Statement

Benefits and limitations of certifications and labels in the context of cyber security

Arguments for a balance between customer information and industrial suitability

January 2017

German Electrical and Electronic Manufacturers' Association

Summary

The electrical criteria industry assesses plans for implementing certification and labelling systems critically, particularly in the industrial B2B context. For one thing, due to consumer protection aspects, most of them can be carried over to the B2B area only with great difficulty, if at all. Furthermore, in many places, industrial initiatives regarding standards and certification for cyber security are already underway. The electrical industry proposes promoting the industry initiatives even more intensively, implementing a clearly separated procedure for B2C and B2B goods and contractual relationships, and always paying attention to the actual informative value of a proposed certification and labelling system. Cyber security will always be dynamic, and some static certification or label statement may even weaken consumer protection instead of strengthening it.

Part 1: Why the debate is important

Private and industry customers are understandably interested in being able to transparently comprehend the degree to which manufacturers have considered cyber security in their products. Customers frequently ask to what extent they can trust products before they integrate them into their home, company or production network. Reliable and transparent customer information is helpful for this purpose.

The electrical industry provides high-quality, robust components and intelligent control systems throughout the entire world. Being a manufacturing industry, it has always been in its own interests to demonstrate the quality and security of its solutions to customers in a transparent way. After all, these are key market arguments. However, the crucial factor is that the information presented is accurate, meaningful, and does not encourage bureaucratic overheads or, in the context of auditing and certification, even weaken the industrial location. There are various ways to provide the product and customer information. This is an established practice in the industry. Level-headed analysis of the topic is therefore required.

Part 2: Standpoints with regard to certification and labels in the context of cyber security

To achieve effective measures, standardised throughout Europe, for strengthening the transparency and development of cyber security in IoT products and systems, the electrical industry believes that the following key points need to be considered:

- **Ensuring future compatibility**: Technical progress also has an impact on protective measures. For example, the requirements regarding the lengths of electronic keys have increased over the years. Hardware and software components need to be able to take account of this development through upgrades. A staggered certification and labelling system must consider future-compatibility when naming any implementation measures.

- **Ensuring technological openness**: Defining specific technical standards can easily result in de facto specification of particular technologies in the area of hardware and possibly even software. In the area of security, in some cases technologies are closely connected to specific products, as niche and special applications are relatively common. When specifying any implementation measures, a staggered certification and labelling system must ensure technological openness, if only for compliance reasons.

- **Taking account of international competitiveness**: International harmonisation of the procedure helps to maintain competiveness. If there are different requirements on foreign markets, this decreases the competitiveness of German products with regard to technology or price.

- **Adaptability of the cyber security conditions**: Cyber security is never static. The level of protection regularly declines over time due to technological progress. In addition, detected vulnerabilities and new attack methods change the security situation in an instant. Certification systems, which can only ever make a statement based on specific time X, thus always risk no longer representing the current protection level of the IoT device. In the worst case, this even weakens consumer protection by implying an incorrect level of protection if customers base their behaviour on this being the case. This can lead to customers no longer trusting the label in the medium term, thus resulting in the affected products with this label being harmed throughout the entire industry.

- **Specify requirements instead of implementation measures**: Ingenuity and innovative strength have always characterised manufacturer companies. They respond to the changing environment of their products on a daily basis. Accordingly, stipulating the technological method for achieving a protection goal would disproportionately restrict entrepreneurial freedom and, over time, result in lower quality solutions. The security and threat situation as well as the possibilities provided by technological progress are too dynamic. Consequently, it is important to allow companies the greatest possible flexibility for achieving the goal. This can be achieved by providing a clear goal – but not by defining the implementation method.

- **A consistently sector-specific approach**: Many industry sectors (e.g. energy, health and mobility) have extremely different framework conditions when it comes to legal bases, application scenarios, customer requirements, technological maturity, and the security and threat situation, as well as in relation to the degree of interconnectedness and digitalization. The supposed common denominator of the IoT definition, “the device can be connected to the Internet”, is not sufficient to sensibly pursue a comprehensive certification and labelling system. Without a product and application-related risk analysis, a statement regarding the security achieved provides no added value for customers. Only a sector-specific approach can address the various framework conditions in a targeted manner.

- **Enable flexibility and competition with manufacturer declarations**: Cyber security will be used across the board in the Internet of Things and will serve as a distinguishing feature. An excessively narrow and static certification and labelling system may actually restrict the range of technical security solutions, particularly if it not only outlines the requirements but also implementation measures. This prevents innovation and market diversity. Using manufacturer declarations, companies can demonstrate in a transparent and comparable manner how they have considered cyber security in their products and solutions and/or which standards they have used as a basis. This enables a more differentiated statement to be made to the customer regarding the security of a product than a generalised label. Bearing in mind that a security statement regarding a product is not future-proof, the latter actually runs the risk of conveying a false conclusion regarding the security of a product to the customer.

- **No certification without standards**: For a certification or label to be meaningful, it must be based on an industry standard that creates a uniform, comparable, practicable and technically proven foundation. In view of the strong export orientation, primarily international standards should form the basis. If there are no dedicated security standards or regulations with references to security for certain sectors or IoT devices, these must be created. International standards can also be provided quickly with the committed collaboration of all interested groups, whereas the transaction costs and uncertainties would be significantly greater for an uncoordinated, technically questionable and possibly national certification procedure.

