CEN CENELEC

DECLARATION

for the 2019-2024 EU term

Questions for

Wolfgang Niedziella,

Head of Digital Safety Centre of Competence at VDE and Chair of IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)

1. How would you describe your role and position within VDE and IEC?

I have been working several years for VDE e. V., the German Association for Electrical Electronic & Information Technologies, having held several management positions in the standardization and the certification fields among others. At the international level I have been the Chair of IECEE/CTL (IECEE Committee of Testing Laboratories) from 2010 to 2015 and since 2016 I am the Chair of the IECEE/CMC (IECEE System of Conformity Assessment Schemes for Electrotechnical Equipment and Components) where we developed cyber security services. Hence, with all this background I am now managing the brand new Digital Security Competence Centre in VDE e. V.,which was created over summer of 2019. Particularly in times of information overload, the transfer of criminal activities to the cyber world, the negative effects of attacks on the information systems of companies, authorities, and individuals and thus on their business activities, information and corporate security is more important than ever. VDE reacted to this and decided to develop offers that give its members and customers neutral orientation and security in their specific application.

I have taken on the task of bundling and further developing the VDE's existing competences in the field of standardization, testing and certification, a Computer Security Incident Response Team (CSIRT) and other cyber-related services in our new "Digital Security" competence centre. This, of course, is due to my international positioning, always taking European and international developments into account.

2. What is the role of standards in helping make new technologies more trustworthy for companies and customers?

International and European standards promote innovation through their voluntary nature, avoiding rigid ‘must-comply’ mentality. This is also enhanced by following a technology neutral approach: not specifying solutions but specifying requirements and performance. The performance-based approach supports recognition of developing technologies and the incorporation of experience-based knowledge and outcomes into the standards.

Moreover, European standards facilitate compliance with EU harmonization legislation and hence the entry and free circulation of goods in the EU Single Market. These Standards, based on a set of requirements, are equally applicable in all Member States of the European Union. The European Standardization System offers therefore with its standards a powerful tool to address market needs and evolutions, as it provides a strong framework that sets the best conditions to enable the seamless deployment of innovation in Europe. As cyber crime does not stop at frontiers an international approach is necessary. For this reason, CENELEC is cooperating with IEC based on the so-called Frankfurt-Agreement.

3. One of the most delicate issues with regards to the possibility of cyber-attacks is the protection of critical infrastructures. How is standardization addressing this issue?

When cyber-attacks target critical infrastructure (systems, facilities, technologies, networks, assets and services essential to health, safety, security, etc.), it is a country's ability to function that is endangered. Imagine the consequences it could have on electricity generation, water distribution or the healthcare of entire populations. Cyber security takes into consideration 5 fundamental aspects were Standards are an important tool: Resilience, Security by design, Technologies in Operational environments (OT) and Informational Technologies (IT), Risk assessment, Standards & Guides. Standards for cyber security and data protection that are being developed both internationally and at European level are key to address the risks posed by cyber-attacks and to help ensuring that protection is being implemented. They set out application guidelines for data protection and privacy for security technologies, systems and services for public authorities and private companies and cover all aspects of the evolving information society by offering best practices in the field.

4. You have been involved since 2016 in IECEE, and are therefore involved in conformity assessment of cyber security and standardization both at the international and European level. How can international and European standardization fit the European policy needs regarding cyber security?

The European Cybersecurity Act was adopted earlier this year by the European Union and will now enter in the critical phase of its implementation where standards, conformity assessment and certification are important tools.

Cyber threats are global and most cybersecurity security standards are being developed at the international level by ISO/IEC JTC 1 on Information Technology, and more specifically its sub-committee SC 27 ‘Information security, cybersecurity and privacy protection’ and IEC/TC 65.

The three European Standardization Organizations are now analyzing and complementing the work done at international level in the frame of CEN-CLC/JTC 13 on 'Cybersecurity and data protection'. Through Agreements, CEN and CENELEC are constantly cooperating and checking with their international counterparts ISO and IEC whether European needs can be taken into consideration with standards at international level, aiming that the international standards are reflecting the European needs. As the market of electrotechnical products is international the European Standards (ENs) and international standards should be identical as much as possible. Moreover, international standards open markets acceptance and strengthen the competitiveness of our European companies. All this collaborative work is crucial to support the implementation of the Cybersecurity Act and facilitate trade for our companies globally.

