ZVEI:
Die Elektroindustrie

White Paper

Horizontal Product Regulation for Cybersecurity

Using the Strengths of the New Legislative Framework for the Digital Single Market

December 2018

German Electrical and Electronic Manufacturers' Association

ZVEI:
Die Elektroindustrie

Horizontal Product Regulation for Cybersecurity

Published by:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
ZVEI - German Electrical and Electronic Manufacturers' Association
Security and Safety Division
Lyoner Strasse 9
60528 Frankfurt am Main, Germany

Responsible: Lukas Linke
Telefphone: +49 69 6302-432
E-mail: linke@zvei.org

Editorial: ZVEI Working Group Cybersecurity

www.zvei.org
December 2018

Contents

1 The need for harmonisation

The challenge: The environment of human beings, companies and states is increasingly shaped by digitalization and networkable end products. Digitalization produces genuine benefits. At the same time, the responsibility of each end product and thus of each manufacturer rises, since networkable end products may be integrated into larger systems (such as communications networks, smart home systems or power grids). The Internet of Things (IoT) will ultimately enable everything to be connected with everything else. In consequence, compromised products may influence the entire system, and the sum of many compromised connected products may impact the environment, health, and ultimately life itself. Unless essential cybersecurity measures are taken, this may result in adverse impacts upon societies and public security.

The consequence: In view of these challenges and recent events (such as Mirai, WannaCry, the hacking of routers, etc.), it is understandable that the EU Commission and national governments are addressing cybersecurity in the interests of consumer protection. Germany's ruling coalition has decided to draw up a second IT security law, intended to cover companies and products outside the critical infrastructures as defined today. In addition, the coalition makes provision for introduction of a label for the IT security of networkable consumer goods. The German Federal Office for Information Security (BSI) has already launched the first pilot projects for technical guidelines governing broadband routers and the area of smart home products. It is becoming clear that policymakers are widening their focus to include products beyond the existing scope for operators of critical infrastructures. At EU level, a European framework for cybersecurity certification is about to be introduced (see EU Cybersecurity Act). Furthermore, serious consideration is being given to adding cybersecurity requirements to existing product directives[1] such as the Radio Equipment Directive or Machinery Directive (refer to Chapter 4 for an overview).

The response of the electrical industry: In the view of the electrical industry, the initiatives concerned must under no circumstances result in cybersecurity being regulated inconsistently or at national level. A clear need exists for product regulation concerning cybersecurity to be harmonised throughout the EU and to be compatible with international standards and WTO agreements. Meeting these stratigic goals in close cooperation with industry is the task of European policymakers. In contrast, incorporating cybersecurity into existing product regulations will weaken the competitiveness of European companies

Conflicting and incompatible security requirements for individual products must be avoided. No sector by sector approach.

The electrical industry favours an EU-wide horizontal product regulation for the cybersecurity of networkable end products. Doing so, we can establish risk-based EU-wide basic cybersecurity requirements within the well proven New Legislative Framework.

A joint course of action by European policymakers and industry should instead have the objective of establishing binding cross-domain and industry-wide security objectives for networkable end products.

[1] The authors are aware that a large number of EU product regulations now exist. The appropriate legal term would therefore be „harmonisation legislation for products". However, since the White Paper is intended for a broad readership, including technical lay persons, the text continues to use the term „product directives", in the interests of readability and comprehensibility.

This proposal is coupled with clear expectations on the part of the electrical industry for cybersecurity actually to be enhanced within the EU and its compatibility with the needs of industry to be assured:

1. No addition of security requirements to existing European regulatory instruments for products (see Chapter 4)
2. No national product requirements or test regulations for cybersecurity beyond those laid down for public authorities or the high-security domain (e.g. military and public authorities); the ZVEI regards a uniform course of action across Europe as crucial
3. Use of the established „New Legislative Framework" (NLF) as a basis for the structure of a horizontal regulation (see Chapter 2)
4. A level playing field for manufacturers and importers
5. Transitional arrangements and provisions for installed and in use solutions, compatible with the needs of industry
6. Maintaining the flexibility and innovative capacity of manufacturing companies

Shared responsibility: Enhancement of cybersecurity requires the involvement of all stakeholders: manufacturers, users, and in the industrial sphere in particular, operators and integrators. An isolated measure is not sufficient to achieve adequate protection; well-coordinated measures must be implemented. The goal is clear: networkable end products must possess an adequate robustness and cybersecurity. The users however have a decisive role in using the end products with consideration for security. In the industrial environment, operators must suitably integrate end product into their solutions, configuring them and maintaining the solution's achieved level of protection throughout its lifetime.

