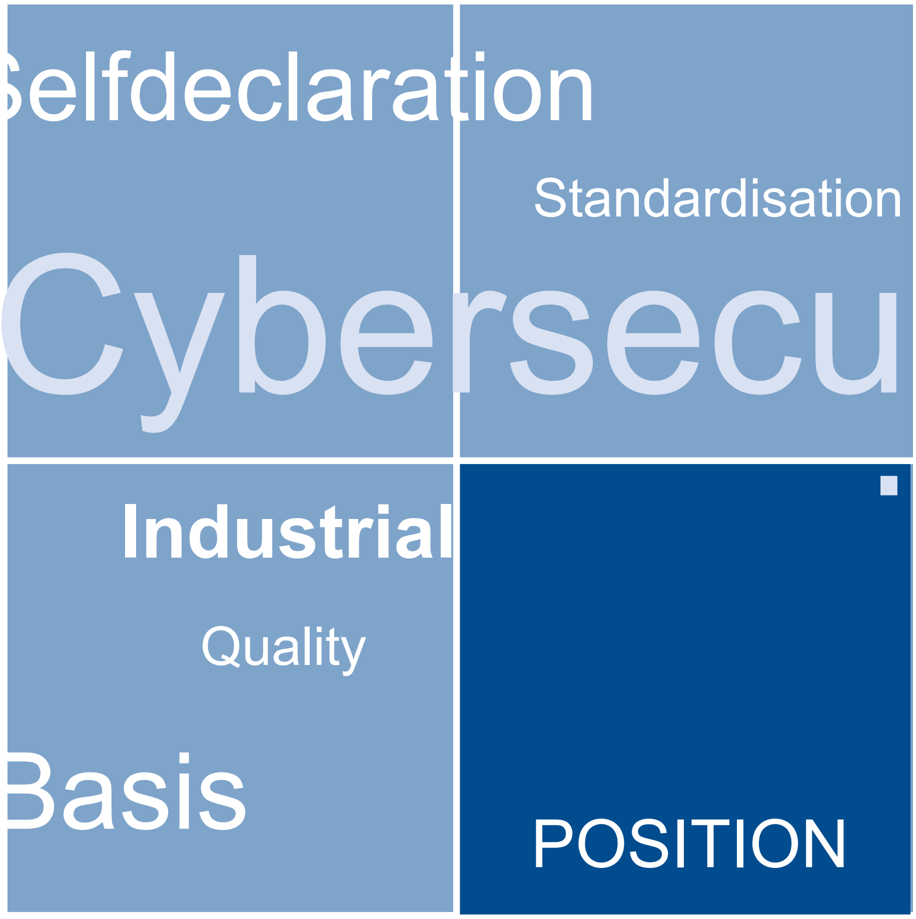
ZVEI:
Die Elektroindustrie

Position Papier

EU Framework for Certification and Labelling

Limits and Possibilities for IoT Security



September 2017
German Electrical and Electronic Manufacturers´ Association

Content

Executive Summary

The electrical industry stands for reliable and robust cyber security in connected devices. This has always been part of the industry's identity. This goal is implemented through industry standardization by creating adaptable standards and increasing transparency. From the point of view of ZVEI's member companies, standardisation is therefore the prime way of achieving the Commission's objectives. Security standards such as IEC 62443 have already been established for the industrial sector. In the field of consumer goods, initiatives have already been triggered, for instance, via the German Institute for Standardisation (DIN): "Security by Design Requirements for IoT-devices in the Small Business/Home environment". Now it is imperative to further advance the security standards in the sectors in accordance with the specific application.

In this view, the voluntary EU “Framework for Certification and Labelling" must be established primarily on the basis of European and international security standards. For those areas where standards are not yet in place, this position paper outlines proposals for basic requirements and a definition for connected devices via the IP-interface. These criteria ensure users and manufacturers can meet the requirements, reduce the complexity of the Internet of Things (IoT) and provide international compatibility. Our common goal is to strengthen the European digital single market. Without common requirements, both digitisation and digital single market cannot be accomplished.

