European Cooperation in
Legal Metrology (WELMEC) e.V.
Bundesallee 100
38116 Braunschweig
Germany

WELMEC Guide 7.3

Acceptable Solutions

Version 2026

For information:

This Guide is made available for the Working Group Measuring Instruments (European Commission expert group E01349) for consideration for future referencing on the Europa Website.

WELMEC WG7 welcomes any kind of feedback on the WG7 Software Guides, which may be sent to the WG7 SG "Evolution of Software Guides" (wg7@welmec.org).

If problems are encountered during software examination due to fundamental changes in these Software Guides, WG7 suggests using Guide 7.2:2025 as an alternative for a **transition period of 18 months** after publication of these Guides.

WELMEC e.V. is a cooperation between the legal metrology authorities of the Member States of the European Union and EFTA. This document is one of a number of Guides published by WELMEC e.V. to provide guidance to manufacturers of measuring instruments and to notified bodies responsible for conformity assessment of their products. The Guides are purely advisory and do not themselves impose any restrictions or additional technical requirements beyond those contained in relevant EU Directives. Alternative approaches may be acceptable, but the guidance provided in this document represents the considered view of WELMEC e.V. as to the best practice to be followed.

Published by:
WELMEC Secretariat

E-mail: secretary@welmec.org
Website: www.welmec.org

Acceptable Solutions

Contents

Foreword

The Guide in hand contains acceptable solutions to comply with the core requirements of Guide 7.2, which applies to software-equipped measuring instruments under the scope of the Measuring Instruments Directive (MID) [1] and Non-Automatic Weighing Instrument Directive (NAWID) [2].

1 Terminology

The terminology explained in this chapter describes the vocabulary as used in this Guide. References to a standard or to any other source are given if the definition is completely or in essential parts taken from it.

Source	Term	Definition
Guide 7.2:2025	acceptable solution	A design or a principle of a software module or hardware unit, or of a feature that is considered to comply with a particular requirement. An acceptable solution provides an example of how a particular requirement may be met. It does not prejudice any other solution that also meets the requirement.
	attack vector	Technical steps taken by an attacker to realize a threat.
	attack probability tree (AtPT)	A graphical representation of a threat and its associated attack vectors highlighting how an attack may be subdivided into intermediate sub-goals/attacks. Note 1: The level of detail of an AtPT is chosen by the assessor. Note 2: Leaf nodes of the tree that are not divided further are referred to as elementary attacks.
	assessor	In this Guide, assessor refers to the person(s) chosen by the manufacturer of a measuring instrument to perform the risk assessment.
ISO/IEC 27005:2022	asset	Anything that has value to the organization, and which therefore requires protection. Note 1: Assets are assigned one or more of the following security properties: availability, integrity, authenticity. Note 2: The essential requirements of the MID and NAWID must be examined to determine which assets are of value from a legal metrology perspective, see Guide 7.1. Note 3: Assets can be properties of measuring instruments which shall be protected.
D31:2023	audit trail	Continuous data containing a time stamped information record of events, e.g., changes in the values of the parameters of a measuring instrument or software updates, or other activities that are legally relevant and which are critical for the metrological characteristics.

D31:2023	authentication	Checking of the declared or alleged identity of a user, process, or measuring instrument. Note: This may be necessary when checking that downloaded software originates from the owner of the certificate.
	authenticity	The asset that was retrieved, received, or loaded corresponds to the same asset that was previously stored, transmitted or processed by the authorized entity. Note: The authorized entity is either the LR SW within the measuring instrument, or, when a software update is performed, the manufacturer.
	availability	The asset can be retrieved, received, or loaded within the required time frame when necessary for its metrological purpose.
D31:2023	checking facility	Facility that is incorporated in a measuring instrument and which enables a significant defect to be detected and acted upon. Note: "Acted upon" refers to any adequate response by the measuring instrument (luminous signal, acoustic signal, prevention of the measurement process, etc.).
Adapted from D31:2023	communication Interface	Physical part of an instrument that enables information to be passed between measuring instruments, components of measuring instruments or other external systems. Note 1: Communication interfaces can be wired, optical, radio, etc. communication and they are usually designed to use a specific protocol. Note 2: This definition does not include communication between software modules, see software interface.
Adapted from D31:2023	component	Identifiable hardware part of an instrument that performs a specific function or functions, and that can be separately evaluated in accordance with WELMEC Guide 8.8, and the specific metrological and technical performance requirements as specified in the relevant WELMEC Guide for that component.

	custom solution	A design or a principle of a software module or hardware unit, or of a feature that is considered to comply with a particular requirement. A custom solution can be implemented by the manufacturer if there is no acceptable solution available. The suitability is proven by a risk assessment.
D31:2023	data domain	Location in memory that each program needs for processing data. Note: Data domains may belong to one software module only, or to several.
D31:2023	device-specific parameter	Legally relevant parameter with a value that depends on the individual instrument, component and/or module(s) subject to legal control.
	event	Action that has an impact on a security property of an asset within a measuring instrument. Note: Examples for events are the change of a legally relevant parameter or the update of the legally relevant software.
D31:2023	fault	Difference between the error of indication and the intrinsic error of a measuring instrument. Note 1: Principally, a fault is the result of an undesired change of data contained in or flowing through an electronic measuring instrument. Note 2: From the definition it follows that a “fault” is a numerical value which is expressed either in a unit of measurement or as a relative value, for instance as a percentage.
	generic attack vector	Attack vector defined in Guide 7.2 to address most common attack paths for measuring instruments.
	integrity (of assets)	Property of maintaining the consistency of assets. Note 1: Assurance that assets have not been subjected to any unintentional, accidental or inadmissible changes, e.g., while in use, transfer, storage, repair or maintenance. Note 2: During repair and maintenance, the measuring instrument does not need to comply with essential requirements of MID.

D31:2023	interface	Shared boundary between two functional units, defined by various characteristics pertaining to the functions, physical interconnections, signal exchanges, and other characteristics of the units, as appropriate.
	legally relevant	Required to fulfill the essential requirements and/or having an impact on the compliance with the essential requirements of annex I and the instrument-specific requirements of the MID and/or the essential requirements of annex I and III of the NAWID.
ISO 27005:2022	level of risk	Significance of a risk expressed in terms of the combination of consequences and their likelihood. Note: This Guide uses the terms “risk” and “level of risk” interchangeably.
D31:2023	measuring instrument	Device used for making measurements, alone or in conjunction with one or more supplementary devices.
D31:2023	measurement data	Data used during the measurement process. Note: Measurement data include the measured quantity value, measurement result relevant data and measurement process data, see D31:2023 Annex C.
D31:2023	measurement result	Set of quantity values being attributed to a measurand together with any other available relevant data. Note 1: The measurement result relevant data may consist of e.g. measurement uncertainty, date and time of measurement, number of measurement, identification of sensor and in the case where price calculation is part of the legally relevant software, unit price and price to pay. Note 2: The measurement result (including the measured quantity value according to OIML V 2:200:2012) is used for the legally relevant purpose, e.g. conclusion of a transaction.

