Verband der TÜV e.V.

TÜV®

Date
24 July 2017

VdTÜV position: Information security of smart products in Europe

The Internet of Things (IoT) is a generation of new products and services which can communicate with one another. This refers to all products, installations, systems and applications which are software-based and have network access, meaning that they possess "smart" features and are therefore "smart products". This also concerns products of public interest, such as medical devices, lifts or toys. It is a dynamically growing market which is increasingly gaining in importance. The German Federal Ministry for Economic Affairs and Energy estimates that" about 20-50 billion devices will be hooked up to the Internet of Things by 2020".[1]

The European legislator is obligated, in particular, to ensure a high level of consumer protection.[2] The regulatory framework must therefore guarantee that the relevant economic operators are able to have sufficient trust in the safety and security of smart products, so that these innovations experience the necessary acceptance and the potentials for growth are fully utilised.

The question is, however, whether the current regulatory framework for product safety remains up to the task in regard to smart products, or whether there exists the need for legislative adjustments.

Information security is part of the essential safety requirements

On the basis of the New Legislative Framework (New Approach) [3], the European legislator regulates a multitude of product sectors. Accordingly, manufacturers may only place products on the market which fulfil the "essential health and safety requirements". These are specified in greater detail in directives and regulations, e.g. those for lifts, pressure equipment, household and garden appliances, toys and personal protective equipment.

The Toy Safety Directive, for example, makes a distinction between general and particular safety requirements[4] in regard to essential safety requirements:

- General safety requirements according to Article 10 (2)

  "Toys, including the chemicals they contain, shall not jeopardise the safety or health of users or third parties when they are used as intended or in a foreseeable way, bearing in mind the behaviour of children."

[1] Press release from the Federal Ministry for Economic Affairs and Energy on 7 February 2017 "State Secretary Machnig: internet safety requires safe equipment" (https://www.bmwi.de/Redaktion/EN/Pressemitteilungen/2017/20170207-staatssekretaer-machnig-sicheres-internet-gelingt-nur-mit-sicheren-geraeten.html)

[2] *cf.* Art. 169 TFEU (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT)

[3] For further information on the New Legislative Framework (New Approach) see: https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en

[4] *cf.* Art. 10 (1) Directive 2009/48/EC (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:170:0001:0037:en:PDF)

- Particular safety requirements according to Annex II

  "Manufacturers shall carry out an analysis of the chemical, physical, mechanical, electrical, flammability, hygiene and radioactivity hazards that the toy may present."

The manufacturer is thus already obligated under current legislation, for the purpose of fulfilling the general safety requirements, to take appropriate protective measures to ensure the safe use or condition of the product or installation whenever it is used as intended or in a foreseeable way. This means that the information security aspect of security-related components or functions of products and installations (including software, hardware, sensor technology, connectivity) in the development of protective measures by the manufacturer must be thoroughly considered within the scope of the obligatory safety and risk assessment. This is necessary to prevent users or other parties being exposed to danger. On the basis of the legal specifications, information security must therefore be considered an integral part of the functional safety of products and installations.

Information security needs to also be part of the particular safety requirements

In the example named above, the aspect of information security can prove significant for the product features of toys and their potential to cause harm. However, this important aspect is missing in the particular safety requirements set out in Annex II of the Toy Safety Directive. At the same time, the extent to which attention should also be paid to the right to privacy and/or informational self-determination must be considered.

The same applies to the particular safety requirements of other sectoral directives and regulations within the New Approach legislation[5] and to the General Product Safety Directive[6] which applies to those consumer products which are not specifically regulated.

These regulatory gaps may seem surprising at first, but are completely understandable. The rapid technological developments in the IT sector and the accompanying extensive change to original product features was not foreseeable on this scale at the time at which most directives and regulations were drawn up.