Products as one element of holistic cybersecurity – further steps required: From the challenge described above, it follows that a need exists for the Internet of Things to be made secure. The „things" in the Internet of Things are, first and foremost, networkable end products (for the definition, refer to Annex 1). A horizontal product regulation could enhance cybersecurity overall and reflect European competence in this area. It is nevertheless clear that further aspects of cybersecurity must be considered: services, platforms, and the obligations of operators and users. Major liability and warranty issues must also be clarified. Solutions to these aspects must be found outside product regulation. Accordingly, these aspects are not addressed by this White Paper.

The White Paper and Annex 1 present the electrical industry's vision how a horizontal product regulation for cybersecurity could look like and be successful. It is intended to initiate a broad debate and does not seek to pre-empt the pending political process. Its content is open to discussion. At the same time, the paper reflects ZVEI member companies' understanding of cybersecurity as an inherent component of product quality, which must therefore be the subject of continual further development.

2 Foundation: the New Legislative Framework

For end products to be regulated effectively, a number of different principles must be considered:

„Better Regulation" principle	„SMERC" principle for requirements
• Regulation lays out the general protection goals; details and requirements are defined through norms and standards • Graded and risk-based • Maintaining of manufacturers' flexibility in implementing the provisions • Incorporation of international standards • WTO acceptance and international compatibility • Level playing field for manufacturers and importers • Neutral with respect to technology and solutions	• Specific – requirements must be considered with respect to the specific application • Measurability – requirements must be clearly measurable/verifiable • Enforceability – compliance with requirements must be enforceable by the market surveillance authorities • Relevance – requirements must be relevant to security and the users • Competition-friendly – significant impacts detrimental to the competitiveness of industry must not arise

The ZVEI is convinced that the New Legislative Framework (NLF) constitutes an ideal foundation for regulatory implementation of these principles. Since the NLF's establishment in the 1980s under the heading of the „New Approach" and its revision in 2008, considerable experience has been gathered in both sectoral regulation (such as the Machinery Directive) and horizontal regulation (such as the EMC Directive). In the view of the electrical industry, no model is better suited to the creation of a regulatory basis for networkable end products for the European Single Market.

The electrical industry calls for taking „SMERC" and „Better Regulation" as foundational principles for cybersecurity regulation, in order to strengthen innovation and be consistent with the needs of industry.

Cybersecurity is a cross-sectional phenomenon. In the future, no area of society or industry will remain untouched by it in some way. The specific underlying conditions in the various areas differ however in some cases with respect to cybersecurity. This raises the question whether it is even possible to address cybersecurity horizontally or whether it should preferably be regulated on a sector-specific basis.

3 Feasibility: a Horizontal Approach for Cybersecurity

From a legal perspective, this challenge is not new. The EMC Directive for example governs electromagnetic compatibility horizontally, completely irrespectively of where the phenomenon of EMC arises. As a „catch-all" directive, it can extend to and govern end products in the most diverse locations of use.

The ATEX Directive covering the area of explosion protection can be regarded as a further model. This directive makes provision in particular for manufacturers themselves to set out the intended use, and therefore the hazard categories, of their products. This in turn yields the respective product requirements specified by the directive and the conformity assessment procedure. The assurance of explosion protection is however not only based upon the regulation for the placing of products upon the market, which is geared to manufacturers, but is also supplemented by regulations governing the operation of ATEX products (Directive 1999/92/EC). Hence, this places requirements upon the operator, such as the classification of hazardous zones, organizational measures, and criteria for the selection of suitable equipment. These aspects are relevant to cybersecurity as well.