	operating system	A collection of software, and firmware elements that control the execution of computer programs and provide services such as computer resource allocation, job control, input/output control, file management and hardware control in a computer system. Note 1: Other programs (such as editors, office programs etc.) not intended for these tasks do not count as part of the operating system. Note 2: An operating system may be legally relevant as a whole, or it is partly legally relevant, or not at all. Note 3: To collect legally relevant parts of the operating system, see Annex III of Guide 7.1, and imagine the "measurement chain". Note 4: In most cases, parts of the operating system like boot loader, kernel, interfaces, resource management, user administration, mathematical and cryptographic libraries, and configuration files are legally relevant.
	physical part	Any legally relevant physical property of a component that can be modified or removed.
	peripheral device	A specific type of a legally non-relevant component that adds functionally to the measuring system. Note: A keyboard or mouse are examples of peripheral devices.
Recast 7.2	prevention	Means that makes it impossible to change an asset.
Recast 7.2	protection	Means that either makes it impossible to change an asset or allows changes to an asset to be detected.
Recast 7.2	relevant documents	Instrument-specific WELMEC Guides, normative documents or harmonized standards.
D31:2023	remote verification	Set of procedures to support verification of an instrument during use, potentially without a person on site.
ISO/IEC 27005:2022	risk	Effect of uncertainty on objectives. Note: This Guide uses the terms "risk" and "level of risk" interchangeably.
ISO/IEC 27005:2022	risk analysis	Process to comprehend the nature of risk and to determine the level of risk. Note 1: Risk analysis provides the basis for risk evaluation and decisions about risk treatment. Note 2: Risk analysis includes risk estimation.

ISO 31073:2022	risk assessment	Overall process of risk identification, risk analysis and risk evaluation.
	risk class	Class that defines the level of risk assessment based on the software protection level, software examination level and software conformity that is applicable to a category of measuring instruments.
	risk estimation	Process to assign values to the probability and consequences of a risk.
ISO 31073:2022	risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk is acceptable or tolerable.
ISO 31073:2022	risk identification	Process of finding, recognizing and describing risks.
Adapted from D31:2023	sealing	Means intended to protect the assets of a measuring instrument. Note: This may be achieved by hardware, software or a combination of both.
	securing	Means of restricting access to assets; makes it impossible to change assets without proper credentials.
Adapted from Guide 7.2: 2023	software download	The process of automatically transferring software to a target measuring instrument or component using any technical means from a local or distant source (e.g., exchangeable storage media, portable computer, remote computer) via arbitrary connections (e.g., direct links, networks).
D31:2023	software examination	Technical operation that consists of determining one or more characteristics of the software according to the specific procedure (e.g., analysis of technical documentation or running the program under controlled conditions).
D31:2023	software identification	Sequence of readable characters (e.g., name, version number, checksum) that represents the software or software module under consideration. Note: Software identification can be checked on an instrument whilst in use.
D31:2023	software interface	Program code and dedicated data domain; receiving, filtering, or transmitting data between software modules. Note 1: A software interface is not necessarily legally relevant. Note 2: A software interface is an interface between two or more software modules, used to exchange data and transmit commands.

D31:2023	software module	Software entity such as a program, subroutine, library, parameter or data set, and other objects including their data domains that may be in relationship with other entities. Note: The software of measuring instruments consists of one or more software modules.
Adapted from MID	sub-assembly	A hardware device (hardware unit) that functions independently and makes up a measuring instrument together with other sub-assemblies (or a measuring instrument) with which it is compatible.
	threat	An unwanted event that may lead to the invalidation of one or more security properties of an asset.
D31:2023	time stamp	Unique value, e.g. in seconds or a date and time string denoting the date and/or time at which a certain incident (e.g. measurement or event) occurred.
D31:2023	type-specific parameter	Legally relevant parameter with a value that depends on the type of instrument, component and/or module subject to legal control. Note: Type-specific parameters are part of the legally relevant software.
D31:2023	user interface	Interface that enables information to be interchanged between the user/operator and the measuring instrument or its (hardware) components or (software) modules. Note: Typical examples of user interfaces are switches, keyboard, mouse, display, monitor, printer, touchscreen, software window on a screen including the software to generate it.

1.1 Abbreviations

This Guide uses the following abbreviations to denote requirements, etc.:

AS	acceptable solution
AWI	automatic weighing instrument
CRC	cyclic redundancy check
ECDSA	Elliptic Curve Digital Signature Algorithm
HMAC	hash-based message authentication code
HTTP	Hypertext Transfer Protocol
IIA1	inadmissible influence via the administration of the operating system
IIA2	inadmissible influence due to accidental modification
IIB1	inadmissible influence via the boot process
IIC1	inadmissible influence by obtaining confidential information
IID1	inadmissible influence by downloading legally relevant software
III1	inadmissible influence via user interfaces
III2	inadmissible influence via hardware interfaces
IIN1	inadmissible influence through legally non-relevant software
IIP1	inadmissible influence on the measurement process by executing other functions
IIR1	inadmissible influence by replacing physical parts within the measuring instrument
IIR2	inadmissible influence by replacing or removing complete components
IIS1	inadmissible influence through incorrect identification of software
IIT1	inadmissible influence through man-in-the-middle attacks
IPC	inter-process communication
NAWI	non-automatic weighing instrument
PIN	personal identification number
SE	secure element
SHA	Secure Hash Algorithm
TCP	Transmission Control Protocol
TEC	type examination certificate
TEE	trusted execution environment
TLS	Transport layer security
TPM	trusted platform module
VPN	Virtual private network
WG	WELMEC Working Group

2 How to use WELMEC Software Guides

Guide 7.1 is the central starting point for readers who are new to software examination. It explains the basic concept of risk-based requirements and provides an overview of the software examination procedure. The Guide also defines structures and procedures to be used by WELMEC members when updating any of the WELMEC Software Guides.

Guide 7.2 implements the core requirements based on the essential requirements of the MID and NAWID detailing that all assets need to be adequately protected. It is the starting point for any software examination.

During such an examination, an examiner first collects all assets that are present in the measuring instrument, then he or she checks that all these assets are protected. Protection means must address all applicable generic attack vectors listed in Annex II of Guide 7.2. For the examination, typically a checklist can be used, see Annex I of Guide 7.2. After that, an examiner has to assess whether the protection means are adequate. To demonstrate this, the manufacturer can either use known acceptable solutions or perform a risk assessment. To document and examine the identified assets and implemented solutions for the attack vectors, see Annex IV of Guide 7.2.

Guide 7.3 provides a collection of acceptable solutions that are suitable for different risk classes of measuring instruments. If a manufacturer implements an acceptable solution in accordance with Guide 7.3, it can be assumed that a corresponding risk assessment has already been performed by WELMEC WG7, see also Guide 7.1, subchapter 5.3.

Acceptable solutions are not mandatory. A manufacturer can implement his own solution. In that case, the appropriateness of the solution has to be shown with a risk assessment.

Guide 7.4 offers an informative overview of examples of how risk-based examination is applied to various measuring instrument designs.

Guide 7.5 contains a gap analysis between EN 45501 and WELMEC Guide 7.2, Version 2019 and has not yet been updated to reflect the recast of the WELMEC Software Guides.