- **It makes more sense to certify processes than product properties**: The effectiveness of the security characteristics within an IoT device always depends on the environment in which the product is used (implementation, user behaviour, networking with other products and systems, etc.). Development, production and quality management processes at the companies generally remain the same or are usually standardised to create efficiency. At the same time, demanding requirements, development, production and testing measures characterise the robustness and quality of the systems and devices themselves or generate added security value for the development as well as the provision of software updates during the product lifecycle. It is therefore already beneficial for the customer simply to know that the device manufacturer has implemented appropriate industry and product-specific processes – and demonstrates this with comparable certification.

- **The principle of voluntary certification by a third party**: Any certification involves considerable costs for the manufacturer and thus for end customers. The auditing procedure itself also requires documentation effort and is time-consuming. In addition, the relevant business models and interests of the companies must be considered for the debate regarding a certification and labelling system. Furthermore, the documentation workload and time expense of other regulatory specifications (e.g. from functional security), some of which require a significant amount coordination, must be taken into account. Other than for the high security area (governmental, military), the product manufacturer should be free to decide whether to take recourse to third-party certification, depending on the customer and market requirements. Manufacturer declarations are also a recognised and tested means of providing the meaningful information to the customer.

- **No reduction to partial aspects of security**: Cyber security is based on hardware, software and processes across the entire lifecycle of the systems and devices. No partial aspect should take precedence over the others. The best technical precautions in the products are of no use if they are not complemented by appropriate implementation, use and behaviour. A certification system that only verifies the security aspects of the hardware or software, for example, narrows the customer’s view and, at best, can provide only a partial statement – and in the worst case even an incorrect statement – regarding the protection level of the device.

- **Separation of data protection and cyber security in design**: Frequently, the principles of data security and cyber security are confused when it comes to discussions regarding the protection of IoT devices. A security architecture may be desired that covers both areas and expresses the respective protection levels through a standardised certification and labelling system. However, this fails to recognise what are sometimes very different objects of the protection (e.g. personal data vs. technical data). In addition, there are already differently structured legal foundations (e.g. General Data Protection Regulation vs. IT Security Act and NIS Directive). The two required key words “security by design” and “privacy by design” are thus not identical and cannot be represented by a single standard or certification.

- **No orientation to the energy efficiency label**: The state of science and research clearly shows that cyber security cannot be measured using conventional means. The conditions change too quickly and, as a consequence, the requirements may no longer be met in the time between certification and product launches. In the case of cyber security, in/for the product this is equally dependent on the technical properties, processes, user competence, deployment environment and implementation within the overall system. This clearly distinguishes cyber security from energy efficiency, which is illustratively printed on relevant products in the form of a traffic-light label. Because of the existing design and methodical discrepancy, this approach cannot be applied to cyber security. To avoid confusion and potentially incorrect information, concepts for a certification and labelling system must take alternative routes.

Part 3: Possible courses of action for designing a certification and labelling system within the EU

- **Support the transfer of international security industry standards**: In the area of cyber security, the international security standard IEC 62443 is concerned with requirements for technical aspects in products (through the security level) and process-organisational aspects in the company (through the maturity level), and combines these to an holistic approach (through the protection level). In particular, the approach discussed above is taken into account by means of process observation instead of product certification. This procedure has gained acceptance and agreement for numerous industrial applications across different sectors. It may therefore be possible to transfer the approach to other sectors. In addition, work regarding security standards is also beginning in other sectors, and the transferability of this needs to be checked. An example is ISO AWI 21434 “Road Vehicles – Cybersecurity Engineering”. Generally, it is advisable to check ISO 27001 on IT security regarding its applicability in an industrial context. The standard IEC 62443 explicitly gives reference to ISO 27001in its foreword.

  The EU Commission may sound out and support work on transferring and implementing the cross-sector security standards as best practices.

- **Approach using voluntary lightweight certification**: With the ANSSI certification system, France provides a lightweight approach for areas below the high-security levels, which is covered by the Common Criteria Standard.

  The EU Commission should examine the possibilities for a common, voluntary transfer to all EU member states.

- **Defining a standardised scheme for security manufacturer declarations**: Certification and labelling systems are understandably concerned with providing end users with clear, trustworthy and comparable information regarding a product or system. Manufacturer declarations can also take care of this function. There is currently no scheme of this type for the security features of products and systems. However, this could be produced quickly using the tried and tested standards process following a mandate by the EU Commission.

In sum, all considerations regarding cyber security should be aligned to the following principles:

1. Risk-based approach for determining application-oriented security requirements
2. System-related consideration that includes hardware, software and processes
3. Always in relation to the respective lifecycle of devices and systems

It can be expected that current European activities such as AIOTI and ECSO will address these principles. Nonetheless, the problems described above remain. Cyber security is a joint task for politics, industry, manufacturers and users. Against this background, ZVEI urgently encourages that support should be provided for existing activities with the aim of achieving a consensus-based solution.