Add value.
Inspire trust.

White Paper

IVD Instruments under the IVDR: challenges for regulatory compliance and testing approaches

Abstract

In contrast to the IVDD, the IVDR places tremendous higher requirements on the conformity assessments of IVD medical devices. Many devices, formerly handled as self-declared product, now fall into a much higher security class, which greatly increases the share of Notified Body participation.

These increased requirements have to be considered when designing, developing and upgrading IVD medical devices across their life cycle. Thereby, IVD medical device testing is a critical step in the process of transforming an innovative design into a safe and effective product.

Integration of all tests into the product development process and high-quality test evidence are essential for the market access. To meet product safety and conformity, TÜV SÜD can conduct testing against various standards.

In this white paper we will discuss multiple test modules with regard to IVD instruments and the related standards to be considered.

Contents

TÜV SÜD Expert

Dr Alexander Stock
Project Manager IVD Medical Device Testing

Dr Alexander Stock is a quality management professional with 20 years of experience in the biomedical and IVD software industry.
At TÜV SÜD he worked as a lead auditor and product specialist for in vitro diagnostic medical devices under IVDD, IVDR, MDSAP, ISO 13485, ISO 9001.
In his current position he is responsible for the expansion of the IVD medical device testing services at TÜV SÜD.
Dr Alexander Stock is a member of RAPS and a regular speaker on international conferences related to IVDR and IVD software topics.

Increased regulatory requirements

The IVDR imposes increased regulatory requirements compared to the previous directive, including more stringent clinical evidence requirements, stricter classification rules and more rigorous post-market surveillance obligations. This can make compliance challenging for IVD instrument manufacturers, particularly those that are new to the market or are developing innovative technologies.

The IVDR requires more comprehensive technical documentation than the previous directive, including documentation on the device design, manufacturing process and risk management. This requires additional resources and expertise for IVD instrument manufacturers to develop and maintain this documentation.

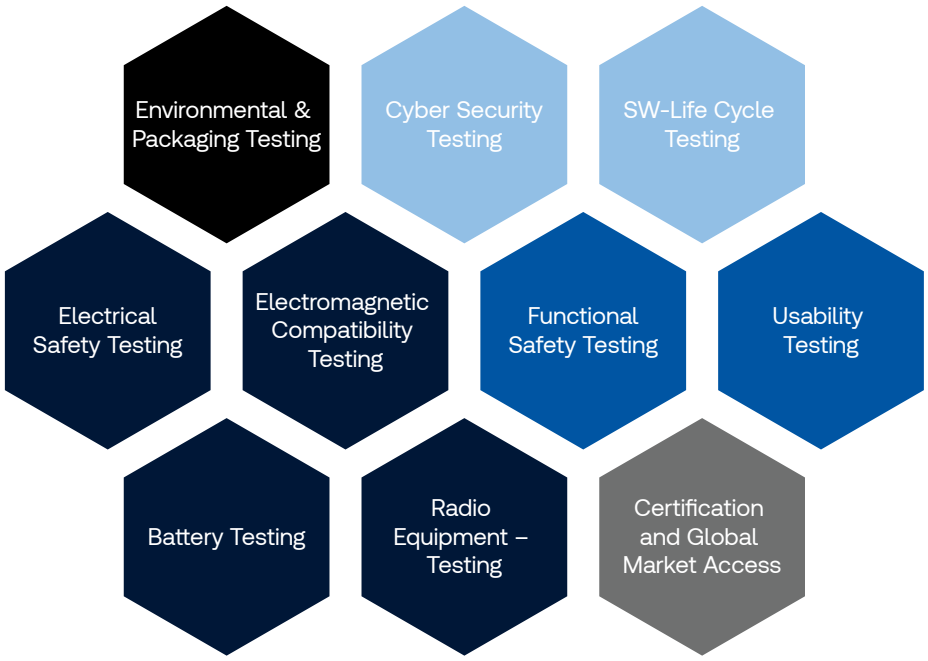
The regulatory landscape for IVD instruments can be complex, with multiple regulatory bodies and different requirements in different jurisdictions. This makes it difficult for manufacturers to navigate the regulatory requirements and ensure compliance.

