**Networked components (IoT) are backbone of the digital future and need appropriate cyber protection**

SC No 19018

**Risk-adequate cyber protection catalogue for components and systems**

The digital transformation and the associated networking of devices and components is already dramatically changing our economy and society today. In the coming decades, this trend will continue to increase dramatically. This networking of devices essentially takes place in the Internet of Things (IoT). There, the skilful combination of sensors and actuators, programming and data evaluation can open up new areas of application. The speed at which these new areas of application emerge is sometimes breathtaking and far too often this speed of further development is at the expense of thoroughness on the technical side

Thoroughness in terms of technical sophistication, stability and security of applications is indispensable not only - but especially - in security-critical environments, such as fire or burglary protection. Much too often in the recent past it can be seen in the media that security researchers have once again succeeded in remotely outwitting a component and, for example, putting it out of operation. If one investigates the causes of these hacks, it often quickly becomes clear that the manufacturers of such products have absolutely neglected the topic of cyber security in the development process. Unfortunately, the lack of security for user access, inadequately protected data transfers or software bugs, which leave the door open for attackers for years due to a lack of patch management, are the order of the day.

VdS Schadenverhütung, as a 100% subsidiary of the Gesamtverband der Deutschen Versicherungswirtschaft (GDV), has therefore been commissioned by insurers to significantly increase the level of cyber security in IoT products with a focus on fire protection and security technology. With its profound knowledge in this economic sector and its many years of experience in the testing and certification of installers and products in the security sector, VdS is currently developing guidelines that will demonstrably increase the cyber security of the products and are tailor-made for use in security technology.

Essential requirements are:

**1. General cyber security aspects**

* Requirements for the management of interfaces to networks and components
* Consistent application of the "Security by Design" principle
* Creation of a safe ground state
* Safe handling of faults and malfunctions

**2. Secure user and access management**

* User authentication secured in a risk-adequate manner (also multi-factor authentication)
* Input integrity checking
* rights management for human and machine access
* Consideration of the minimum principle

**3. Securing confidentiality and integrity**

* Encrypted transmission and storage of data
* Integrity check for incoming data and commands

**4. Event capture and logging**

* Capture of safety-critical events
* tamper-proof logbook
* immediate notification of critical processes and statuses

**5. Accompanying measures**

* Transparent information as to when the component will be supplied with security updates.
* Ensuring risk-adequate update management
* transparent settings for automated data transmission to manufacturers or third-party users (so-called "call home" functions)
* EU-GDPR-compliant data processing

In order to ensure acceptance of the requirements, the requirements must not overshoot the mark, but must be levelled in a manner commensurate with the risk. The proven VdS class concept is used for this purpose. Class A marks the baseline for all products, Class C the highest level. Within the framework of an individual risk analysis, individual safety measures can be reassessed and adapted to the specific area of application or replaced by other measures. This ensures the greatest possible flexibility.

The guidelines VdS 3836 "Cyber security for software-controlled systems and components of fire protection and security technology" are developed jointly with the associations and take into account relevant modules of Edition 2019 of the current basic protection compendium of the Federal Office for Information Security (BSI) as well as internationally recognised standards. This ensures the greatest possible acceptance. The guidelines are subject to a public consultation procedure before final publication. Publication is planned for 2019.