposed voluntary compliance during the transition period from the application of the Delegated Regulation (EU) 2022/30 to the CRA – where products with digital elements comply with the CRA, they shall be considered also to comply with Delegated Regulation (EU) 2022/30. But in our understanding some additional aspects of this voluntary compliance have to be considered and some aspects are unresolved:

The idea, to enable manufacturers to voluntarily comply with the CRA, so that their products shall be considered also to comply with the Delegated Regulation (EU) 2022/30 in the meantime, would significantly facilitate the application of the CRA and avoid duplication of regulation. But this has to be limited to products [resp. radio equipment] falling under the scope of the RED and therefore Delegated Regulation (EU) 2022/30, to ensure appropriate market surveillance and prohibit unfair competition.
In general respective market surveillance has to be ensured and may pose a challenge when regimes and responsible authorities may change from the Delegated Regulation (EU) 2022/30 to the CRA. Therefore in our opinion additional work and clarification are needed for this proposal to work.

Issue: **Entry into force and time until application**

Recitals and articles: **Art. 57**

Comment: The currently discussed transition periods of 24 or 36 months do not sufficiently take into account the comprehensive measures that need to be taken to implement the CRA and the different implementation steps needed, especially the time needed to develop the harmonized standards. In addition, there will be requirements from other digital regulations (AI Act, Data Act) that will also have an impact on the design of products with digital elements. That is why the applicability date for affected manufacturers must be at least 48 months after entry into force of the CRA. For some products additional transitional provisions in Art. 55 will be necessary (staggered approach).

Recommendation for changed text: We recommend, to change the date of applicability for all articles to 48 months after the date of entry into force.

> Art. 57 This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
> It shall apply from [~~24~~ **48** months after the date of entry into force of this Regulation]. ~~However Article 11 shall apply from [12 18 months after the date of entry into force of this Regulation].~~

Recommendations for other important topics

The following recommendations should also be considered, as they have the potential to hinder the implementation of the CRA or could disrupt the single market, e.g., by not adhering to NLF-principles and procedures.

Issue: **Substantial modification**

Recitals and articles: **Art. 3 (31) & recitals 22, 22(a) (EC), 23, 24**

Comment: The existence of a specific definition of substantial modification for the CRA is in principle welcomed, as the regulatory goals of the CRA including the protection goals bring with them some special aspects, which would make a direct reference to the concept of substantial modification in the blue guide difficult. Products with digital elements can be changed by digital means, often without changing the risk, which was assessed to choose the applicable security measures. This has to be considered in a concept of substantial modification, which is used for the CRA, and it is not only true for security measures that aim to mitigate vulnerabilities, like security updates, but for minor digital changes, like minor functional updates as well.

Recommendation for adjusted Parliament text: **We therefore recommend the Parliament text in Art. 3 (31) and Recital 22 as well, which already address this issue.**

But to ensure, that the intention of recital 22 of the Parliament is clearly understood we propose to change the text slightly, as it is currently misleading. Because the listed instances are not examples for substantial modifications but cases, where there is no substantial modification:

> (22) In order to ensure that products with digital elements, when placed on the market, do not pose cybersecurity risks to persons and organisations, essential requirements should be set out for such products. When the products are subsequently modified, by physical or digital means, in a way that is not foreseen by the manufacturer and that may imply that they no longer meet the relevant essential requirements, the modification should be considered as substantial. **But** ~~**For example**~~, ***necessary security updates,*** software updates or repairs ~~*could be assimilated to maintenance operations*~~ ***such as minor adjustment of the source code that can improve the security, should not be considered to be substantial modifications,*** provided that they do not modify a product already placed on the market in such a way that compliance with the applicable requirements may be affected, or that the intended use for which the product has been assessed may be changed. ***This is generally the case for new software versions which aim at improving performance and fixing vulnerabilities. Minor functionality updates, such as visual enhancements, the addition of new languages to the user interface or of a new set of pictograms, should generally not be considered to be substantial modifications.*** ~~**As is**~~ **In** the case ~~**for**~~ **of** physical repairs or modifications, a product with digital elements should be considered as substantially modified by a software change where the software update modifies the original intended functions, type or performance of the product and these changes were not foreseen in the initial risk assessment, or the nature of the hazard has changed or the level of risk has increased because of the software update***, as is generally the case for software revisions. The Commission should issue guidelines on how to determine what constitutes a substantial modification***.

Issue: **Scope, without a clear focus on cybersecurity risk**

Recitals and articles: **Art. 2 (1) & Art. 3 (1)**

Comment: Art. 2 (1) in combination with the definition of products with digital elements in Art. 3 (1) covers all products that possess an indirect logical or physical data connection. This broad scope of application of the CRA will lead to significant problems and delays in implementation, especially in standardization, and consequently in conformity assessment.