Guide 7.6 describes the risk assessment method that applies to all measuring instruments. It also provides a procedure for additional attack vectors that have to be addressed when a measuring instrument belongs to risk class D or higher.

Acceptable solutions and generic attack vectors only need to be considered for assets that are present in a measuring instrument and that are legally relevant.

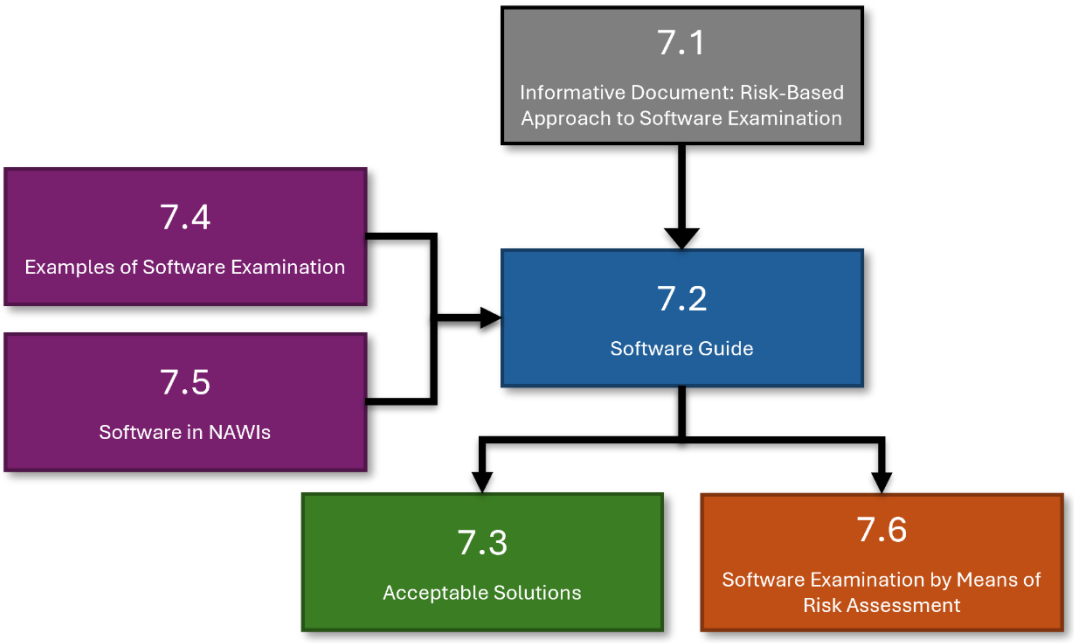

Figure 1: Relationship between the WELMEC Software Guides

The new risk-based approach, which is further described and used in Guides 7.2, 7.3, 7.4 and 7.6, may seem comparable to the traditional requirement-based approach in WELMEC Guide 7.2:2025.

However, there are differences that are discussed in Annex V of Guide 7.1.

Although not specifically mentioned in the text, if a notified body examines the software in accordance with the WELMEC Software Guides, the use of Guide 7.2 is required to ensure that the assets are protected. When the manufacturer applies an acceptable solution, Guide 7.3 is required to examine the correct implementation of the acceptable solution, and Guide 7.6 is required if the manufacturer chooses to use his own solution to assess the adequacy of that solution, taking into account, where applicable, the guidance in Guide 7.4.

The software examination results in a report combining the outcome of the software examinations with regard to the requirements in Guide 7.2, the acceptable solutions in Guide 7.3 and the risk assessment procedure in Guide 7.6. A template for a test report is given in Guide 7.2, Annex V.

The workflow of the software examination described above is visualized in Figure 2.

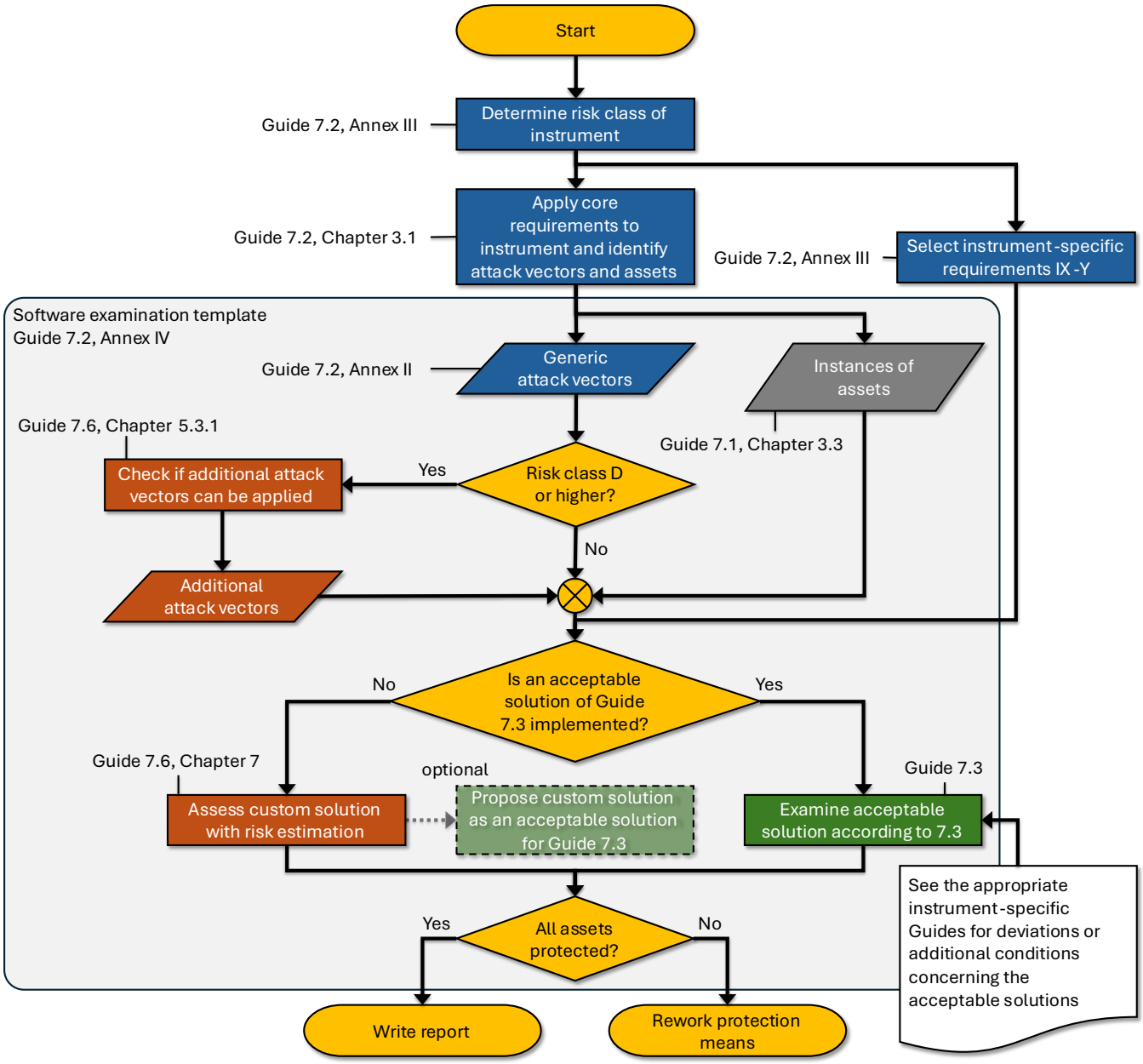

Figure 2: Workflow of the examination of the requirements using Guides 7.1, 7.2, 7.3, 7.6, and instrument-specific Guides (see the WELMEC website).

