Verband der TÜV e.V.

TÜV®

Date
24 July 2017

VdTÜV position: Regulatory improvement for safe and secure IoT products in Europe required

Internet of Things (IoT) describes the connecting of clearly identifiable physical objects (things) via internet. Functionalities, scopes and product features are thus significantly changing and the complexity is increasing.

It is therefore necessary to ask whether the current regulatory framework for product safety remains up to the task in regard to IoT products, or whether there exists the need for legislative adjustments, particularly at EU level.

Under Article 169 of the TFEU, the legislator is obligated to ensure a high level of consumer protection. The European regulatory framework must guarantee that the relevant public can sufficiently trust in the security and safety of IoT products so that these innovations gain the necessary acceptance.

The connecting of devices and machines via the internet to complex systems leads to extended functionalities which can no longer be solely located within the individual product itself, but are instead located within the back end system and/or product network. As a result of these extended functionalities and the significantly greater number of digital connections, the potential exists for access by unauthorised parties, along with the accompanying threats and attack scenarios. These new functionalities and product features should be tested across all products.

With this, the issue of the "robustness"[1] of IoT products against cyberattacks takes centre stage among the product safety aspects. It has to be established whether, and to what extent, "robustness" is to be added to the applicable safety requirements placed upon a product. Where it is imperative for an IoT product to be protected against cyber attacks by means of corresponding technical security measures, this would also need to be examined or, as the case may be, tested within the course of the required conformity assessment.

According to the General Product Safety Directive (2001/95/EC), a "safe product" is defined as follows: "any product which, under normal or reasonably foreseeable conditions of use [...] does not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons [...]"[2].

However, this fails to provide a clear answer to the critical matter at hand: Of whether a harmful influence exerted upon the product by other parties is to even be seen as "use" within the sense of the law and thus needs to be a subject of the safety-related examination.

[1] The terms "resilience" and "resistance to sabotage" are also used synonymously.
[2] *cf.* Ch. I, Art. 2 (b) Directive 2001/95/EC (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001L0095&qid=1501167859053&from=EN)

The term “reasonably foreseeable conditions of use” [of the product] is clearly tied to the previously typical possibility of an influence being physically exerted on the product, but does not relate to virtual possibilities of influence and the potential resulting dangers. A regulatory gap therefore exists.

The sector-specific directives and regulations under the New Approach are also lacking clear, consistent and adequate safety requirements for IoT products in terms of the necessary protection against cyberattacks.

It is also unclear whether, in light of their connectivity, certain products which previously have not been required in principle to undergo an independent conformity assessment because of the minimal risks they present also need to be reassessed now in regard to their risk potential and accordingly required functional safety measures/devices. In the course of a necessary reassessment of safety and security risks, such products could also now require testing by an independent third-party in light of their internet connectivity and the associated risks of misuse.

The conformity assessment of IoT products should always cover the aspects of safety and security because the product safety and the information security of an IoT product are inseparably linked to each other. In the future, the necessary “robustness” of products should be viewed as a prerequisite for a “safe and secure IoT product” and be legally defined. For this purpose, the respective conditions and/or specifications must be established at EU level, namely by extending the product safety term and the fundamental requirements accordingly in the sector-specific directives and regulations. A horizontal EU legislative act, one strictly following the principles of the New Approach, is most likely the appropriate regulatory instrument to meet the required demands.

VdTÜV e.V. (the Association of Technical Inspection Agencies – TÜV) proposes to the EU Commission:

1. A prompt and comprehensive review of the European regulatory framework pursuing the objective of integrating the aspect of the robustness (data protection and information security) and the extended functionality (interoperability etc.) of IoT products into the definition of a safe product and into the fundamental requirements for products.

2. A thorough, risk-based analysis of the extent to which, for IoT products, the conformity assessment and appraisal – particularly by independent and qualified third parties – need to be expanded in their scope and nature, or whether new test procedures are in fact necessary.