To overcome these challenges, IVD instrument manufacturers might take a risk-based approach to compliance and focus their resources and efforts on the most critical areas. They might also invest in building regulatory expertise and developing strong relationships with regulators. In addition, they could involve qualified testing laboratories early in the development process for product safety and conformity compliance.

Important testing modules and their normative fundamentals

In the graphic below, relevant test modules for IVD instruments are compiled.
Depending on the device, several or all of them may be applicable.

IVD-Instruments Testing – Test Modules



For the following test modules the related normative references will be discussed:

- Electrical Safety
- Electromagnetic Compatibility
- Radio Equipment
- Functional Safety
- Cyber Security

Electrical Safety

In vitro diagnostic instruments are used in laboratory settings to analyse samples and provide diagnostic results. IVD instruments may pose potential electrical hazards, therefore electrical safety is an important aspect in their design, installation and operation.

For the electrical safety of active medical devices, the IEC 60601 family is applicable. Whereas for electrical safety of IVD instruments, the IEC 61010 family which outlines safety requirements for electrical equipment used in laboratory settings is applicable.
IEC 61010 consists of a main standard IEC 61010-1 and several particular standards IEC 61010-2-XX.

IEC 61010-1
In the context of IEC 61010, electrical safety is often mentioned as the focus topic. However, the requirements of the IEC 61010 family are based on different types of hazards that may apply for the product under testing. It is not limited to electrical safety and also includes:

- Electric shock and burn (Clause 6)
- Mechanical hazards (Clause 7)
- Effects of mechanical stresses (Clause 8)
- Spread of fire from the equipment (Clause 9)
- Excessive temperatures (Clause 10)
- Effects of fluids and fluid pressure (Clause 11)
- Effects of radiation, including laser sources, and sonic and ultrasonic pressure (Clause 12)
- Liberated gases, explosion and implosion (Clause 13)

Also, various Annexes are included in the standard, some of which are **informative** only. The following are **normative** and thus are required for compliance with this standard where applicable:

- Annex A: Measuring circuits for touch current
- Annex B: Standard test fingers
- Annex C: Measurement of clearances and creepage
- Annex D: Parts between which insulation requirements are specified
- Annex F: Routine tests
- Annex H: Qualification of conformal coatings
- Annex K: Insulation requirements not covered by 6.7

IEC 61010-2-XX
Particular standards IEC 61010-2-XX are intended to be used **in conjunction** with IEC 61010-1. They supplement or modify the corresponding clauses in IEC 61010-1 so as to convert that main standard to a **product-specific** safety standard. There are three different options regarding the -2-XX particular standards. Either there is an addition to the clause in the main standard -1 or the clause in the main standard fully applies, or there is a replacement given through the -2-XX particular standard (as illustrated in table 1).

Table 1:

Examples 61010-1 and 61010-2-101 supplement

IEC 61010-1	IEC 61010-2-101
1.1.2 Equipment excluded from scope This standard does not apply to equipment within the scope of: a) IEC 60065 (Audio, video and similar electronic apparatus); b) IEC 60204 (Safety of machinery – Electrical equipment of machines); c) IEC 60335 (Household and similar electrical appliances); ...	**1.1.2 Equipment excluded from scope** **Addition:** **Add the following new item:** aa) Equipment within the scope of IEC 61010-2-081 unless it is specifically intended by their manufacturer to be used for in vitro diagnostic examination.
9 Protection against the spread of fire **9.1 General** There shall be no spread of fire outside the equipment in NORMAL CONDITION or in SINGLE FAULT CONDITION. Figure 11 is a flow chart showing methods of conformity verification. ...	**9 Protection against the spread of fire** **This clause of Part 1 is applicable.**
5.2 Warning markings Warning markings specified in this standard shall meet the following requirements:	**5.2 Warning markings** **Replacement:** **Replace the first paragraph by the following:** Warning markings specified in 5.1.5.1, 5.1.5.2 c), 5.1.5.2 d), 5.1.5.101, 6.1.2 b), 7.3.2 b) 3), 7.4, 10.1, 13.2.2 and 13.101 shall meet the following requirements:

In table 2, the main standard and the particular standards with regard to laboratory equipment are listed (in total there are 19 particular standards, also belonging to further product categories), including information about the particular scopes. There are just 2 particular standards related to medical products: IEC 61010-2-40 (focus on medical devices) and IEC 61010-2-101 (focus on IVD medical devices).

Table 2:

Product Category	Standard	Scope
Measurement, control and laboratory equipment	**IEC 61010-1**	**(General) electrical equipment for measurement, control and laboratory use. Used in conjunction with applicable particular (Part 2) standard(s) for the specific product type.**
Laboratory equipment	IEC 61010-2-010	Laboratory equipment for the heating of materials
	IEC 61010-2-011	Refrigerating equipment
	IEC 61010-2-012	Climatic and environmental testing and other temperature conditioning equipment
	IEC 61010-2-020	Laboratory centrifuges
	IEC 61010-2-040 MED-MD	**Sterilizers and washer-disinfectors used to treat medical materials**
	IEC 61010-2-051	Laboratory equipment for mixing and stirring
	IEC 61010-2-061	Laboratory atomic spectrometers with thermal atomization and ionization
	IEC 61010-2-081	**Automatic and semi-automatic laboratory equipment for analysis and other purposes**
	IEC 61010-2-091	Cabinet X-Ray systems
	IEC 61010-2-101 MED-IVD	**In vitro diagnostic (IVD) medical Equipment**

Related to the electrical safety testing, also certifications in support for the global market access have to be considered, e.g., CB and NRTL certification. These certifications are an important component for achieving a global market access for the IVD product.

The CB Scheme (Certification Body Scheme) is an international programme for the mutual acceptance of product safety test reports and certifications. It is administered by the International Electrotechnical Commission (IEC) and helps to facilitate international trade by eliminating the need for manufacturers to have their products tested and certified multiple times for each country they wish to sell in.

NRTL stands for Nationally Recognized Testing Laboratory and it is a designation granted by the Occupational Safety and Health Administration (OSHA) in the United States. An NRTL is an independent third-party testing laboratory that is recognised by OSHA as meeting the requirements for safety testing and certification of products covered within OSHA. For Canada, NRTL certification is also required and the related accreditations are granted by the Standards Council of Canada (SCC).

Electromagnetic Compatibility

Electromagnetic Compatibility (EMC) comprises two main aspects: emission and immunity.

EMC emission refers to the ability of electronic devices and systems to control the electromagnetic energy they generate and to limit the interference they cause. Emissions testing measures the electromagnetic energy emitted by an electronic device or system and verifies that it is below certain limits.

EMC immunity refers to the ability of electronic devices and systems to function properly in the presence of electromagnetic energy from other sources. The immunity test measures the ability of an electronic device or system to function properly in the presence of electro-magnetic energy.

For IVD instruments, the standards IEC 61326-1 and IEC 61326-2-6 have to be considered. Whereas the -2-6 standard contains the specific EMC requirements for in vitro diagnostic medical equipment regarding immunity and emission.

For the US market it is important also to follow the standard IEC 60601-1-2 since the FDA requires the same for IVD EMC testing (IEC 61326: non-recognized standard by FDA).

If there is further a radio module integrated in the IVD instrument, the testing has to be expanded related to Radio Equipment Testing.

Radio Equipment

Testing Europe
For the testing with regards to the market access in Europe, the regulatory basis is represented by the **Radio Equipment Directive (RED) 2014/53/EU.**

For the EMC part from RED, the standard series **ETSI EN 301 489 – XX**, 'Electro Magnetic Compatibility (EMC) standard for radio equipment and services' has to be considered.