3 Explanation of Solution Blocks

Each acceptable solution consists of the following:

- A general and (if applicable) specific description.
- Its variants, i.e., slightly different implementations of this AS that fulfill the same purpose.
- Conditions, i.e., technical requirements for the design or functionality of the measuring instrument for this AS to be applicable.
- All keywords that apply to this AS.
    - Assets - The assets that are protected by this solution
    - Security properties - The security properties of the assets that are protected
    - Attack vectors - the attack vectors covered (at least partially) by this solution
    - Status - Indicates whether the solution is active or withdrawn (outdated solutions will not be deleted, instead, they will be marked as withdrawn and remain in the Guide as a reference)
- The required documentation for this AS that must be provided by the manufacturer.
- The functional checks that should be performed to verify the implementation of this AS. In addition to these specific functional checks, the general functional checks listed for each attack vector covered should also be carried out.

In some cases, the specifying notes in Guide 7.2 specify that the manufacturer or examiner has to refer to the instrument-specific documents (relevant documents), about how a specific requirement shall be interpreted or applied.

> *Example:*
>
> In R2.1/N1 it is stated: The information the evidence of an intervention shall contain can be found in the relevant documents.

In this Guide, general responses of the measuring instrument in the event of a detected discrepancy are listed but the manufacturer has to consult the relevant documents to check whether this response is appropriate specifically for his measuring instrument or application. Furthermore, the listed response does not exclude the possibility to use other appropriate responses listed in the relevant documents.

The same applies to how often a check needs to be performed. The manufacturer and examiner have to refer to the relevant documents for information, in this Guide an arbitrary period for such checks is given.

> *Example:*
>
> A checking facility that checks the integrity of the software at start-up might be adequate for a NAWI but not for continuous measurements, such as utility meters.

Relevant documents might also specify that a specific AS shall be used.

Example 1:

Gas meters require registers to be protected by a hardware seal to prevent the registers from being reset.

Example 2:

Electronic signatures may be required by relevant documents if components with limited protection capabilities communicate via open networks.

Manufacturers shall therefore also refer to the relevant documents to determine whether a specific AS can be applied for their measuring instrument or application.

An AS can be active or withdrawn. This is noted in the title together with the year the AS became active or was withdrawn. This also contains a reason why this AS has been withdrawn.

Example:

This AS has been withdrawn in 2023 because a key length of 2 bytes is no longer sufficient for the checksum. Since 2023, a key length of at least 4 bytes is required.

The ASs are divided into different chapters in this Guide.

- Chapter 4 is divided into:
  - 4.1, containing general solutions applicable to multiple inadmissible influences,
  - 4.2, containing solutions to prevent inadmissible influences via the operating system,
  - 4.3, containing solutions to prevent inadmissible influences by the misuse of hardware resources,
  - 4.4, containing solutions to prevent inadmissible influences via interfaces,
  - 4.5, containing solutions to prevent inadmissible influences by man-in-the-middle attacks,
  - 4.6, containing solutions to prevent inadmissible influences by incorrect software identification,
  - 4.7, containing solutions to prevent inadmissible influences by obtaining confidential information, and
  - 4.8, containing solutions to prevent inadmissible influences by modifications of the hardware.
- Chapter 5 contains ASs that address recording evidence of an intervention.
- Chapter 6 contains ASs that are instrument-specific.

4 Acceptable Solutions for Core Requirement R1

4.1 General solutions

4.1.1 Solution: protection against manipulation by using reference values (active)

<table>
<tr><th>Risk Class B</th><th>Risk Class C</th><th>Risk Class D</th></tr>
<tr><td colspan="3">General
A reference value is calculated based on the content of the asset. This reference value is then compared to a previously calculated reference value.
If the values differ, i.e., the content of the asset has changed, the asset is not further processed for legally relevant purposes or there is a clear marking that the asset is no longer legally relevant.
Specific
The reference values and any other input data, e.g., a start value or a secret key, are assets themselves and must be protected as such.
The calculation of the actual value and subsequent comparison with the reference value are legally relevant processes.
The reference values are based on the complete content of the asset.
Certain input data, e.g., start values or secret keys, are considered confidential information.
If the examined asset is the software of the measuring instrument:
• A violation of the security properties results in the measuring instrument either being inoperable or it being clearly indicated that the software is not operating in a legally relevant mode. If a valid and feasible alternative to the corrupted software is available, that version may be used.
• The reference value is indicated to enable independent checking of the software.
For appropriate algorithms, see Variants.</td></tr>
<tr><td colspan="3">Variants
The suitability of the algorithm depends on the “window of opportunity” (see Guide 7.6) of the attacker on the asset and the risk class.
Examples are:
If the window of opportunity is unnecessary or unlimited, the following algorithms are appropriate:
• an HMAC with secret keys, e.g., HMAC-SHA-256
• an ECDSA to create a signature</td></tr>
<tr><td>If the window of opportunity is moderate, difficult, or none, a CRC-32 with a hidden reference value is used (hidden within the measuring instrument or its software).</td><td colspan="2">If the window of opportunity is moderate, difficult, or none, a CRC-32 with a secret start value is used. The start value and reference value are hidden inside the measuring instrument or its software.</td></tr>
</table>

Conditions

-

Keywords

Assets:
software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions

Security properties:
integrity, authenticity, availability

Attack vectors:
IIP1, III1, IIB1, IIA1, IIN1, IIC1, IIR1, III2, IID1, IIR2, IIT1, IIA2, IIS1

Status:
active

Required Documentation

Description of the algorithm and how manipulations are detected.

Identification of the software modules involved in the calculation and comparison of reference values.

Description of the reaction of the measuring instrument in the event of a mismatch.

Description of how confidential material is handled.

Functional Checks

Attempt to modify the assets and check that the modification is detected and an appropriate reaction is taken.

4.2 Inadmissible influence via the operating system

4.2.1 Inadmissible influence via the boot process

4.2.1.1 Solution: bootloader secured with a password (active)

Risk Class B	Risk Class C	Risk Class D

General

The boot configuration is secured by a password, see *4.4.2.1.*

The integrity of the legally relevant parts of the operating system is checked by the bootloader by means of a reference value, see *4.1.1*.

The integrity of the bootloader is physically protected by means of a hardware seal, see *4.4.3.1*.

Variants

-

Conditions

-

Keywords
Assets: software Security properties: integrity, authenticity, availability Attack vectors: IIB1 Status: active
Required Documentation
Description of the boot order and the interactions between boot configuration, bootloader and operating system.
Functional Checks
Check that modification of the boot configuration is not possible without entering a password. Check that booting of a modified boot configuration is not possible.