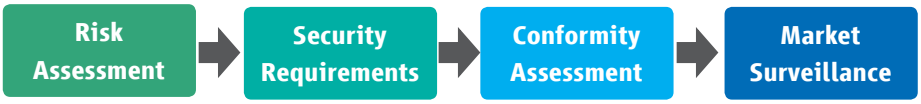
These models show that a regulation is suitable to cover a horizontal phenomenon, to set out requirements of general validity, and to support them within standards with respect to specific sectors. To what extent is this approach transferable? The objectives of cybersecurity (availability, integrity and confidentiality) can be applied horizontally to all areas of application, albeit with differences in their prioritization, as a function of the respective risk and threat analysis. The assurance of these cybersecurity objectives is important in all domains for the security, robustness, and stability of the Internet of Things. In the future, the properties of networkable end products must be such that they assure at least a basic cybersecurity in consideration of the risk in accordance with the state of the art (as defined in international standards) and their intended use.

The opportunity presented by the horizontal approach is also that of formulating uniform requirements concerning cybersecurity for the greatest possible number of networkable end products by way of a binding mandate to standardisation bodies or other suitable platforms. This creates a basis for end products that fail to satisfy the required cybersecurity to be excluded from the EU Single Market. The setting out of a generic and mandatory security objective creates a common foundation upon which more uniform measures for wide-ranging implementation can in turn reliably be created. In the same time, this approach allows for sectors with stricter security requirements to keep their established requirements, when these go beyond the basic cybersecurity requirements.

The electrical industry's view is that cybersecurity can be and must be addressed horizontally, despite its lack of physical measured values. The guiding principles are the risk-based approach and the state of the art.

The EMC and ATEX Directives serve as best-practice models.

In addition to its horizontal approach, the NLF covers all aspects of the security chain and makes it available for the entire EU Single Market. Current debates focus mainly on (functional) requirements and ways of conformity assessment for cybersecurity. It is not sufficient however for discussion to be limited to one or two aspects. Only when risk assessments precede the definition of security requirements, followed by a suitable system of conformity assessment and market surveillance, cybersecurity will be strengthened overall.



4 A horizontal regulatory instrument for cybersecurity supplements current European regulation and initiatives

NIS Directive and GDPR

The NLF approach to product regulation is the logical extension of the existing regulatory framework for cybersecurity. Up to now, the operators of critical infrastructure and services have been addressed through the NIS Directive. Secure infrastructure and services must in turn be underpinned by secure products. The same applies to consumer protection and the General Data Protection Regulation, which are also conditional upon basic cybersecurity in networkable end products. Infrastructures, networks, companies and end products must therefore be considered together in the enhancement of cybersecurity. In this respect, the approach of the NLF supplements the NIS Directive and GDPR.

Cybersecurity Act

The horizontal approach to cybersecurity can also support the new EU Cybersecurity Act. This Act represents a valuable first step in the harmonization of existing national certification schemes. Companies can show a voluntary security commitment to their customers for the B2C and B2B markets (outside critical infrastructures) harmonised throughout Europe. The Cybersecurity Act also addresses processes and services, two areas that must be added imperatively to the product focus. The horizontal NLF approach goes a step further and lays the foundation for mandatory, harmonised basic cybersecurity for end products on the EU Single Market. In combination, the two approaches "EU-wide basic cybersecurity" and "security certification" for high-risk environments" can become a European core brand. They set new international standards and express our European values of personal sovereignty and trust through cybersecurity. This is conditional however upon a horizontal regulatory instrument for products.

Common Criteria

The focus of the Common Criteria (CC) and the Mutual Recognition Agreement of Information Technology Security Certificates (SOG-IS MRA) lies upon security products and the high-security area. Correspondingly high specific requirements apply to the products and evaluation methods. These requirements do not readily scale to the normal B2B and B2C mass market. The NLF approach can be implemented without difficulty parallel to the sphere of the CC and without impact upon it.

Existing EU regulatory instruments for products

As outlined in the first chapter, the EU Commission considers to integrating cybersecurity into certain existing product directives. The following regulatory instruments are under consideration: the Radio Equipment Directive (RED), Machinery Directive (MD), Low-voltage Directive (LVD) and Medical Devices Directive (MDR).

In the view of the electrical industry, cybersecurity should not be integrated into existing product directives for four reasons.