Furthermore, the RED references on standards for module integration or full device testing, e.g.,

- **ETSI EN 300 328** (Wi-Fi 2.4 GHz/BT)
- **ETSI EN 301 893** (Wi-Fi 5 GHz)
- **ETSI EN 300 330** (RFID – Radio Frequency Identification)
- **ETSI EN 301 908-1** (Cellular Networks, LTE)
- **ETSI EN 303 417** (Qi charging)
- and many more …

Finally, also EMF (Electro Magnetic Fields) in the context of human exposure have to be considered for the radio equipment testing, meaning following the requirements of the standard:

- **IEC 62311** – Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz to 300 GHz)

Global Market Access
Globally, there are many different region- and country-specific requirements which have to be fulfilled for the successful market access of instruments containing radio modules. For that reason, it is very important to organise a test set to fulfil the requirements for the target countrie in the most effective way possible. In this context, some examples of different national requirements are listed below.

- RED (Radio Equipment Directive) 2014/53/EU (**Europe**)
- FCC (Federal Communications Commission) Part 15 B/Part 15 C (**US**)
- FDA Wireless Co-Existence Standard IEEE ANSI C63.27-2017 American National Standard for Evaluation of Wireless Coexistence (**US**), e.g., influence LTE on Wi-Fi
- Interference-Causing Equipment Standard ICES-003/Radio Standard Specification: RSS-Gen, RSS-210, RSS-247 (**CAN**)
- Japan ARIB (Association of Radio Industries and Businesses) Standards/MIC (Ministry of Internal Affairs and Communication) Ordinances (**Japan**)

Functional Safety

IVDR Requirements
Under the IVD Regulation, requirements for functional safety are explicitly mentioned in conjunction with single fault condition. ANNEX I GENERAL SAFETY AND PERFORMANCE REQUIREMENTS defines four different requirements in this regard:

13. Construction of devices and interaction with their environment
13.3. Devices shall be designed and manufactured in such a way as to minimise the risks of **fire** or **explosion** during normal use and in **single fault condition**. Particular attention shall be paid to devices the intended use of which includes exposure to or use in association with flammable or explosive substances or substances which could cause combustion.

16. Electronic programmable systems — devices that incorporate electronic programmable systems and software that are devices in themselves
16.1. Devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, shall be designed to ensure repeatability, reliability and performance in line with their intended use. In the event of a **single fault condition**, appropriate means shall be adopted to eliminate or reduce as far as possible consequent risks or impairment of **performance**.

17. Devices connected to or equipped with an energy source
17.1. For devices connected to or equipped with an energy source, in the event of a **single fault condition**, appropriate means shall be adopted to eliminate or reduce as far as possible consequent risks.

17.5. Devices shall be designed and manufactured in such a way as to avoid as far as possible the risk of accidental **electric shocks** to the user, or other person both during normal use of the device and in the event of a **single fault condition** in the device, provided the device is installed and maintained as indicated by the manufacturer.

In contrast to the functional safety for medical devices which are directly connected to a patient, for IVD medical devices the focus is on the performance. Meaning, for IVDs, in the event of single fault condition the performance shall not be impaired. The reason is that the accurate test result of an IVD device is essential for an appropriate medication/therapy. The worst case in this respect is a supposedly correct result which could lead to an incorrect therapy and as a consequence to patient harm. This means that either the IVD test result must be accurate or an error (message) shall appear.

Testing
For the testing of functional safety, the following standards are to be considered:

- **IEC 61010-1**: Safety requirements for electrical equipment for measurement, control, and laboratory use
  Part 1: General requirements

- **IEC 61508-1**: Functional safety of electrical/electronic/programmable electronic safety-related systems
  Part 1: General requirements

- **IEC 61508-2**: Functional safety of electrical/electronic/programmable electronic safety-related systems
  Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

- **IEC 61508-3**: Functional safety of electrical/electronic/programmable electronic safety-related systems
  Part 3: Software requirements

- **IEC 61508-7**: Functional safety of electrical/electronic/programmable electronic safety-related systems
  Part 7: Overview of techniques and measures

- **Software**:
  IEC 62304 & **IEC 82304** Software Life Cycle

Whereby basic functional safety requirements are also mentioned in IEC 61010-1, the focus here is the IEC 61508 for the consideration of first failure safety in connection with the performance of the IVD device.