4.2.1.2 Solution: bootloader secured by trusted environment (active)

Risk Class B	Risk Class C	Risk Class D
General		
A trusted environment either stores the necessary key for verification or directly verifies the electronic signature of the bootloader. The bootloader then verifies the operating system, which in turn verifies and starts the legally relevant software. Examples for trusted environments are a TPM, a TEE and an SE. The signature is created in accordance with *4.1.1*.		
-		The TPM is certified in accordance with Common Criteria Evaluation Assurance Level 4.
Variants		
-		
Conditions		
-		

Keywords Assets: software Security properties: integrity, authenticity, availability Attack vectors: IIB1 Status: active
Required Documentation Description of the boot order and the interactions between the trusted environment, bootloader and operating system.
Functional Checks Modify the bootloader and check that booting is prevented.

4.2.1.3 Solution: secure boot (active)

Risk Class B	Risk Class C	Risk Class D
General Only a signed kernel can be loaded by the bootloader. During the boot process and prior to starting the operating system, the electronic signature of the kernel is verified. If the check fails, the operating system will not start, and an error message is displayed. The signature is created in accordance with *4.1.1*.		
-		The secure boot mechanism is certified in accordance with Common Criteria Evaluation Assurance Level 4.
Variants -		
Conditions -		
Keywords Assets: software Security properties: integrity, authenticity, availability Attack vectors: IIB1 Status: active		

Required Documentation
Description of the boot order and the interactions between bootloader and operating system.
Functional Checks
Modify the bootloader and check that booting is prevented.

4.2.2 Inadmissible influence via the administration of the operating system

4.2.2.1 Solution: access rights configuration (active)

Risk Class B	**Risk Class C**	**Risk Class D**
General Full use is made of the protection and privacy rights provided by the operating system or programming language. All user rights for reading and writing on assets are removed and access is controlled via utility programs. The administrator account is either sufficiently secured, e.g., with a password (see *4.4.2.1*), or permanently deactivated.		
Variants -		
Conditions -		
Keywords Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity, authenticity, availability Attack vector: IIA1 Status: active		
Required Documentation Description of the administration of the user access control and how the administrator account was deactivated.		

Functional Checks	
Check that the administrator account cannot be accessed. Check that user permissions are set in an appropriate manner.	
-	Check that user and group privileges as well as the administrator account are configured correctly. Check that mounted storage media, partitions and media with access attributes are configured correctly. Check that policies for storage media and auxiliary devices correspond to the information contained in the documentation and are configured correctly.

4.2.2.2 Solution: restricted administration (active)

Risk Class B	**Risk Class C**	**Risk Class D**
General Access to administrative tasks is restricted by protecting the administrator account with a password. **Specific** Access to exchangeable media and auxiliary devices has been restricted by means of group policies. Only legally relevant tasks are granted read, write, and execute permissions for files on the system, and only if appropriate.		
Variants Access to administrative tasks is prevented by permanently deactivating the administrator account.		
Conditions -		
Keywords Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity, authenticity, availability Attack vector: IIA1 Status: active		

Required Documentation
Documentation of the configuration of the administrator account.
Functional Checks
Check that administrative tasks cannot be performed without entering the correct password.

4.2.2.3 Solution: kiosk mode (active)

Risk Class B	Risk Class C	Risk Class D
General		
With each start up, the operating system boots into a kiosk mode in which only the legally relevant application is accessible. Keyboard shortcuts have been limited to legally relevant usage.		
Variants		
-		
Conditions		
-		
Keywords		
Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity, authenticity, availability Attack vectors: IIA1 Status: active		
Required Documentation		
The configuration of the operating system.		
Functional Checks		
Check that it is impossible to open legally non-relevant applications.		

4.3 Inadmissible influence by the misuse of hardware resources

4.3.1 Inadmissible influence via processing resources

4.3.1.1 Solution: runtime limitations (active)

Risk Class B	Risk Class C	Risk Class D
General		
The manufacturer limits the runtime for legally non-relevant tasks.		
Specific		
The settings for the limitation of runtime are an asset and must be protected as such.		

Variants

-

Conditions

-

Keywords

Assets:
software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions

Security properties:
integrity

Attack vectors:
IIP1, IIN1

Status:
active

Required Documentation

Description of the runtime limitations for legally non-relevant tasks.

Functional Checks

Export the runtime limitation settings and check that they match with the documentation.

4.3.1.2 Solution: processes are administrated by the operating system (active)

Risk Class B	Risk Class C	Risk Class D

General

The operating system regularly checks that there are enough resources for the execution of the legally relevant software and prevents operation if minimum resources are not available.

Variants

-

Conditions

An operating system is present in the measuring instrument.

Keywords

Assets:
software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions

Security properties:
integrity

Attack vectors:
IIP1, IIN1

Status:
active

Required Documentation

Description of the configuration of the installed operating system parts.	
-	Description of the processes running during use of the measuring instrument.
Functional Checks	
Export the running processes and check that they match the documentation. Check that the manufacturer has documented that there are sufficient system resources for the legally relevant software during use. If possible, check via the system utilization that there are sufficient system resources for the legally relevant software during use.	

4.3.1.3 Solution: removal of unnecessary operating system parts (active)

Risk Class B	Risk Class C	Risk Class D
General		
By means of the package administration of the operating system, the manufacturer removes all operating system packages unrelated to the legally relevant operation. The installation of additional operating system packages unrelated to the legally relevant operation is prevented, see *4.2.2*.		
Variants		
-		
Conditions		
An operating system is present in the measuring instrument.		
Keywords		
Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity Attack vectors: IIP1 Status: active		
Required Documentation		
Description of the configuration of the installed operating system parts.		
-	Information regarding the legally relevant running processes during use of the measuring instrument.	
Functional Checks		
Export the legally relevant running processes and check that they match the documentation. Check that the manufacturer has documented that there are sufficient system resources for the legally relevant software during use. If possible, check via the system utilization that there are sufficient system resources available to the legally relevant software during use.		

Check that no additional operating system packages that are unrelated to the legally relevant operation can be installed.

4.3.1.4 Solution: custom interrupt hierarchy (active)

Risk Class B	Risk Class C	Risk Class D
General The interrupt hierarchy is designed in such a way that adverse influence is prevented.		
Variants -		
Conditions -		
Keywords Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity Attack vectors: IIP1 Status: active		
Required Documentation Description of the configuration of the interrupt hierarchy.		
Functional Checks Export the interrupt hierarchy settings and check that they match with the documentation.		

4.4 Inadmissible influence via interfaces

4.4.1 General

4.4.1.1 Solution: command interpreter (active)

Risk Class B	Risk Class C	Risk Class D
General There is a legally relevant module that receives and interprets commands from the interfaces. It only forwards permitted commands to the other legally relevant modules. **Specific** All inputs through the interfaces are handled by the command interpreter. The examiner decides whether the inputs passed through the command interpreter are permitted. All unknown or not permitted commands are rejected, and known commands do not inadmissibly influence the legally relevant assets.		

No hidden or undocumented functions, commands or data exist.

There are no functions for reading or modifying confidential information.