ZVEI member companies take careful note of the fact that a possible need for regulation is to be reviewed by the Commission. Where a legitimate need for regulation exists, the New Legislative Framework (NLF) should be used as framework. The NLF provides the most appropriate way to ensure rapid and adaptable implementation of the Directive via Module A. In this case, the electrical and electronics industry in this position paper formulates proposals for the implementation. ZVEI members are always open for dialogue.

1 Cyber Security is Part of the Industry's Identity

The electrical industry is both the backbone of digitisation. Its products are applied in all relevant social and economic sectors: from consumer electronics, smart home & smart building as well as industrial equipment to (electrical) mobility, energy, and health. ZVEI’s 1600 member companies are knowledge leaders in consumer and industrial goods, for instance for embedded software in devices and components (e. g. smart TV, household appliances, video cameras, medical devices, and industrial controls). Aspects of cyber security and IT regulation therefore directly affect the electrical industry.

Strengthening cyber security is in the interest of the electrical industry. Without protecting personal and technical data, the advantages of digitisation cannot be realised. Our customers should always be able to use their devices and apps in a secure way. Industrial mechanics can remotely access machines anywhere in the world via secure communication channels avoiding the need for travel. Security incidentsdirectly impact customer confidence and brand perception in a negative way. Therefore, it is in line with the ZVEI members' understanding of quality to continuously advance security-by-design. We are convinced of the ever-growing importance of cyber security for consumer protection, product quality, and customer loyalty. This understanding is reflected in standardisation. Numerous security standards are already in place. More than 800 guidelines and standards have been drawn up by industry and other stakeholders already (see section 2.7.).

2 ZVEI’s Positions and Recommendations

ZVEI member companies are contributing the following aspects concerning the design of the voluntary EU framework to the discussion. The main objective is to strengthen cyber security for all stakeholders and the competitiveness European industry.

2.1 Criteria for requirements

There are general principles that should play a decisive role in the selection of requirements to ensure practicality. The requirements should be aligned with the established "SMERC" principle:

- **Specific** – Requirements must be considered on an application-specific basis.
- **Measurability** – Requirement must be clearly identifiable or verifiable.

- **Enforceability** – Requirements must be enforceable through market surveillance.
- **Relevance** – Requirements must be relevant for security and users alike.
- **Competition friendly** – There must not be significant adverse effects on industry competitiveness.

These criteria ensure that the requirements match the capabilities of products. It also ensures that adjustments can be made at any time, which is urgently called for due to the complexity and dynamics of the world of IoT.

2.2 Basic requirements

It is evident that security requirements in individual product groups and sectors have to be examined in a differentiated way. Nevertheless, it is likely that common approaches can be defined. ZVEI member companies contribute the following aspects on the basis of the "SMERC” principle to the discussion:

1. Software maintenance (e.g. via updates) relevant to security is implemented by the manufacturer for clearly defined and communicated periods of time. Known or newly detected vulnerabilities can be resolved in a timely manner. If the user operates the connected device beyond this defined period, he or she is responsible for securing it. In view of the different innovation and product cycles in the consumer and industrial goods sectors (ranging from a few months to several decades), it is not possible to set uniform deadlines. The determination must therefore be carried out in close consultation with all stakeholders based on the experiences in the sectors.
2. If it is not possible to close vulnerabilities, especially for out-dated equipment, the manufacturer will provide alternative methods (e. g. switching off certain functionalities). The customer will be informed about the effects of these alternatives so that he may be able to make a risk-conscious decision.
3. Connected devices provide verifiable basic cyber security measures; tailored to the intended use and operating environment.
   Suggestion:
   - a) Identification and Authentication (user and/or device)
   - b) User and rights management
   - c) Communication Security
   - d) Integrity protection measures (data, systems and processes)
   - e) Updating capability

Of course, all regulatory requirements, such as functional safety and privacy at product and process level, are also enforced by manufacturers. Thus, there is no additional explanation in the list.

2.3 Definition of the application range via IP-interface

What is a connected device? The current definition "any device that can be connected to the Internet" does not really help. ZVEI proposes an initial definition on a functional basis. Connected devices have an IP interface to the outside. They are connected directly or via a point-to-point connection (e. g. via router or mobile phone) to the Internet. Certainly, there are many other communication standards that characterise the IoT-world. However, it will be helpful to start with a core area and, if necessary, to extend the scope of application.