With regard to the reduction of the risks or impairment referring to the performance of software based IVD devices, also the software life cycle standards IEC 62304 and IEC 82304 are considered, since good software development practice and good coding practice are key for avoiding unexpected errors during the runtime of the software.

Cyber Security

Why is it important for IVD medical devices, too?
The main problem arises here because of the increasingly connected medical infrastructure such as medical devices, IVD medical devices, information systems (LIS, HIS), etc. This results in complex systems with a variety of different interfaces which potentially can be attacked by cyber criminals.

With an IVD medical device, manipulated test data could lead to an incorrect diagnosis and, therefore, an incorrect therapy which can lead to patient harm.
Time-critical diagnostic systems used in the intensive care area (e.g., Near Patient Testing Devices) could be attacked and prevent the urgently needed diagnostic result which can also lead to patient harm.
Manipulated test data from diagnostics of life-threatening infectious diseases could lead to false negative results which can even lead to a public health threat.
And, finally, it doesn't matter if a medical device or an IVD medical device is hacked to perform a ransomware attack on a hospital.

Therefore, an in vitro diagnostic medical device requires the same (like a medical device) threat analysis process to ensure comprehensive Cyber Security coverage.
Meaning, Cyber Security is critical when designing, developing and upgrading IVD medical devices across their life cycle.
In this context, high-quality test evidence is an important component for demonstrating compliance and for ensuring product safety and effectiveness.
Cyber Security testing shall be considered on different levels to support the whole product life cycle.

IVDR Requirements
According to ANNEX I GENERAL SAFETY AND PERFORMANCE REQUIREMENTS, the software focused Cyber Security requirements are as follows:

13. Construction of devices and interaction with their environment
13.2. Devices shall be designed and manufactured in such a way as to remove or reduce as far as possible:
(d) the risks associated with the possible negative interaction between **software** and the **IT environment** within which it operates and interacts;

16. Electronic programmable systems — devices that incorporate electronic programmable systems and software that are devices in themselves
16.1. Devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, shall be designed to

ensure **repeatability**, **reliability** and **performance** in line with their intended use. In the event of a single fault condition, appropriate means shall be adopted to eliminate or reduce as far as possible consequent risks or impairment of performance.

16.2. For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including **information security**, verification and validation.

16.4. Manufacturers shall set out minimum requirements concerning **hardware**, **IT networks** characteristics and **IT security** measures, including protection against **unauthorised access**, necessary to run the software as intended.

20. Label and instructions for use

20.4.1. The instructions for use shall contain all of the following particulars:

(ah) for devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, minimum requirements concerning **hardware**, **IT networks** characteristics and **IT security** measures, including protection against **unauthorized access**, necessary to run the software as intended.

In addition to that, there are also cyber security related requirements which go beyond the pure software focused part of Annex I. In the following table, there are in total 14 cyber security IVDR requirements from Annex I compiled (according to MDCG 2019-16).

