European Office

Cybersecurity: integrated part of a Single European Market

VDMA discussion paper on shaping a European framework for Industrial Security

Registration number
in the register of representative bodies:
976536291-45

August 2017

Cybersecurity: integrated part of a Single European Market

1. Strategic task for Industrie 4.0 and for Europe

Cybersecurity is an essential issue not only for the Internet of Things, but also for the "Industrial Internet of Things", Industrie 4.0, and thus also for the mechanical engineering industry. The connectivity that accompanies the digitalisation of industry creates new opportunities for increased productivity, better resource efficiency and new business areas; but at the same time, more players, more interfaces and constantly increasing exchange of data mean new risks. Digital representations of business secrets and safety-relevant process data find their way into the net and might be jeopardised as a consequence.

Production and business processes can be successfully digitalised only if the following are ensured:

- Safety for humans and the environment
- Availability of machines, systems and services
- Protection of know-how
- Data integrity
- Transparency of data transmission and data usage
- Confidentiality, and
- Compliance with current legal and contractual obligations

Cybersecurity makes an essential contribution toward meeting these objectives, and thus constitutes a strategic task for businesses, while safeguarding their business interests.

Companies in the mechanical engineering and plant construction industry play a dual role in the digitalisation of industry: as factory operators, they digitalise their own production and business processes; and as technology integrators, they make state-of-the-art interconnected machines and production systems available to their customers.

Cybersecurity also offers challenges for policy-makers, who find themselves obliged to shape an appropriate and effective framework. It is essential, and beyond question, that such a framework must be structured at a European and an international level. What must be avoided is a patchwork of national regulations and schemes, which is the situation that currently threatens to arise in Europe. Neither digitalisation of value chains nor attacks on networks stop at national borders. Rather, a uniform, harmonised framework is the foundation for digital business, and the precondition for the competitiveness of European companies.

2. Cybersecurity depends on context

Cybersecurity is not an end in itself: it serves to protect systems and infrastructure against attacks and thus helps to achieve higher-level objectives such as public safety (protection of people and the environment), privacy, and availability of public and private services. This helps to minimise connectivity-based risks.

In the context of Industrie 4.0, cybersecurity supports digitalisation and networking of industrial firms in serving private-sector objectives such as maintaining functionality, confidentiality of business information, and the integrity and availability of systems and operational functions. Protection cannot be absolute, but must be appropriate to the level of business risk, and allow sufficient free space for innovations and business decisions.

Cybersecurity is not equally important at all times or in all places. The same attack directed at the same components in different environments can trigger different consequences, and will come across users with different levels of preparation. It is therefore important to differentiate, depending on the risks and players, when structuring a framework for cybersecurity. VDMA considers that a distinction can be made between three general classes:

B2C: cyber risks in Internet-of-Things mass markets

Many applications for IoT devices will involve a B2C context in which the device operator is a private end user. The main characteristics of this area are the following:

- The **devices** are consumer goods with a service life of 3-10 years (smartphones, home routers, thermostats, refrigerators) in the low to medium price segment (as opposed to capital goods), and are mostly manufactured in large unit quantities. They often lack a screen for user access (e.g. IP cameras). For their basic function, the devices do not necessarily require a constant network connection (e.g. domestic appliances).
- **Users** have little security know-how, in most cases. Protection of know-how and capital tends to play a minor role, whereas the role of privacy and confidentiality is much greater (e.g. protection of Personal Identifiable information/sensitive personal information). Data protection is governed by law under the General Data Protection Regulation (2016/679) and the future Regulation on Privacy and Electronic Communications ("ePrivacy").
- **Contracts**: individual contractual arrangements play no part. Contracts are concluded on the basis of General Terms and Conditions of Business (GTCB).

B2B: cybersecurity in digitalised value-adding networks

In the "Industrial Internet of Things", the users are mainly companies that connect their production systems and machinery:

- The "things" are **capital-intensive investment goods**, which tend to be manufactured in a wide range of varieties, quite small series or even as single-unit, build-to-order production. They tend to have a longer service life, which may be up to 30 years. Placement on the market and operation are subject to exhaustive regulation. Processes and process changes – and thus also retrofit and updates – are often highly formalised and/or standardised (e.g. in accordance with EN ISO 9001, IEC 62443 and ISO/IEC 27001). Usage can vary widely.
- The **users are companies** or other organisations. Security know-how will vary, but in general be higher than among private end-customers. Protection of operating capital, know-how and conformity with legal requirements play a major role.
- **Contracts** are sometimes negotiated on an order-by-order basis. That means security requirements can also be individually formulated, in principle. Otherwise, contracts may also be concluded on the basis of General Terms and Conditions of Business (GTCB) in the B2B area.