1. It would be virtually impossible to retain mutual compatibility between the various different requirements. Owing to differences in perspective and different parties being involved, the legislative processes in the Parliament and Council alone make the creation of a consistent regulatory system unlikely.
2. Attaining consistent regulation is very time-consuming. The ZVEI is therefore highly sceptical of the argument that additions to existing directives can be implemented more swiftly.
3. "White spots" and missing links would follow. Even were security requirements to be incorporated into all four directives, more areas would remain unaffected than if networkable end products were regulated horizontally.
4. Limited public awareness. Splitting the security requirement across multiple legislations is an obstacle to the raising of awareness for cybersecurity among the public. Conversely, a horizontal regulatory instrument can enhance awareness for cybersecurity and ultimately of European competence in this area, both in Europe and abroad.

The horizontal NLF approach is also compatible with the sectors for which product-specific security requirements already exist. In these cases, the following assessment should be made:

1. Does the existing product regulatory instrument contain requirements governing cybersecurity? If so, following the Lex Specialis principle, the more specific principles apply. Accordingly, sector-specific regulation external to the NLF approach with its CE marking, such as individual or type approval for example in the automotive or railway sector, can be retained, provided the same or a higher security objective is reached.
2. Should no security requirements exist, at least the horizontal requirements initiated by the NLF approach described here should apply. Within the Lex Specialis principle, higher or additional security requirements can also be specified in the sectors at a later stage should a specific need exist.

Annex 1: Possible Content of a Horizontal Product Regulation bBased on the NLF

This annex is intended to outline a possible layout of horizontal product regulation for cybersecurity along the lines of the NLF. The structure has been adopted from the framework of Decision No 768/2008 and the EMC Directive. The content of this annex is intended to provide a solid basis for further exploration for further discussion. ZVEI's members are open to get involved with European policymakers and stakeholders.

Possible content of an EU regulation based on the model of the EMC Directive

A.1 Subject matter

The subject of the regulation is the cybersecurity of networkable end products. It calls for a level of cybersecurity that is risk-based and commensurate with the state of the art.

A.2 Scope

This regulation applies to networkable end products as defined under „Definitions".

In accordance with the Lex Specialis principle, this regulation does not apply to end products of which cybersecurity is governed specifically in other directives or regulations. In other words, more specific requirements take priority. Should however a deviation arise between the more specific requirements and the horizontal NLF regulatory instrument, the deviation must be eliminated by application of the latter

A.3 Essential requirements for cybersecurity

Networkable end products must be designed and manufactured in consideration of the risk and the state of the art such that, under intended or reasonably foreseeable use, they:

a. do not significantly compromise or impair the cybersecurity of other networkable end products;
b. provide adequate resistance to anticipated cybersecurity threats without significant impairment of their use.

Note: The ability to achieve a higher level of cyber security, or the availability of other end products that present a lower risk, is not a sufficient reason to consider an end product to be insecure.

Note: Any specific technical and process-related requirements are set out in standards and specifications. The objective is the creation of a horizontal security standard that can be supplemented or substituted by sectoral security standards (as in the Lex Specialis approach). An important principle of the NLF is that the regulatory instrument does not set out technical specifications; only the objective of protection is set out in binding form.

A.4 Definitions

A.4.1 Specifically:

Networkable end products:
a. Products intended for communication directly or indirectly over the Internet;
b. Products for which direct or indirect communication over the Internet is reasonably foreseeable, irrespective of their intended use.

Networkable end products also include the associated embedded firmware and software that is essential for the primary function of the end product and is either
c. pre-installed on an end product in accordance with 1a or 1b, or
d. placed on the market by the hardware manufacturer or a software manufacturer commercially, separately, and at a later stage for an end product in accordance with 1a and 1b, for example in the form of an extension to functionality or an update.

Note: As with virtually any regulatory instrument, arrangements for necessary exemptions must be discussed at a subsequent stage. Such discussions do not fall within the scope of the present White Paper.

Note: The term „end product" also includes the sphere of „solutions", i.e. the nesting of end products to form a complex solution.

Note: In the sections below, the term „product" is used in all cases in the sense of an „end product".

Cybersecurity in the sense of this regulation:
Cybersecurity encompasses all measures and capabilities of a product (hardware and software) for assurance of the confidentiality, availability and integrity required for assurance of its intended use.

