Revolution in household appliances.

How to successfully launch smart home products on the market

The market for household appliances, AV/IT products, lights and similar devices has changed dramatically in recent years. Conventional vacuum cleaners turned into robot vacuums; lamps, washing machines and refrigerators became smart appliances that can be controlled via an app from anywhere. To be successful in the market, smart home products must be both easy to connect and easy to use. Users want the operation of these products to be intuitive. In addition, devices should not only be able to communicate with each other in a specific smart home system, but also in a variety of eco-systems. Data protection and data security are another focus of product development and of product use.

www.tuv.com

TÜVRheinland®
Precisely Right.

CHALLENGES FOR MANUFACTURERS OF SMART HOME DEVICES

Manufacturers no longer have to consider only the (electrical) safety of the product during product development and design, but a multitude of other criteria which, due to built-in radio interfaces in the devices, can affect the successful market launch. Manufacturers must have a concept that takes into account interoperability, device safety, data protection and data security. Of course, all this needs to be considered before a device is produced, because if these criteria are not taken into account, failure to meet the requirements can result in significant additional costs or even require a complete redesign of the product.
Assessing the following criteria is essential during the production of networked devices:

1. Interoperability – Communication and compatibility among devices.

a. Can my device communicate with existing systems?
b. How much effort is required of the user, e.g., in terms of ease of operation?

2. Data protection

The home is a private space. All data collected there is also private. This already applies to the selected room temperature, because it allows conclusions about the living habits of the occupants and their presence or absence – and extends to all data from smart household appliances. The legislator specifies strict requirements in this area, and consumers do not want to be spied on by their smart appliances. This can and must be addressed with two design principles: "Privacy by Design" and "Privacy by Default".

3. Cyber security – Identifying vulnerabilities

Major vulnerabilities taken into account during the production of smart home products are:

a. Faulty or defective software
b. Incorrectly configured network access
c. Inadequate password policies
d. Improper disposal and deletion of data on the device
e. Malware and spyware

4. Usability – Ease of use ensures acceptance by users

An important factor for purchase and user acceptance is the intuitive operability as a performance indicator for efficient use. International usability standards such as the ISO 9241 series form the basis for establishing the requirements for interactive products. Compliance with these requirements can be assessed and verified using established assessment methods (e.g., the Usability Guideline of the German Accreditation Body DAkkS).

5. Different approval regulations for different countries

One of the most common issues manufacturers are facing when they try to get their products to market is compliance with approval requirements. These requirements are based on the technology, the product type, the product application, and the target country. In addition, many countries have very different approval regulations for the introduction of electrical and electronic products. This makes it often difficult to keep track. If your products do not meet the regulatory requirements, it can lead to costly delays and compliance issues, making it difficult for you to access your target markets.
Learn more about IoT product testing at TÜV Rheinland

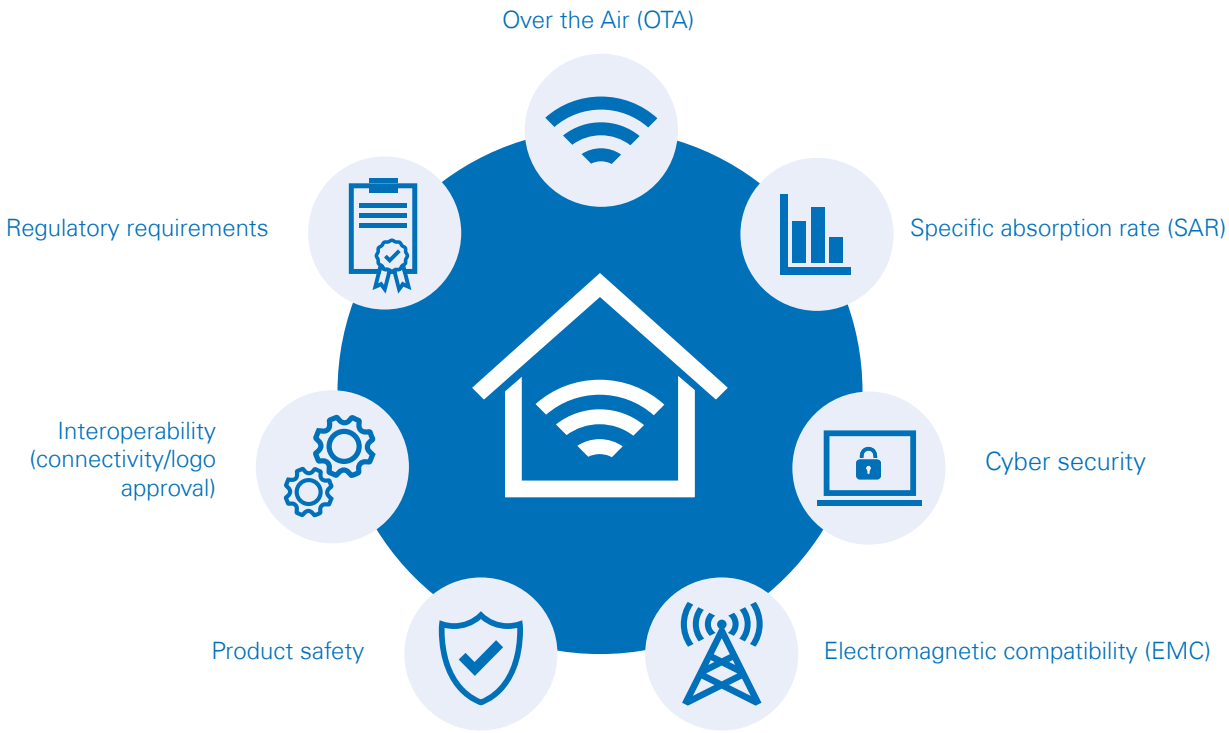
SECURITY AND ASSURANCE WITH COMPREHENSIVE TESTING BY TÜV RHEINLAND

Facing the challenges of our increasingly connected world, how can manufacturers ensure that their products meet the requirements? This can best be achieved with comprehensive testing at all stages of the production process, from design to the final product, and throughout the entire lifecycle of the product.
Here are some relevant sample tests that you can have performed at TÜV Rheinland:

1. Radio transmission (protocols, conformity to standards)
2. Electrical properties (e.g., EMC)
3. Compatibility, interoperability, and interaction with other devices
4. Functionality and functional safety of the individual devices
5. Ergonomics and usability, user acceptance rating
6. Data protection and data security of the device/service (server, app)
7. International market approvals
8. Mechanical properties of a device, mechanical safety, and flammability
9. Chemical properties, if applicable (e.g., vapors)

Smart home systems are subject to constant changes – new components are being added, existing ones are continuously updated. This can lead to unforeseen problems. A modification at one point can lead to errors in the entire smart home system.

OUR SMART HOME TESTING AND CERTIFICATION SERVICES



TÜVRheinland®
Precisely Right.

With TÜV Rheinland, you have a compliance partner at your side who offers comprehensive services from a single source and is well positioned to facilitate access to global markets. TÜV Rheinland has laboratory sites worldwide and 150 years of experience in the field of testing and certification. Our laboratories are also able to perform testing services related to security and data protection. Data protection and the reliability of digital systems and smart products are critical factors for innovation and for building trust in manufacturers and suppliers.

TÜV Rheinland LGA Products GmbH
Am Grauen Stein
51105 Cologne
Phone +49 911 655 5225
Fax +49 911 655 5226
service@de.tuv.com

www.tuv.com

DE22_P03_2200374_Flyer 2-Pager IoT Products_DIN_A4

TÜVRheinland®
Precisely Right.