"B2Critis": cybersecurity to protect critical infrastructure

Where networking of plants, machinery and components involves critical infrastructure, security is of particular importance. This is where protection against general economic and societal risks is needed. The operators of this critical infrastructure are subject to the terms of

the NIS Directive. Companies that act as suppliers of hardware or software for identified critical infrastructures must satisfy appropriately stringent security requirements.

These three basic classes require different approaches to deal with the associated risks and circumstances. A one-size-fits-all solution will not work in practice and a silver bullet will never exist.

The answers to the following questions will differ for the three separate classes of B2C, B2B and B2Critis:

- Which tasks will European policy makers assume, and which will be left to the industry?
- How much protection is provided due to self-interest on the part of the private sector (availability, protection of know-how, confidentiality, data integrity)?
- Is there a sufficient number of appropriate security products and services available on the market that SMEs can use to ensure their own cybersecurity strategy and support them in competition with large companies?
- Does networking as part of Industrie 4.0 or the IoT create risks for the general public that go beyond the level of regulated protection already in place for critical infrastructure, e.g. through DDoS (Distributed Denial of Service) attacks via IP cameras or home routers?
- Are there market failures or overriding societal interests that demand political action?
- How will responsibility be shared between the manufacturers of IoT components, machines, and systems on the one hand, and users on the other?

3. Challenges, opportunities and the status quo regarding cybersecurity

Cybersecurity is more complex and further reaching than other product regulation that were based on formulating goals for protection. While it is already a complex matter for manufacturers to consider security aspects through to the commissioning stage, ensuring security during its use represents a further challenge. The existing regulations on marketing products apply only as far as the point when products are placed on the market, or as far as commissioning in isolated cases.

In detail, the following are the aspects that will make cybersecurity a particular challenge:

- Cybersecurity is a moving target, one that depends on the product life cycle: after being placed on the market, networked devices are exposed to a constantly changing risk situation. New threats (e.g. new attacks, new attack patterns, previously undiscovered vulnerabilities, automated attackers) make the security status of a product at the time of delivery irrelevant to a certain extent, and demand constant monitoring and updating. Network-capable devices are also incorporated into different types of products (e.g. machines and production systems). These IoT components and the machine may potentially undergo significant changes while in use. For example, a software installation may add a new functionality. The software or function in question may be supplied by a third party that was previously not involved in the process.
- Responsibility lies with several parties: the manufacturer of the IoT component, the machine manufacturer, the integrator and the user. The boundary between product and service grows hazy in the IoT and Industrie 4.0 environment. Additional players (e.g. service companies) become involved as a consequence.

- Depending on the industrial sector, updates often cannot be applied to machines and systems in a timely manner. In process manufacturing, processes sometimes run continuously for months at a time, since powering down and up again is a cost- and labour-intensive process. Moreover, it cannot be taken for granted that stable Internet connections will be available.
- Demands on security capabilities of products and services will depend on the environment, location, criticality, scheduled useful life, and the value of the business process.
- The extended life cycles and high investment costs of industrial equipment will, in many cases, necessitate retrofitting of connectivity components of systems in use.

In addition to these specifically digital aspects, there are further challenges that do not relate specifically to cybersecurity alone, but must still be taken into consideration:

- Products are developed for a specific purpose (“intended use”), on which risk considerations and product security capabilities are based. This means that devices may be specifically designed either for local networking or for direct Internet access. Requirements on product cybersecurity must take this situation into account and accommodate the obligation for products to be used as intended.
- Cybersecurity cannot be measured in the same way as energy consumption, for example. There are no limit values for performance that are stable over time and will allow for comparison or the establishment of key figures.
- How cybersecurity is implemented plays a large part in determining how effective the level of protection will be. Security is always part of a business process and its implementation must always be sound, at a technical and organisational level. Single or uncoordinated measures cannot guarantee cybersecurity in an industrial setting. There is no silver bullet. An appropriate protection strategy is needed to hedge against each individual risk environment.
- The security level of entire systems is not defined by the sum of its components. Rather, the entire risk to the system must be evaluated. Not only is secure component design important, but also a secure structure to the entire system – the protection strategy – and its operating processes, as determined by the use.

On the other hand, an industrial B2B environment offers good opportunities to identify and address cybersecurity requirements swiftly and at an appropriate level:

- Processes are in place, and experience has been gathered, for working together in value chains. In principle, contractual solutions make it possible to establish the ideal definitions and forms of implementation.
- Established Industrie 4.0 stakeholder networks help companies to expand their know-how and abilities in this area. This is where business associations make a valuable contribution.
- There are established standardisation processes at a European and international level that can be built on.