A.4.2. Adopted from 765/2008:

Making available on the market: Any supply of a product for distribution, consumption or use on the Community market in the course of a commercial activity, whether in return for payment or free of charge

Placing on the market: The first making available of a product on the Community market

Manufacturer: Any natural or legal person who manufactures a product or has a product designed or manufactured, and markets that product under his name or trademark

Distributor: Any natural or legal person in the supply chain, other than the manufacturer or the importer, who makes a product available on the market

Harmonised standard: A harmonised standard as defined in Article 2 (1) c of Regulation (EU) 1025/2012

Accreditation: Has the meaning assigned to it by Regulation (EC) 765/2008

National accreditation body: Has the meaning assigned to it by Regulation (EC) 765/2008

Conformity assessment: The process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled

End user: Any natural or legal person, residing or established in the Union, to whom a product was made available either as a consumer outside any trade, business, craft or profession, or as a professional end user in the course of his industrial or professional activities

Note: Regulation (EC) 765/2008 makes provision for further market players, such as the importer, authorised representative and distributor. In order to reduce the scale and complexity of the annex, these roles have not been included in this initial step; they would of course need to be included in any complete analysis in order to satisfy the reality of e-commerce.

A.5 Obligations of the market players

A.5.1 Manufacturers

1. When placing their products on the market, manufacturers shall ensure that they have been designed, manufactured and assessed in accordance with the essential requirements (see A.3).

2. Manufacturers shall draw up the necessary technical documentation and carry out the relevant conformity assessment procedure or have it carried out.

3. Where compliance of the product with the applicable requirements has been demonstrated by that procedure, manufacturers shall draw up an EU declaration of conformity and affix the CE marking.

4. The obligations with respect to the conformity assessment procedure, declaration and marking do not apply when, during manufacture of the product:
   - products are used that fully satisfy the cybersecurity requirements of this regulation;
   - these products are installed as intended, and
   - the cybersecurity of the product as a whole is ensured as a result.

   This requires assessment by the manufacturer combining the products of whether the combining of the products may necessitate further measures.

5. Manufacturers shall keep the technical documentation and the EU declaration of conformity [normally for 10 years] after the product has been placed on the market.

6. Manufacturers shall ensure that procedures are in place for series production to remain in conformity and that changes in product design or characteristics and changes in the harmonised standards or in technical specifications by reference to which conformity of a product is declared are adequately taken into account.

7. Manufacturers shall, if necessary, keep a register of complaints, of non-conforming products and product recalls, and shall keep distributors informed of any such monitoring.

8. Manufacturers shall ensure that their products bear a type, batch or serial number or other element allowing their identification, or, where the size or nature of the product does not allow it, that the required information is provided on the packaging or in a document accompanying the product. This also applies to software constituting a networkable end product in accordance with A.4.1.

9. Manufacturers shall indicate their name, registered trade name or registered trade mark, and the address at which they can be contacted, on the product or, where that is not possible, on its packaging or in a document accompanying the product. This also applies to software constituting a networkable end product in accordance with A.4.1.

10. Manufacturers shall ensure that the product is accompanied by instructions, safety information and information on cybersecurity, as well as the product category (see A.6) in a language which can be easily understood by consumers and other end-users, as determined by the Member State concerned.

11. Manufacturers shall publish in unambiguous and transparent form the period of time or point in time within which or up to which they will make support and corrective measures available for their product. Up to this date, manufacturers who have reason to believe that a product placed by them on the market no longer adequately assures cybersecurity in consideration of the current state of the art shall immediately undertake required corrective measures. Examples of possible corrective measures are updates, compensatory measures or information and instructions for operators and end users.

12. Manufacturers shall further immediately inform the central competent European authority should the product present cybersecurity hazards to the general public or hazards to the life and health of persons.

    Note: No central authority exists for this procedure at the present time. The procedure by which it is to be ensured that companies throughout Europe need report to only a single body is to be clarified in a later step.

13. Manufacturers shall, further to a reasoned request from a competent national authority, provide it with all the information and documentation necessary to demonstrate the conformity of the product, in a language which can be easily understood by that authority. They shall cooperate with that authority, at its request, on any action taken to eliminate cybersecurity risks posed by products which they have placed on the market.