Table 3:

Main topic	Section number IVDR Annex I
Device performance	1.
Risk reduction	2.
Risk management system	3.
Risk control measures	4.
Minimisation of foreseeable risks, and any undesirable side-effects	8.
Combination / connection of devices / systems	13.1.
Interaction between software and the IT environment	13.2. (d)
Interoperability and compatibility with other devices or products	13.5.
Repeatability, reliability and performance	16.1.
Development and manufacture in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation	16.2.
Minimum IT requirements	16.4.
Residual risks (information supplied by the manufacturer)	20.1. (g)
Warnings or precautions (information on the label)	20.2. (m)
Minimum IT requirements (information in the instructions for use)	20.4.1. (ah)

Testing
The regulatory basis according to Regulation (EU) 2017/746 (IVDR) is supported by the following guidance and position papers:

- **MDCG 2019-16** Guidance on Cybersecurity for medical devices_rev.1
- **Team-NB Position Paper** Cyber Security Ver. 1, 2022-10-05
- **2023_IG-NB** – Questionnaire Cybersecurity for Medical Devices – Audit – Ver. 1, 2023-03-21
- **2023_IG-NB** – Questionnaire Cybersecurity for Medical Devices – Technical Documentation – Ver. 1, 2023-03-21

For the testing itself, the following standards and state-of-the-art industry frameworks have to be considered:

- **ISO 14971** Application of risk management to medical devices
- **IEC 81001-5-1** Security – Activities in the product life cycle (SDL – Security Development Lifecycle)
- **IEC TR 60601-4-5** Guidance and interpretation – Safety-related technical security specifications
- **OSSTMM**
- **OWASP**
- **NIST (SP 800-115)**
- **PTES**
- **ISSAF**

At TÜV SÜD, a 5-step approach has proven to be most effective for integrating cyber security for an IVD medical device across the entire product life cycle:

1. **Cyber Security Training**
   The learning output for the client is to understand the cyber security related requirements regarding risk management, regulatory frameworks and standards. This is an essential prerequisite for being capable to implement appropriate cyber security measures.

2. **Concept Evaluation**
   An assessment of the technical documentation is performed to ensure that cyber security is an integral part of the connected IVD medical device. The goal is to detect and understand potential gaps in the technical documentation.

3. **Fuzzing**
   This is a method to find implementation bugs by using malformed/semi-malformed data injection. The objective is to find out if the system can handle unexpected input.

4. **Vulnerability Scanning**
   This method aims at the identification and detection of known weaknesses in computers, networks or applications/programmes, meaning to detect known vulnerabilities.

5. **Penetration Testing**
   This test method represents a simulated cyber attack to evaluate the security status of the product, and thus detecting potential unknown vulnerabilities.

How TÜV SÜD is working with the IVD medical device industry to address the required testing

TÜV SÜD Medical Device Testing Services is a unit of TÜV SÜD which provides testing services independently from conformity assessments performed by the Notified Body. In support of IVDR requirements, TÜV SÜD Medical Device Testing Services can conduct testing to ensure conformity against various standards.

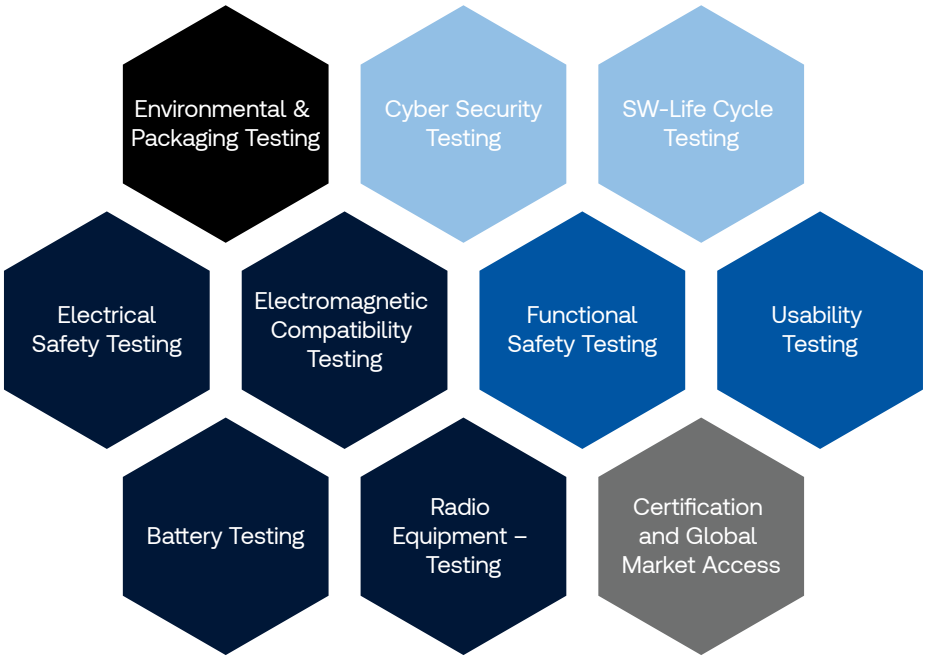
Medical device testing is a critical step in the process of transforming an innovative design into a safe and effective product. Integration of all tests into the product development process is essential for time to market.