4. Steps toward an EU cybersecurity framework – initial approaches

To formulate the right answer to these challenges, the important precondition is to determine the requirements before contemplating legislative measures. It would be too hasty and counterproductive to introduce mandatory requirements or even third-party certification across the board in the short term. That would be putting the cart before the horse.

Certification involves testing to ensure that requirements are being met. But until the requirements are clearly established, certificates do not provide the desired transparency and security. Because product certificates are just a snapshot taken before the product is even placed on the market and cannot deal satisfactorily with “moving targets”, certification would not help to achieve a solution at this stage.

It is more important to take the established procedures for shaping regulatory regimes as a guide, and build the path toward an EU framework in line with the following three steps:

Step 1: Identify scope and target group

Right now, it is not clear to whom the European activities with regard to cybersecurity are aimed – operators of critical infrastructure, the European private sector, service providers, IoT providers or the ICT sector - and which products or services are affected. The expressions “IoT” and “IIoT” need to be defined in more detail and further differentiated.

Step 2: Define security requirements and compare against existing standards

The maximum priority must be, firstly, to identify and define the *security requirements* for the previously identified target group(s). Any potential conformity assessment procedure will also rely on defined requirements when it comes to drawing up assessment criteria, be it third-party certification, self-declaration of conformity or contractual assurance. Incoherent requirements, requirements drawn up by the auditors or conformity assessment bodies themselves, or conflicting national requirements, will lead to conflicts of interest, uncertainty, risks and loss of transparency on the market.

The requirements for different areas of application for digitalised products should be defined by neutral entities. This could happen with the support of standardisation bodies, standardisation platforms, or, in some cases, through legislators. There may also be areas in which contractual arrangements under civil law between the parties will suffice. Requirements should be formulated in a technology-neutral way, to avoid creating barriers to product and service innovation and to be able respond to the fast technological development on the attackers side.

The requirements must be reviewed at set intervals to ensure they are still up-to-date and effective. Requirements can be defined only involving users and suppliers. Industry associations can serve as appropriate networks in this regard. This would mean working out requirements in an open, industry-specific consortium and then coordinating them with the affected interest groups in the form of a consensus-based standard. It must take place on widely accessible platforms organised by the industry (e.g. CEN/CENELEC, DIN/DKE or OPC Foundation). It is important in this regard to ensure the transferability to international standardisation committees. Implementing the identified security requirements as part of international standards (ISO/IEC) bolsters European industry in global trading; purely European requirements, on the other hand, lead to fragmentation of the world market to the detriment of European industry.

In VDMA’s view, there is no point in establishing further platforms and non-transparent consortia that set definitions and requirements in respect of digitalisation in the capital goods industry. Unlike platforms that have to be created from scratch, the processes and procedures to be used in the standardisation are known and have been proven.

This is a proven way to analyse the risks and to identify any potential loopholes. It achieves a broad level of support and enables implementation of cybersecurity requirements. As a network of industrial users, VDMA already has experience in formulating cybersecurity requirements. Thus, for example, the VDMA “Industrial Security” working group, with support from Fraunhofer AISEC, formulated concrete recommendations for Industrie 4.0 Security.

Step 3: Select conformity assessment procedures where necessary

If European policy-makers observe market failures and consider regulatory intervention necessary, VDMA considers that any regulatory approach must be defined based on the *“New Legislative Framework”.* Once the requirements, and thus also the required level of protection, have been established, decisions can then be taken regarding the essential legislative requirements and the necessary conformity assessment procedure (including labelling). Decision (EC) 768/2008 describes all the relevant modules for conformity assessment following a risk-based approach. These should be also used in the in the area of security and, where necessary, be further developed.

VDMA and its members firmly believe that this is the only way of rigorously ensuring consistency with the Single European Market.

For the great majority of cases in the B2B area, the conformity assessment based on Module A (self-declaration) under Decision (EC) 768/2008 is sufficient. For critical infrastructures, the use of a different module must be examined, e.g. third-party certification or type approval testing. This process presupposes identifying gaps in standardisation as described above, and the subsequent establishment of the basic requirements in a sector-specific open consortium.

In reaching a decision, it must always be remembered that mandatory third-party testing, and thus labels and certification, always constitute an intervention in the autonomy of enterprises. Precisely for a dynamic, cross-cutting field such as cybersecurity that involves a high level of innovation, policy-makers should exercise great caution. If labelling is deemed necessary, consideration should be given to options provided within the NLF (e.g. CE conformity marking).