2.4 ”New Legislative Framework“ as central process

Dynamics of development in the field of cyber security are fast-paced. Methods of attack and appropriate protective measures are constantly adapting. No regulation can define a static, fixed set of security requirements under these conditions. Within a few months, it would lose its effectiveness and become a major competitive disadvantage for European companies, especially if specific implementing measures were laid down in the directive.

The NLF ensures that requirements match capabilities of products. This requires a process that complies with antitrust law. Individual actors, be they platforms, agencies or consortia, are unable to accomplish this. The European standardisation organisations also guarantee important principles that are essential for the success and practicality of the Directive:

- uniformity and international compatibility of results
- continuous integration of technical developments
- high acceptance in industries
- coverage of all relevant perspectives (consumers, authorities, companies) and market roles (manufacturers, integrators, installers, operators)

2.5 Module A (manufacturer self-declaration) as conformity assessment

The EU directives provide various procedures to demonstrate conformity with underlying harmonised standards.[1] Via module A (manufacturer self-declaration) companies can react flexibly to modifications of requirements and standards. Thus compared to other modules, costs and time delays are significantly lower, as those bindingly stipulate a third-party certification.

ZVEI member companies categorically reject mandatory third-party certification for the assessment of conformity. It constitutes a disproportionate interference with the private autonomy of companies outside critical infrastructures. In addition, it does not provide any advantage in terms of security quality of products or legal certainty for companies. Manufacturer self-declarations are equally strengthening transparency and commitment. It is a matter of course for companies that all information is complete and correct. This is further ensured by market surveillance. Thus, a certification does not contain any security advantage for users compared to manufacturer's self-declaration.

2.6 Standardisation mandate for CEN/CENELEC

Together with other user industries such as mechanical engineering, the electrical industry has always promoted European standardisation at CEN/CENELEC. They combine mechanical and electrical engineering standardisation with aspects of digitisation and cyber security. The successful outcome is characterised by high acceptance of results by industry users of cyber security and by consensus-oriented opinion-forming according to the "one representative, one vote" principle. This way, the position of medium-sized companies is reinforced. ZVEI therefore strongly advocates granting the NLF standardisation mandate to CEN/CENELEC.

2.7 Consideration of existing security standards

A sectoral, step-by-step approach is urgently necessary. There is no need for regulation if security standards, operator concepts or protection zones exist. There are numerous security standards in place or are currently being reviewed. The Security Navigator of the German Commission for Electrical, Electronic & Information Technologies (DKE) lists 819 existing guidelines and standards for cyber security.[2] In addition, cyber security has also been set internationally:

[1] refer to decision 768/2008/EC

[2] See https://www.security-standards.de/ITSecurityGrid.html

- The international IEC 62443 standard plays a central role in the industrial sector. It defines graduated security requirements for products and processes for all parties involved: manufacturers, integrators and operators. Other sectors are already beginning to transfer its content for their respective areas.
- Work on cyber security has also been underway in the automotive sector for some time. One example of such a project is the ISO/TC22 "Automotive Security" project.
- In Germany, DIN is driving efforts in the consumer goods and industrial sectors through its projects "IoT-Security" and "Secure Identities".

The EU Commission assumes an important responsibility in this context:

1. Existing security content has to be included and taken into account for the respective application range of the EU Framework. No double or even contradictory requirements may be imposed.
2. To perform an analysis on European level to identify where security content is still lacking. Numerous organisations have carried out preparatory work in this area.[3]

This way, potential inefficiencies and duplications can be effectively avoided. ZVEI is pleased to provide input for the analysis.

ZVEI:
Die Elektroindustrie

German Electrical and Electronic
Manufacturers´ Association
Lyoner Strasse 9
60528 Frankfurt am Main, Germany

Contact:
Lukas Linke
Phone: +49 69 6302-432
E-mail: linke@zvei.org
www.zvei.org

September 2017

[3] These include the Cyber Security Coordination Group (CSCG) at CEN/CENELEC and the WG 1 of the European Cyber Security Organisation (ECSO).