If there is a legally relevant operating system, the operating system does not inadmissibly influence the configuration of the command interpreter.

The interface does not provide direct memory access.

Variants

-

Conditions

-

Keywords

Assets:
software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions

Security properties:
integrity, authenticity, availability

Attack vectors:
III1, III2, IIN1, IIA2, IIC1

Status:
active

Required Documentation

Any function that can be activated through the command interpreter and any data exchange.

Functional Checks

Check that unknown commands are not forwarded.

Check that commands or data received via the command interpreter cannot inadmissibly influence the assets.

4.4.2 Inadmissible influence via user interfaces

4.4.2.1 Solution: password (active)

Risk Class B	Risk Class C	Risk Class D
General		
An asset cannot be inadmissibly influenced without prior authorization, e.g., a dialog statement or window asking for confirmation and a password. Password entry attempts are limited to three every minute.		
Variants		
The password length is at least four. The password consists of numbers.	The password length is at least six. The password consists of letters and numbers.	The password length is at least eight. The password consists of symbols, numbers, lowercase and uppercase letters.
Conditions		

-
Keywords Assets: measurement data, parameters Security properties: integrity, authenticity, availability Attack vectors: IIA2 Status: active
Required Documentation Format of and restrictions on the password. Information, which software module verifies the password.
Functional Checks Check that creating a password outside the given restrictions is rejected.

4.4.2.2 Solution: smart card (active)

Risk Class B	Risk Class C	Risk Class D
General Access to functionality that might influence the assets is only granted by a smart card. If a person wants to access a parameter, that person needs to insert his or her smart card and enter a personal identification number (PIN) as part of a cryptographic certificate. The software of the measuring instrument is able to verify the authenticity of the PIN by the certificate and allows access to the asset. The format of the PIN complies with an acceptable solution of this Guide, see 4.4.2.1.		
Variants -		
Conditions An operating system is present in the measuring instrument.		
Keywords Assets: measurement data, parameters Security properties: integrity, authenticity, availability Attack vectors: IIA2 Status:		

active
Required Documentation Restrictions on the PIN. Information regarding the software module that verifies the PIN.
Functional Checks Check that creating a PIN outside the given restrictions is rejected. Attempt to access the assets without the smart card or correct PIN, and check that access is denied.

4.4.2.3 Solution: restricted permissions (active)

Risk Class B	Risk Class C	Risk Class D
General The user operates on an account with restricted rights for the user interfaces. The user cannot perform actions that would have inadmissible influence on assets. A configurable operating system is in control of the user interfaces, and the operating system configuration is protected.		
Variants -		
Conditions An operating system is present in the measuring instrument.		
Keywords Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity, authenticity, availability Attack vectors: III1, IIA2 Status: active		
Required Documentation Description of the operating system configuration and how the configuration is protected.		
Functional Checks Check that it is impossible to access and modify the assets via the user interfaces.		

4.4.2.4 Solution: labelled assets (active)

Risk Class B	Risk Class C	Risk Class D

General

The asset is labelled with metadata, e.g., automatic time stamps that indicate whether the asset may be deleted, e.g., if the invoice has been paid.

A utility program may only move/delete data if in accordance with the label.

Specific

The attached label is considered an asset and must be protected as such. Admissible changes to the labels are possible without requiring new evidence of an intervention.

Manual deletion of an asset via the user interface, despite a label indicating that it may not be deleted, is only possible after entering an appropriate password, see *4.4.2.1*.

Variants

The label forces the measuring instrument to stop further measurements if a deletion is not possible and assets would be overwritten.

Conditions

-

Keywords

Assets:
measurement data, parameters

Security properties:
integrity, authenticity, availability

Attack vectors:
III1, IIA2

Status:
active

Required Documentation

Description of the algorithm that creates and attaches the label.
Description of how deletion is prevented.

Functional Checks

Check that all created labels are appropriate (attempt to manually trigger label creation if possible).

Check that it is impossible to inadmissibly change the content of the label.

Check that the label prevents deletion of assets by attempting to delete assets that are not indicated as deletable by the label.

4.4.2.5 Solution: multi-factor authentication (active)

Risk Class B	Risk Class C	Risk Class D

General

The user is prompted to insert another authentication item that is sent to him/her via a separate interface.

The number of additional authentication items (factors) may vary depending on the risk.

Variants	
Two factors are used.	Either two factors, including a biometric factor, or three factors are used.
Conditions	
-	

Keywords
Assets: measurement data, parameters Security properties: integrity, authenticity, availability Attack vectors: IIA2 Status: active
Required Documentation
Description of how the additional authentication item is sent to the user.
Functional Checks
Check that multi-factor authentication is implemented and test it.

4.4.3 Inadmissible influence via hardware interfaces

4.4.3.1 Solution: sealed hardware interfaces (active)

Risk Class B	Risk Class C	Risk Class D
General		
The hardware interface is protected by physical means, e.g., inaccessible inside a case. It is not possible to access the interface without breaking the hardware seal.		
Variants		
-		
Conditions		
-		
Keywords		
Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity, authenticity, availability Attack vectors: III2 Status: active		
Required Documentation		
Description of the hardware seals and their properties. Description of the placement of the hardware seals.		

Functional Checks
Check that it is impossible to access the hardware interfaces without removing a hardware seal. If a seal is present, check that it is impossible to remove the seal without damaging it or without it being clearly visible that the seal was removed. Check that it is impossible to bypass the seal to access the interface.

4.4.3.2 Solution: disabled by the operating system (active)

Risk Class B	Risk Class C	Risk Class D
General The use of the interface is prevented by the operating system. The configuration of the operating system is protected.		
Variants -		
Conditions -		
Keywords Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity, authenticity, availability Attack vectors: III2 Status: active		
Required Documentation The configuration of the operating system.		
Functional Checks Check that it is impossible to connect to the device via the disabled interface.		

4.4.3.3 Solution: disconnected from power supply (active)

Risk Class B	Risk Class C	Risk Class D
General The hardware interface is disconnected from the power supply. The connection between hardware interface and power supply is protected.		
Variants -		
Conditions -		

Keywords
Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity, authenticity, availability Attack vectors: III2 Status: active
Required Documentation
Description of the protection means for the disconnected power supply.
Functional Checks
Check that it is impossible to reconnect the interface to the power supply.

4.4.3.4 Solution: firewall and whitelist (active)

Risk Class B	**Risk Class C**	**Risk Class D**
General		
The use of the interface is prevented by means of a firewall or whitelist for serial protocols.		
Variants		
-		
Conditions		
Any part of the interface not covered by the firewall or the whitelist complies with an acceptable solution from this Guide. The protection means of the configuration of the firewall or the whitelist complies with an acceptable solution from this Guide.		
Keywords		
Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity, authenticity, availability Attack vectors: III2, IIN1 Status: active		
Required Documentation		
The configuration of the firewall. The content of the whitelist.		

Functional Checks	
-	Check that it is impossible to connect to the device via the disabled ports. Perform a port scan on the measuring instrument and check that the result matches with the documented configuration.