Recommendation for changed text: The scope should be narrowed to products, which possess a relevant risk, inherently benign products should be excluded:

This regulation applies to products with digital elements whose intended, or reasonably foreseeable use includes a logical or physical data connection to a device or network, **and which are not inherently benign.**

The concept of inherently benign products was already introduced in recital 12 (inherently benign in terms of electromagnetic compatibility) of the EMC-directive (2014/30/EU), we think it would also be of beneficial use in the context of the CRA referencing to cybersecurity (inherently benign in terms of cybersecurity). To ensure, that such a differentiation to exclude "inherently benign" products does not lead to a circumvention of the CRA it is crucial to define the term accordingly:

3 (4a) inherently benign product means a product which cannot cause a cybersecurity risk, because it is technically too limited,

Such an exemption would lead to more legal certainty without lowering the resilience, as it only would exclude inherently benign products, like simple sensors, circuits or switches. Further clarification for the identification of inherently benign product could be needed, e.g. through guidelines or delegated acts.

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 should not be seen under the scope of the CRA, as those products are only capable to perform simple signal processing.

Issue: **Essential product requirements – functional separation of security updates from functionality updates**

Recitals and articles: **Annex I 1. (4) (aa) (EP) & recital 32b (EP)**

Comment: The German Electro and Digital industry is concerned by the functional separation of security updates from functionality updates as it is proposed by the Parliament: For a lot of products with digital elements it is often not feasible not only from a technical point of view but from an organizational point of view as well. First, there could arise the need to change certain minor functional aspects to make a security update work as security is intertwined in the software. Secondly, especially SMEs are already hard pressed by the requirements of the CRA. They are already forced by limitations in capacities to bundle update releases, being forced to plan and carry out every security update and functional update separately will increase their workload and therefore burden their already strained capacities further without a clear need to do so. In the case of new vulnerabilities those of course have to be handled according to article 10 and Annex I (2) "without delay", but even in those cases already planned updates could be used to deliver those security updates even faster by adding them to the release of the update.

Recommendation for deletion of Parliament text: **We recommend from abstaining from a requirement of – functional separation of security updates from functionality updates.**

Issue: **Essential product requirements – automatic updates**

Recitals and articles: **Art. 10 (6) (EP), Annex I 1. (4) (aa) (EC), I 1. (4) (ab) (EP), Annex I 1. (4) (k) (EC), Annex I 2. (6) (2) (EP) & Recital 11a (EC)**

Comment: It is problematic to call for automatic updates in general and without distinction, as there are environments, especially considering operational processes in industrial manufacturing, where this requirement could interfere with operations. In our understanding the different adaptions done by the Council and the Parliament to include automatic updates in the requirements for the cases, where they could be useful, especially in the B2C-context, and to exclude them for cases, where they are problematic show the difficulties to address this issue properly. Both attempts are confusing, we therefore call to keep the original proposal by the Commission, which did not regulate this detail in such a problematic granularity. To highlight and encourage the use of automatic updates where possible, we recommend adding recital 11a as proposed by the Council.

Recommendation for : **We recommend the Commissions original text in regard to automatic updates and welcome the adaption of recital 11 (a) by the Council**

Issue: **Essential vulnerability handling requirements – security updates free of charge**

Recitals and articles: **Annex I 2. No. (8) (EP)**

Comment: We welcome the addition of the Parliament as it reflects the realities especially in the B2B-context where long product lifetimes and long lasting contractual organized support are usual, making free of charge updates unreasonable. Unfortunately, the current Parliament text could become ineffective due to national laws like the German AGB-Law[1]. In case of the German AGB-Law the mentioned agreement between parties is nearly impossible to reach in a way, which is legally incontestable. Therefore, to allow agreements on a charge for security updates in principle for the business-to-business contexts with legal certainty, the logic in the wording has to be turned around.

Recommendation for adjusted Parliament text: **We recommend the Parliament text in Annex I 2. No. (8) with the following change:**

> Annex I 2. No. (8) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and, ~~**unless otherwise agreed between the parties in a business-to-business context,**~~ **between parties in a business-to-consumer context** free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken;

Issue: **Manufacturer obligations – instructions of use in electronic form**

Recitals and articles: **Art. 10 (10)**

Comment: It is increasingly important to allow the use of new digital formats to fulfil the information requirements of product legislations, especially in the case of the CRA, which addresses tangible and intangible products, like standalone software, as well. Additionally, the possibility to use electronic forms promotes digitalization efforts and saves on printed paper, thereby reducing waste and energy and resource consumption.

In article 10 (7) of new machinery directive (EU) 2023/1230 the legislators already found a fitting solution, which allow for the usage of electronic forms and also enables new digital solutions, like the Digital Product Passport (DPP).

Recommendation for Parliament text: **ZVEI therefore strongly welcomes and recommends the addition made by the Parliament in art. 10 (10.)**

The orientation and use of the wording of the new machinery directive is particularly important, as this wording should constitute a blueprint for this aspect in other regulations in the future.