For helping to optimise/accelerate the testing phases, our offering covers the full design and production cycle from prototype testing to lab tests and to CB/NRTL certification.

For overcoming the challenge of coordinating all test laboratories for a testing project, there is a dedicated project handler as a single point of contact. The project handler (PH) coordinates all test laboratories involved in one customer project. Furthermore, the PH communicates the progress of all tests, reviews the test reports and provides an executive summary of all tests conducted.

In the following figure the test modules which are offered by TÜV SÜD are compiled.

In Vitro Diagnostic Medical Device Testing – Test Modules provided by TÜV SÜD MHS



We can help customers with the execution of the required tests and deliver high quality test reports for being in conformity with the relevant standards needed to be fulfilled for all these IVD medical device testing modules.

The test modules are individually adaptable to the product-specific and, where applicable, to country-specific requirements, which is essential for the market access.

Furthermore, there are also early bird assessments possible for detecting potential product safety issues already in the early development phase, where issues can be fixed more easily and more cost-effective compared to fixes for a product already in production.

Conclusion

IVD medical device testing is important for several reasons:

- Patient safety: the accuracy and reliability of IVD medical devices play a critical role in patient safety. Incorrect diagnoses or treatment decisions can lead to serious harm or even death. Testing ensures that IVD devices are safe for use by patients and healthcare providers.
- Regulatory compliance: regulatory bodies such as the FDA and the European Union's CE mark require IVD medical devices to be tested and meet certain general safety and performance requirement/standards before they can be marketed and sold. Compliance with these regulations is essential to ensure the safety and effectiveness of IVD devices.
- Quality assurance: testing is an essential part of quality assurance for IVD devices. It helps to identify defects or problems in the device and to ensure that it meets the required standards for accuracy and reliability.
- Research and development: testing is also important for the development of new IVD devices. It helps to identify areas for improvement and to ensure that new devices are accurate, reliable and safe for use.

IVD device testing is an essential part of the product development process and can have an impact on time to market. While it is important to ensure that IVD devices are thoroughly tested and meet regulatory requirements, delays in testing can cause delays in getting the product to market.

To minimise the impact of testing on time to market, it is important to plan for testing early in the product development process. This can help to identify potential issues and to ensure that the necessary testing is completed in a timely manner. It is also important to work closely with testing labs and regulatory bodies to ensure that all requirements are met and that the testing is conducted efficiently.

Overall, while IVD device testing is essential for ensuring patient safety and regulatory compliance, it is important to plan for testing early in the product development process and to work efficiently to minimise the impact on time to market.

Our experts are happy to help – don’t hesitate to contact them!

www.tuvsud.com/ps-pruefung-medizintechnik
myrequest@tuvsud.com

Choose certainty. Add value. TÜV SÜD is a premium quality, safety and sustainability solutions provider that specialises in testing, inspection, auditing, certification and training. Represented in over 800 locations worldwide, we hold accreditations in Europe, the Americas, the Middle East, Asia and Africa. By delivering objective solutions to our customers, we add tangible value to businesses, consumers and the environment.

TÜV SÜD Product Service GmbH
Ridlerstr. 65
80339 Munich, Germany
Tel.: +49 89 5008-4747
www.tuvsud.com/ps