4.4.3.5 Solution: protected accessible USB interfaces (active)

Risk Class B	Risk Class C	Risk Class D
General		
The USB interface is used only for legally non-relevant purposes, and the legally relevant software runs under a separate user account of the operating system (see more details in *4.4.4.3*). Interaction with the USB interface is only permitted for the legally non-relevant user account if there is no inadmissible influence on the assets.		
Variants		
Linux The configuration of the USB interface (including /etc/udev/rules.d) is protected. Windows The configuration of the USB interface (including policies, resp. registry keys) is protected. Android The configuration of the USB interface (including uevents daemon or system/core/init/devices.c) is protected.		
Conditions		
The measuring instrument contains legally non-relevant software. An operating system is present in the measuring instrument.		
Keywords		
Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity, authenticity, availability Attack vectors: III2 Status: active		

Required Documentation
The configuration of the operating system.
Functional Checks
Attempt to establish a connection with a device via the operating system interface and check that there is no influence on the legally relevant software.

4.4.4 Inadmissible influence via software interfaces

4.4.4.1 Solution: encapsulated legally non-relevant software (active)

Risk Class B	Risk Class C	Risk Class D
General		
The legally non-relevant software is encapsulated in a library for the calculation of legally non-relevant data. Thus, the legally relevant software has full control over all interactions with the legally non-relevant software.		
Variants		
-		
Conditions		
An operating system is present in the measuring instrument.		
Keywords		
Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity, authenticity, availability Attack vectors: IIN1 Status: active		
Required Documentation		
Each call from the legally relevant software to the library, including the transmitted data.		
Functional Checks		
See the functional checks regarding protection of the operating system in subchapter *4.2*. Perform spot checks by using functions of any known legally non-relevant software and check that there is no inadmissible influence on the assets.		

4.4.4.2 Solution: restricted access for legally non-relevant software (active)

Risk Class B	Risk Class C	Risk Class D
General The asset is not made available to legally non-relevant software.		
Variants The asset is not made available to legally non-relevant modules, components, and/or parts until all legally relevant operations that are based on this asset have concluded.		
Conditions -		
Keywords Assets: measurement data Security properties: integrity, authenticity, availability Attack Vectors: IIN1 Status: active		
Required Documentation Description of the means implemented to prevent access to assets prior to primary indication.		
Functional Checks Check that it is impossible to influence the asset via the software interfaces or, if applicable, check that it is impossible until all legally relevant operations that are based on this asset have concluded. This includes obfuscation of legally relevant assets during indication. Perform spot checks by using functions of any known legally non-relevant software and check that there is no inadmissible influence on the assets.		

4.4.4.3 Solution: software interfaces configured by the operating system (active)

Risk Class B	Risk Class C	Risk Class D
General The operating system is configured in such a way that the legally relevant software cannot be inadmissibly influenced by other software. This includes execution of legally relevant software under a separate account and the correct setting of read/write/execute permissions to ensure that legally non-relevant software cannot influence the assets. The IPC framework (software bus) of the operating system is configured in such way that legally non-relevant processes are prohibited from writing to processes that can influence the assets.		

Variants

-

Conditions

An operating system is present in the measuring instrument.

Keywords

Assets:
software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions

Security properties:
integrity, authenticity, availability

Attack vectors:
IIP1, IIN1

Status:
active

Required Documentation

Description of the configuration of the installed operating system parts.
Description of the software interface configuration.

-	Description of the running processes during use of the measuring instrument.

Functional Checks

Export the running processes and check that they match the documentation.

Perform spot checks by using functions of any known legally non-relevant software and check that there is no inadmissible influence on the assets.

4.5 Inadmissible influence by man-in-the-middle attacks

4.5.1 Solution: physically sealed connection (active)

Risk Class B	Risk Class C	Risk Class D

General

The connection, i.e., the hardware interfaces between the sending and receiving components, is physically protected by means of a hardware seal, see also *4.4.3.1*.

If the connection exists only between two components, the transmitted assets are automatically considered as authentic. Otherwise, authentication needs to be achieved by other means that enable traceability, e.g., by a unique identification or a signature.

Variants

-

Conditions

-

Keywords
Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity, authenticity, availability Attack vectors: IIT1 Status: active
Required Documentation
See *4.4.3.1*.
Functional Checks
See *4.4.3.1*.

4.5.2 Solution: cryptographically paired connection (active)

Risk Class B	**Risk Class C**	**Risk Class D**
General		
All connections, i.e., the hardware interfaces, are configured by the operating system to only accept cryptographically paired connections to certified components. For details regarding the cryptographic algorithms, see *4.1.1*.		
Variants		
-		
Conditions		
An operating system is present in the measuring instrument.		
Keywords		
Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity, authenticity, availability Attack vectors: IIT1 Status: active		
Required Documentation		
See *4.1.1*.		
Functional Checks		
If applicable, check that it is not possible to establish a connection with a different secret key. Check that it is not possible to establish a connection with an unknown device.		

See *4.1.1*.

4.5.3 Solution: TCP and TLS (active)

Risk Class B	Risk Class C	Risk Class D
General The network protocols TCP and TLS are used to protect the transmission. TLS ensures integrity and authenticity by using cryptographic signatures and TCP enables availability. **Specific** The client, i.e., the measuring instrument, only stores a single certificate of the server. Therefore, only direct connections to the server are allowed. The server performs client-side authentication.		
Variants -		
Conditions -		
Keywords Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity, authenticity, availability Attack vectors: IIT1 Status: active		
Required Documentation Identification of the software modules that realize TCP and TLS.		
Functional Checks Attempt to establish a connection without TLS (only HTTP) and check that it is not possible to connect.		

4.5.4 Solution: TCP and TLS for transmission to an indicating module (active)

Risk Class B	Risk Class C	Risk Class D
General An arbitrary device is used to indicate measurement data. The network protocols TCP and TLS are used to protect the transmission of the measurement data. TLS enables integrity and authenticity due to cryptographic signatures and TCP ensures availability of the indicating software module on an arbitrary receiving		

device. **Specific** The maximum round trip time of the underlying TCP is set to a minimum value to continually monitor the availability of the software module on the arbitrary device.
Variants -
Conditions -
Keywords Assets: software, measurement data Security properties: integrity, authenticity, availability Attack vectors: IIA1, IIR2 Status: active
Required Documentation Identification of the software modules that realize TCP and TLS.
Functional Checks Attempt to establish a connection without TLS (only HTTP) and check that it is not possible to connect.

4.5.5 Solution: VPN (active)

Risk Class B	Risk Class C	Risk Class D
General A virtual private network (VPN) is set up to protect the transmission against man-in-the-middle attacks. Only authenticated components are permitted access to the VPN.		
Variants -		
Conditions -		
Keywords Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity, authenticity, availability Attack vectors:		

IIT1 Status: active
Required Documentation
Identification of the software modules that realize the VPN. Description of the configuration of the VPN.
Functional Checks
Check that it is not possible to connect without a VPN.