Issue: **Documentation of risk assessment**

Recitals and articles: **Art. 10 & recital 32aa**

Comment: In our opinion the major strengths of the CRA is its risk based approach, which allows to identify the appropriate security measures according to the intended use and the intended operational environment of a product through a risk assessement. This process of identifying the essential requirements applicable to a respective product and the security measures needed for an appropriate level of security has to be documented. In our understanding therefore the “clear justification” only refers to the correct documentation of the risk assessment, and not a separate justification.

Recommendation for Council text: **We therefore welcome the newly added recital 32aa of the Council, as it makes this process clearer.**

[1] Background information in German could be found in the following ZVEI position: https://www.zvei.org/presse-medien/publikationen/industrie-40-ermoeglichen-reform-des-deutschen-agb-rechts-im-b2b-flyer

Issue: **Penalties**

Recitals and articles: **Art. 53**

Comment: The implementation of CRA, although being a worthwhile effort, will put substantial additional strain on the already quite burdened European industry. The implementation will be a process, which will take definitely more time, than the co-legislators are currently foreseeing with 24 to 36 months. Europe is the first market, which introduces such an exhaustive, detailed and demanding regulation regime for product security. It is therefore not understandable, why the CRA as the product regulation, which lays down the most ambitious goals for one of the newest regulation targets also has the highest penalties of all other product regulations by referencing fines as percentages of total worldwide annual turnover.

Recommendation for deletion or change: **In orientation to other regulations, like the new machinery regulation (EU) 2023/1230 we recommend the deletion of article 53 (3) to article 53 (5) or at least the following change in all three sub-articles to ensure proportionality and not overburden European industry in an ever more competitive international environment:**

> Art. 53 (3) […] shall be subject to administrative fines of up to 15 000 000 EUR or, if the offender is an undertaking, up to 2,5 % of the ~~its~~ total ~~worldwide~~ annual turnover for the **respective product in the European market in the** preceding financial year, whichever is higher.
>
> Art. 53 (4) […] shall be subject to administrative fines of up to 10 000 000 EUR or, if the offender is an undertaking, up to 2 % of the ~~its~~ total ~~worldwide~~ annual turnover for the **respective product in the European market in the** preceding financial year, whichever is higher.
>
> Art. 53 (5) […] shall be subject to administrative fines of up to 5 000 000 EUR or, if the offender is an undertaking, up to 1 % of the ~~its~~ total ~~worldwide~~ annual turnover for the **respective product in the European market in the** preceding financial year, whichever is higher.

Issue: **Transitional provisions – no staggered approach**

Recitals and articles: **Art. 55**

Comment: Some sectors, e.g., non-road mobile machinery (NRMM), the rail sector, machine builders, system integrators, and end users will need additional time for implementation. In keeping with a phased approach, longer transitional arrangements will be necessary for such sectors. We are especially concerned for non-road mobile machinery because compliance with the CRA will entail numerous complex modifications to NRMM, not just for the software, but also for the hardware, therefore impacting the entire architecture of the machinery. A product upgrade for the non-road mobile machinery sector takes normally 3 to 5 years, and the lifecycle of a particular product platform could be 20 years. The current scope would also mean that all sensors, actuators and controllers currently deployed in the machine for internal functions, with low cyber-risk, must be checked as well. As some of these significant changes will inevitably affect the different functions and related health and safety compliance, the new CRA-related obligations trigger a complete redesign and re-homologation of the machinery.
Therefore, we call for an additional 24 month transition period for non-road mobile machinery, on top of the below overall 48 months transitional period.

Recommendation for changed text: **We recommend adding the following new provision to article 55:**

> *new* Art. 55 (4a.) By way of derogation, for non-road mobile machinery as defined in Regulation (EU) 2016/1628, and agricultural vehicles as defined in Regulation (EU) 167/2013, the application date referred to in Article 57 is extended by 24 months.

Issue: **Data base on security support periods**

Recitals and articles: **Article 41 (9)**

Comment: The Parliament calls in article 41 (9) for the establishment of a data base about “the average support period set by the manufacturers, as well as when available the average expected product lifetime, and

disaggregated per category of product with digital elements." We understand the intention, but this data base would not have the desired effect. This is because of the following reasons: (1) This data base can always only look at the past, therefore it is of little use for current purchasing decisions as it does not compare the current offerings. This possibility of comparison on the other hand is already covered by the transparency requirements of the manufacturers. (2) This data base would disadvantage manufacturers of products, which try to lead the way in regard of long support periods and lifetimes as the focus on the average would blur their efforts. (3) It is nearly impossible to find a right balance of detail of product categories, either quite different products would be compared, or the sample sizes will be too small.

Recommendation for deletion of Parliament text: **We recommend, to abstain from establishing such a data base, which will have no practical use as it will only generate the illusion of transparency for purchase decisions.**

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

05.10.2023