A.5.2 Integrators

The legal role of the integrators is dependent on a case-by-case basis upon the influence of their integration work upon the cybersecurity of the end product that they assemble:

- When integrators solely use products fully assessed in accordance with this legal instrument, the obligations and procedures are reduced (refer to No 4 in A.5.1.). This can lead to the integrator acquiring the role merely of a distributor within the NLF.
- Should however the integration work have an influence upon the cybersecurity of the end product, the integrator has the role of a manufacturer. In this case, the integrator must assess and declare the cybersecurity of the complete end product assembled by him. Provided the components used have already been assessed and are used as intended, the integrator can however also adopt the results of conformity assessment for these components (refer to Point 3 of Module A in A.7.1.).

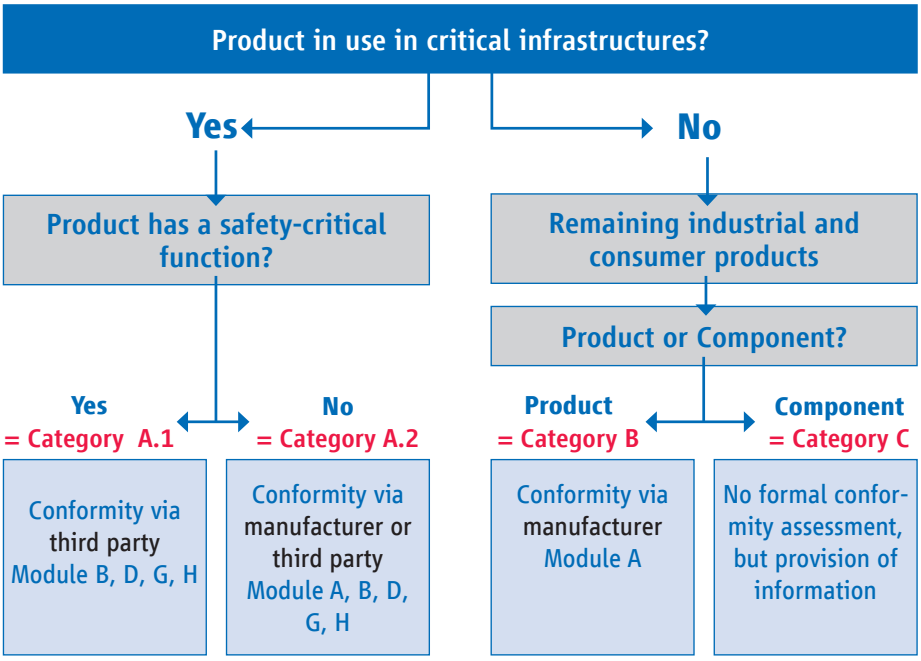
Note: In the sphere of consumer goods and private individuals, the role stated here may be associated with other (legal) obligations and/or understood differently. The differences arising between the obligations in this case and those stated here must be evaluated and stated in a subsequent step.

Note: As already referred to in the main part of the White Paper, the operator's obligations constitute a substantial element of the security chain in the context of shared responsibility. Operator obligations are not governed in a regulatory instrument for a product; they are addressed for example in the German Workplace Ordinance (ArbStättV). It is clear that the operator's obligations may have to be extended in other regulatory instruments. These include, for example, the installation of updates and the continual patching of products as part of operator-specific risk assessment and reduction.

A.6 Classification and product categories

Note: The requirements concerning the security functions and the security process are set out in standards, and not by the conformity assessment module. In theory, Modules A to H may all relate to the same standard. Module A may consequently also contain demanding requirements

Overview:



Note: The authors are aware that multiple approaches and conventions exist (for example with regard to functional security) for the creation of a decision tree. The approach selected here is intended in the first instance to permit the easiest and swiftest classification. The module selection presented here is derived from the assessed risk environment, but must of course be extended subsequently.