First ideas for an approach: improve transparency about capabilities

From VDMA’s perspective, the key to solving the “moving target” problem lies not in trying to create a general assessment plan based on meeting requirements, but in relying on greater transparency with regard to the security-relevant *capabilities* of the products to be connected and their *intended use*.

Suppliers and manufacturers already have to integrate cybersecurity requirements into their products and services. That means products and services have to meet demands that may vary depending on the industry, legal framework, service life and critical nature of the application. A *transparent, comparable and verifiable presentation of capabilities* can make it easier to compare the properties of products and services against requirements.

Requirements and capabilities can be compared in practice only if operators use the devices properly. Here, too, transparency of capabilities and product properties in relation to cybersecurity offers a highly promising approach to ensuring that devices are suitable for their intended purpose.

5. Summary: Nine principles for shaping a European cybersecurity framework

1. The legal framework for cybersecurity must be shaped at a European level and be a part of the Single European Market. A patchwork of national regulations would burden companies with a multiplicity of rules and put Europe behind in the international digitalisation competition.
2. As a “moving target”, cybersecurity requires firstly, that every manufacturer in the value chain take responsibility for his final product – from the component manufacturer to the machinery manufacturer and the system integrator. On the other hand, operators must ensure that the systems are used properly as intended, and that security aspects are observed in their areas of responsibility. The objective of a cybersecurity framework must be to share responsibilities between the manufacturer and operator effectively, sustainably, and in a way that is compatible with practical application.
3. The priority must be to define technology-neutral security requirements. The resulting definition will then form the basis for all further steps. These requirements for different areas of application for digitalised products could be defined by neutral authorities. This could happen with the support of standardisation bodies, standardisation platforms, or, in some cases, through legislators. In many cases, contractual arrangements within GTCB between the parties may suffice. Principles such as “security by design” and “security by default” must apply in this regard.
4. Missing standards to define industry-specific cybersecurity requirements must be elaborated by economic operators on established, open and industry-driven standardisation platforms.
5. There must be no across-the-board, hastily introduced, mandatory requirements or even third-party certification or labelling requirement. Conformity assessment tools cannot be envisaged before a basis has been established in the form of defined requirements. Certification generates unnecessary costs and restricts the solution space for innovations. Complexity and costs would increase exponentially in the very areas where overriding levels of legislation and sector/context-dependent requirements are already in place.
6. If European lawmakers identify a market failure and consider legislative action necessary, VDMA considers the appropriate way forward is a cross-sectorial approach within the *New Legislative Framework*. Only at that point can discussions take place regarding the suitable conformity assessment procedure. VDMA considers that Module A (self-declaration) is appropriate for the bulk of the capital goods industry.
7. In assessing the need for action, lawmakers should take account of the fact that cybersecurity is embedded in the business models and innovation processes of companies. In the context of Industrie 4.0, it is extremely difficult to prescribe a level of technical protection. There are a large number of potential use cases and constantly changing situations. Care must therefore be exercised in determining where regulatory intervention is necessary. In a B2B context, it should be left as far as possible to private players to determine the level of protection they wish to achieve in their business policy and industry-specific aspects. A prescribed level of protection by the lawmakers would be justified only in the face of elevated societal risks for the public at large, e.g. for critical infrastructure or to meet higher-level protection goals.
8. In an initial stage, we recommend improving the transparency and comparability of security-relevant capabilities of IoT products. This would make it easier to compare user requirements against the capabilities of the product as declared by the manufacturer. Transparently documenting product capabilities makes it easy for

users to compare against all security requirements throughout the entire period of use, from generally formulated basic requirements to their business process-specific (or potentially application-specific) rules. This statement of security capabilities, which is stable over time, expressly supports the dynamics in security requirements, during the product life cycle and its service life. A label cannot reflect this dynamic. Examples of these capability descriptions on the part of the manufacturer could be: timeframe of how long security measures are provided after the product is marketed ("End of Support" (EOS)); or the documentation of interfaces, protocol types and open/hidden ports.

9. At a political level, increased awareness and a build-up of capacity should be supported. Established partnerships and alliances play an important role in this regard. The cPPP in the area of cybersecurity is a meaningful way of pooling research activities at an EU level and thus driving forward the EU market for cybersecurity. It must not, however, replace the current, industry-driven platforms and processes, and cannot define requirements on behalf of the user industries.

Contact:

Steffen Zimmermann
VDMA Competence Center Industrial Security
+49 69 6603-1978

Naemi Denz
VDMA Technology, Environment and Sustainability
+49 69 6603 1226

Kai Peters
VDMA European Office
+322 7068219