The aforementioned regulatory weaknesses in the current annexes to the directives and regulations create ambiguity regarding a smart product's information security aspects which already need to be considered in a specific and uniform manner. Without harmonised specifications, a consistent and uniform risk analysis of smart products and a uniform conformity assessment are barely possible in respect to the smart product's information security. In addition, this creates legal uncertainties and incalculable liability risks for smart products.

Assess the risk potential of smart products using a risk-based approach

The New Approach legislation provides that a product's conformity with the requirements is determined and declared using a risk-based approach with different procedures (the CE mark). De-

[5] See, among others, Directive 2014/35/EU (low voltage), Directive 2014/33/EU (lifts), Directive 2014/68/EU (pressure equipment) and Regulation 2016/425/EU (personal protective equipment).
[6] *cf.* Directive 2001/95/EC (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:011:0004:0017:en:PDF)

pending on the product's risk potential, the conformity assessment modules to be used range from a simple self-declaration on the part of the manufacturer to the mandatory involvement of an independent test organisation (Notified Body).

In the case of a smart product with a fundamentally low risk potential, a new and substantially higher risk potential can arise with regard to information security, an aspect which is becoming increasingly common due to technological progress. It must be ensured that the manufacturer's risk analysis relating to all the relevant information security aspects of the smart product is of an appropriate and reliable quality. In light of the above, the European legislator must examine whether a Notified Body (NB) needs to be involved as a result of the potentially greater risk potential of certain smart products.

The testing of information security requires access to interfaces and software

In order to adequately incorporate the aspect of information security in the framework of the safety testing of products and installations, the independent testing body will in future need full access to the control technology linked to the product's security and safety, to the control technology's software and also to a smart product's digital interfaces and data. Furthermore, the manufacturer must in future inform the NB about changes to IT components (e.g. software updates or extensions) so that such modifications of the smart product and their associated impact upon product safety and security can be assessed.

The European legislator must establish the respective conditions for these access rights and reporting obligations – in particular, clear rights and obligations as well as testing competence.

This is all the more applicable given that, during the periodic assessment of smart products with a high risk potential, the IT aspects are also to be examined in order to take the safety requirements fully into account over the entire product life cycle.

Conclusion: Regulate information security across Europe in accordance with the principles of the New Approach

The regulatory framework must continually keep pace with technological developments and innovations in Europe. In the spirit of a coherent EU legal framework, the regulatory instrument of the New Approach, which has shown itself to be both flexible and conducive to innovation for some 30 years now, should be consistently applied. Precise legal specifications set out in directives and regulations represent the best means for a thorough assessment of every relevant information security aspect before a smart product is placed on the market. The particular safety requirements in regard to information security should be laid down accordingly in these directives and regulations.

Directives and regulations which are currently being revised, or which are revised in the future (e.g. legislation concerning general product safety and lifts), should give full consideration to the aforementioned requirements, in a manner which is open to all technologies, in order to keep pace with the development of smart products.

At sub-statutory level and, in particular, at standardisation level (CEN, CENELEC and ETSI standards), the technical assessment bases for the information security of smart products and for the

corresponding conformity assessment must also be defined and developed. The European Commission must lay the foundations for this by issuing respective standardisation mandates. Only through a close interaction between legislation and standardisation will the convergence required for a uniform information security framework for smart products in Europe be swiftly ensured.

In reviewing the European regulatory framework for smart products, the European Commission is urged:

(a) To also include the aspect of information security in the particular safety requirements for smart products in the respective annexes to the directives and regulations in conformity with the New Approach and to thereby swiftly close regulatory gaps.

(b) To put the risk potential presented by smart products through a fundamental reassessment, while taking information security into account.

(c) To assess and to adapt the applicable conformity assessment procedures in accordance with the newly determined risk potential of the smart product (based on the relevant conformity assessment modules).

(d) Where the risk potential of the smart product is significantly increased by the IT components, to prescribe that an independent body (Notified Body) be mandatorily involved.

(e) Where the smart product is to be assessed by a Notified Body, to grant this body sufficient access to the product's source codes/software.