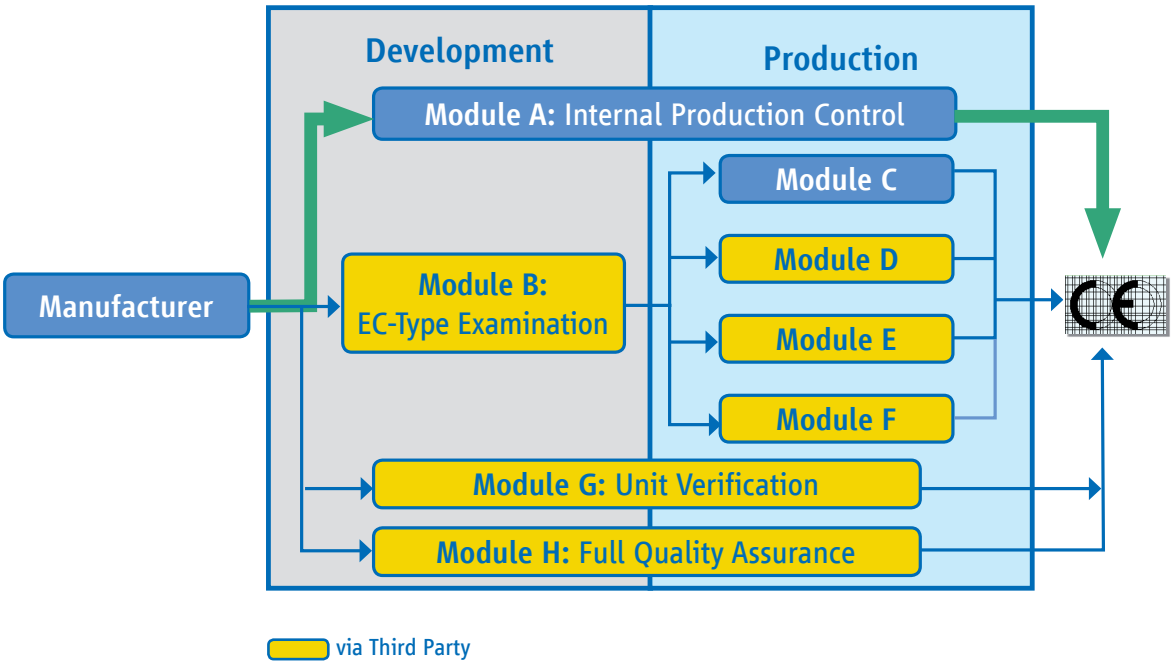
Explanation:

Product Category	Explanation	Specification of the module
A.1	Networkable products intended for use in critical infrastructures and the failure, malfunction or manipulation of which would pose a threat to the security of the infrastructure	Involvement of a third party by one of: Modules B + D Module G Module H
A.2	Networkable products intended for use in critical infrastructures and the failure, malfunction or manipulation of which would not endanger the security of the infrastructure	Involvement of a third party by one of: Module A Modules B + D Module G Module H
B	All other networkable products	Module A with manufacturer's own declaration
C	Networkable products that are intended to be fitted by a manufacturer as components into other products or installations and that therefore contain only limited security functionality	No conformity assessment method, but provision of information to the user regarding the cybersecurity measures taken. „What can the component do and what can it not do?"

A.7 Overview of conformity assessment methods

It is to be assumed that Module A can be used for numerous networkable products in the low-risk environment. It is therefore described separately here in order to permit an initial impression.

Overview: Conformity assessment method in accordance with the NLF
(Annex 2 of Decision No 768/2008/EU)



Overview of the Module A requirement (in accordance with 768/2008) – Internal production control[3]:

1. Internal production control is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 4, 5 and 6, and ensures and declares on his sole responsibility that the products concerned satisfy the requirements of the legislative instrument that apply to them.

2. Assessment of the cybersecurity: The manufacturer shall assess the cybersecurity of his product in order to determine whether it satisfies the essential requirements in accordance with Annex A.3. During assessment of the cybersecurity, all usual conditions shall be considered that can be anticipated during intended and reasonably foreseeable use.

3. Use and assessment of components: Where components are used/combined as intended for a product, the manufacturer can adopt the results of conformity assessment for these products with respect to the cybersecurity.

4. Technical documentation: The manufacturer shall establish the technical documentation. The documentation shall make it possible to assess the product's conformity to the relevant requirements, and shall include an adequate analysis and assessment of the risk(s).[4] The technical documentation shall specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and operation of the product.

[3] Note: The requirements 2 and 3 of Module A also apply to the other modules.
[4] International standards and specifications may serve as the basis for the risk analysis.