The unique link between European and international standardization helps supporting European legislation: if we want to set the rule, hence the standards, at the global level by fueling European values and needs, CEN, CENELEC and ETSI should be the preferred partners for European policymakers.

5. What is the role of standards in the wider ecosystem of standardization, conformity assessment and certification, with regards to cybersecurity?

Cybersecurity needs a holistic approach to tackle the challenges it faces by combining standards reflecting the state of the art with testing and conformity assessment. Such an approach ensures that all requests of regulators, manufacturers, end-users, and consumers are addressed:

- The Standard offers to all stakeholders the confidence in the product/system/etc. Thanks to the use of security measures based on the state of the art. Standards ensures a common approach that allows that different products are properly working together in a system;

- Conformity Assessment demonstrates that an organization has efficiently and effectively implemented the security measures in his products, systems and services as described by the standard(s). Hence, standards build the foundation leading to a safe ecosystem. Besides, not only they offer best practices but without standards as a basis there would be the risk of experiencing technical barriers to trade.

The IEC being active both in international standardization and conformity assessment offers a risk-based system approach following this holistic view. It is the only organization in the world that provides an international and standardized approach to testing and conformity assessment, and where international standardization and conformity assessment can be tackled in a concerted effort.

For cybersecurity such a service is supplied by the IECEE through its IECEE industrial cybersecurity programme: in accordance with the international standards IEC 62443 series, its members test and certify cybersecurity in the industrial automation sector. As IEC 62443 has a very modular and generic approach, IT can also be used and applied by other sectors.

6. Is the European Standardization System, with its consensus-based and somewhat lengthy process, fit to meet the new challenges of cyber security, or does it risk making standards unable to catch up with rapidly evolving technology?

It is possible to develop basic standards with a generic set of security requirements that will not lose their importance over time. Standardization in the field of cybersecurity has to be considered from the beginning, i. e. starting at the initial design and development phase of a product. During that phase, the basic and generic principles have to be implemented to later guarantee that the product withstands cyberattacks. And all this knowledge can be found in our standards. Having all the stakeholders around the table makes sometimes the standardization process somewhat time-consuming, but it is also essential to make sure that all the needs are taken into consideration.

7. The most essential standards on cyber security (such as the EN ISO/IEC 27000 series or the EN IEC 62443 on OT security) are horizontal. How can we ensure that horizontal standards are applied and adopted in all vertical sectors? What incentives can standards provide to companies to update their systems and mitigate cyber risks?

The two main horizontal standards series in cybersecurity are indeed the ISO/IEC 27000 series, which is a management standard providing a horizontal framework for benchmarking against best practices in the implementation, maintenance and continual improvement of controls; and the IEC 62443 series, which is a product standard establishing cybersecurity guidelines and specifications for a wide range of industries and critical environments in order to keep OT systems running in the physical world.

In the field of cybersecurity horizontal product standards are essential as different products are integrated into one same system. If the different products are designed according to different standards they will hardly work together (interoperability). Horizontal standards are more generic and flexible and can therefore be easily used across the different vertical sectors (nuclear industry, industrial automation, healthcare, railways, the maritime industry, etc.).

DECLARATION

for the 2019-2024 EU term

According to the German Federal Office for Information Security (BSI) Management Report 2019, by the end of May 2018 there were more than 800 million malware programs worldwide, to which 390,000 variants were added every day. Over the past two years, sabotage, data theft and espionage - ultimately due to a lack of cyber security - have caused damage of 43.4 billion euros to German industry alone.

The application of standards and the application of conformity assessment schemes help all stakeholder to reduce their risks and to avoid high damages and hence consequences. It also helps companies as they will be forced to integrate cyber security features in their products and cyber management systems in their organization as more and more countries are issuing corresponding laws and regulations.

#TrustStandards

DECLARATION

for the 2019-2024 EU term

Trust in New Technology

@Standards4EU   www.standardsbuildtrust.eu   policy@cencenelec.eu