The technical documentation shall, wherever applicable, contain at least the following elements:

- A general description of the product including its specified product class in accordance with A.6.
- Descriptions and explanations necessary for the understanding of this documentation and the operation of the product
- A list of the harmonised standards and/or other relevant technical specifications the references of which have been published in the Official Journal of the European Union, applied in full or in part, and descriptions of the solutions adopted to meet the essential requirements of the legislative instrument where those harmonised standards have not been applied. In the event of partly applied harmonised standards, the technical documentation shall specify the parts which have been applied
- Results of design calculations made, examinations carried out, etc.
- Test reports

5. Manufacturing: The manufacturer shall take all measures necessary so that the manufacturing process and its monitoring ensure compliance of the manufactured products with the technical documentation referred to in point 4 and with the requirements of the legislative instruments that apply to them..

6. Conformity marking and declaration of conformity:
   a. The manufacturer shall affix the required conformity marking set out in the legislative instrument to each individual product that satisfies the applicable requirements of the legislative instrument.
   b. The manufacturer shall draw up a written declaration of conformity for a product model and keep it together with the technical documentation at the disposal of the national authorities for 10 years after the product has been placed on the market. The declaration of conformity shall identify the product for which it has been drawn up. A copy of the declaration of conformity shall be made available to the relevant authorities upon request.

7. Authorised representative: The manufacturer's obligations set out in point 6 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.

Note: The existing CE directives always assume hardware for which only the concept of application of CE marking to the product is appropriate. For software that is placed on the market independently of an item of hardware, for example by download, an equivalent solution must thus be found in a subsequent step. The exploration of such a solution lies outside the scope of the present White Paper, however.

A.8 Further information on structuring of the regulation

A.8.1 Relevance of market surveillance

Market surveillance is governed generically, for example in Regulation (EC) 765/2008. Effective and functioning market surveillance is important if the regulation is to be effective.

A.8.2 Role of international security standards

Presumption of conformity: Where networkable products satisfy harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union, conformity is presumed with those requirements of A.3. that are covered by the standards or parts thereof concerned. International standards are generally given priority in European standardization activity in accordance with the Frankfurt and Vienna agreements.

A.8.3 Transitional periods

The transitional periods are to be defined in consideration of the respective product life cycles. Staggered transitional periods would appear advantageous. In accordance with normal practice, the transitional period should begin at publication in the Official Journal for products that are then placed on the market (= relinquishing onto the market by the manufacturer, or crossing of the external EU border in the case of imported products).

A.8.4 Dealing with installed solutions and inventory

Die aus diesem Vorschlag resultierenden Anforderungen gelten nur für neu in VerThe requirements resulting from this proposal apply only to end products newly placed on the market following expiration of the transitional periods. Products already placed on the market and installed are not affected; no obligations therefore arise for the manufacturers.

Furthermore, it may be the case, particularly in the industrial environment, that end products that have already been produced but not yet placed on the market are in storage and are not to be placed on the market until several years later. Reasonable transitional periods in the sense of A.8.3. must be specified for this particular situation. Conventional exemption arrangements must be formulated in the context of the necessary supply of spare parts.

It thus follows that the existing practice should be continued according to which, should products no longer satisfy the state of the art with respect to cybersecurity, for example owing to a change in the risk environment, manufacturers may continue to place them on the market by way of a change in or limitation of their intended use (refer to the principle of continued marketability). This adaptation of the intended use to the risk environment must of course be communicated to the end customer and made technically possible (for example by means of updates where required). In addition, “Defence in Depth” concepts are suitable in order to operate a solution securely, although some end products within that solution may not reach the state of the art anymore.

About the ZVEI

The ZVEI (Zentralverband Elektrotechnik- und Elektronikindustrie e. V.) represents the common interests of the electrical industry and associated service companies in Germany. Around 1,600 companies have chosen to become members of the ZVEI. The sector employs over 872,000 people in Germany and a further 706,000 throughout the world.

The ZVEI represents a sector with revenues of €192 billion in 2017. Around 40% of these are attributable to novel products and systems. One new development in three in manufacturing industry overall has its origins in the electrical industry.

ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e.V.
Lyoner Straße 9
60528 Frankfurt am Main
Telefon: +49 69 6302-0
Fax: +49 69 6302-317
E-Mail: zvei@zvei.org
www.zvei.org