4.5.6 Solution: identification of sensors (active)

Risk Class B	Risk Class C	Risk Class D
General		
An identification of the sensors that contributed measurement data for the measurement result is included in the transmitted measurement data.		
Variants		
-		
Conditions		
Authenticity is only guaranteed if either intentional modification of the transmitted measurement data is impossible or another solution of this Guide is deployed that guarantees authenticity.		
Keywords		
Assets: measurement data Security properties: authenticity Attack vectors: IIT1 Status: active		
Required Documentation		
Description of how the identification of the sensors is defined and how the assignment between identification and physical sensor is realized.		
Functional Checks		
Check that the transmitted measurement data contain information that link the measurement result to all sensors that contributed to the measurement result.		

4.6 Inadmissible influence by incorrect software identification

4.6.1 Solution: formatted identifiers (active)

Risk Class B	Risk Class C	Risk Class D
General The identifiers are clearly recognizable. The identifiers are easy to present, without requiring additional tools. Each identifier is a unique string that may include the version number or checksum. **Specific** The identifiers are clearly distinguishable from any other legally non-relevant identifiers.		
Variants The identifiers are imprinted on a plate, see *4.6.2*. The identifiers are presented during start-up. The identifiers are presented on command.		
Conditions -		
Keywords Assets: software Security properties: integrity, authenticity, availability Attack vectors: IIS1 Status: active		
Required Documentation Description of how the identifiers are created. Description of how the identifiers are protected. Description of how the identifiers are presented. If other legally non-relevant identifiers are present, description of how the legally relevant identifiers are clearly distinguishable from legally non-relevant identifiers. Description of how each legally relevant module is covered by the identifiers.		
Functional Checks Check that the identifiers are unique and distinguishable. Check that the identifiers are presented as described in the documentation. Check that the presented identifiers match with the identifiers in the documentation.		

4.6.2 Solution: imprint (active)

Risk Class B	Risk Class C	Risk Class D
General The software identification is imprinted on the exterior of the measuring instrument. See *4.6.1* for how identifiers should be formatted.		
Variants -		
Conditions The measuring instrument has no interfaces that enable the transmission or indication of the identification. The software cannot be updated. The imprint is not erasable and any tempering leaves evidence of an intervention.		
Keywords Assets: software Security properties: integrity, authenticity, availability Attack vectors: IIS1 Status: active		
Required Documentation Description of how the prevention of deletion is implemented.		
Functional Checks Check that it is impossible to change or remove the imprint without leaving evidence of an intervention.		

4.7 Inadmissible influence by obtaining confidential information

4.7.1 Solution: storing assets in encrypted form within legally relevant software (active)

<table>
<tr><th>Risk Class B</th><th>Risk Class C</th><th>Risk Class D</th></tr>
<tr><td colspan="3">General
Confidential assets, e.g., secret keys, and associated information such as the reference values, start values, etc., are embedded in the legally relevant software in encrypted form. The legally relevant software does not offer any features to read or change these assets.</td></tr>
<tr><td>The confidential assets are scrambled within the binary code.</td><td>The confidential assets are scrambled within the binary code.
A simple encryption algorithm such as Caesar Code or XOR is used.</td><td>The encryption key is device-specific.
Regarding the algorithms and minimum key lengths, consider the requirements or recommendations of the national and international institutions for data security.</td></tr>
<tr><td colspan="3">Variants
-</td></tr>
<tr><td colspan="3">Conditions
-</td></tr>
<tr><td colspan="3">Keywords
Assets:
software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions
Security properties:
integrity, authenticity, availability
Attack vectors:
IIC1
Status:
active</td></tr>
<tr><td colspan="3">Required Documentation
Description of how and where the secret key is stored.
Description of how the legally relevant software accesses the key.</td></tr>
<tr><td colspan="3">Functional Checks
Check that the keys are encrypted.</td></tr>
</table>

4.8 Inadmissible influence by modifications of the hardware

4.8.1 Inadmissible influence by removing or replacing physical parts

4.8.1.1 Solution: sealed hardware housing (active)

Risk Class B	Risk Class C	Risk Class D
General The hardware housing of the measuring instrument is protected against opening or replacing internal parts by physical means, e.g., a hardware seal.		
Variants -		
Conditions -		
Keywords Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity, authenticity, availability Attack vectors: IIR1 Status: active		
Required Documentation Description of the hardware seals and their properties. Description of the placement of the hardware seals.		
Functional Checks Check that it is impossible to open the housing of the instrument without breaking a hardware seal. If a seal is present, check that it is impossible to remove the seal without damaging it or without it being clearly visible that the seal was removed. Check that it is impossible to replace parts within the instrument without removing a hardware seal. If a seal is present, check that it is impossible to remove the seal without damaging it or without it being clearly visible that the seal was removed.		

5 Acceptable Solutions for Core Requirements R2 and R3

5.1 Solution: audit trail (active)

Risk Class B	Risk Class C	Risk Class D
General The legally relevant software records events, including evidence of an intervention, as continuous data together with a time stamp. Examples are parameter changes or software updates. A checking facility is implemented within a software module that checks regularly if no changes have been made to the audit trail. If a change is detected, a message is displayed and the measurement function is disabled so that it is not possible to further interact with measurement data. If the audit trail has no more capacity, the software prevents further actions. Usually, this means that the measurement function is stopped. The content of the audit trail can be shown on the device display upon command. The audit trail can only be reset if there is subsequent evidence of an intervention. **Specific** The clock function is an asset and must be protected as such. The audit trail fulfills the functional requirements as listed in the applicable relevant documents, particularly regarding the information required to be listed in the audit trail.		
Variants Instead of date and time, the time stamp of the event contains the value of a timer that continuously counts the passage of time in one direction in a repeatable manner. In that case, the type-approval certificate explains how the passage of time can be calculated, e.g., how the value of the timer relates to the number of days that have passed. Instead of indicating the content of the audit trail on the device display, the measuring instrument sends the content to another device for indication. The transmission complies with an acceptable solution of this Guide.		
Conditions -		
Keywords Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions Security properties: integrity, authenticity, availability Attack vectors: IIP1, III1, IIB1, IIA1, IIN1, IIC1, IIR1, III2, IID1, IIR2, IIT1, IIA2, IIS1 Status: active		

Required Documentation
Description of the audit trail mechanism.
Description of the protection of the audit trails.
Description of the timestamps and clock function, or other forms of sequencing the entries.
Description of the structure of audit trail entries.
Functional Checks
Trigger an event and check that it is recorded correctly in the audit trail.
See functional checks for acceptable solutions that realize protection of the audit trail, for example *4.4.2*.

5.2 Solution: event counter (active)

Risk Class B	**Risk Class C**	**Risk Class D**
General		
The legally relevant software records events in a non-resettable event counter that increments each time an event occurs.		
A checking facility is implemented within a software module that checks regularly that no changes have been made to the event counter. If a change is detected, a message is displayed, and the measuring function is disabled so that it is not possible to further interact with measurement data.		
A mechanism exists within the measuring instrument to prevent overflow of the event counter.		
Specific		
The value of the event counter after (subsequent) verification is marked on the measuring instrument.		
Relevant documents may give further details on the content of the event counter, e.g., if significant defects must be recorded as well.		
Relevant documents may specify that an event counter is not adequate, and require an audit trail.		
Variants		
-		
Conditions		
This solution is not used for parameters that may be set by the user (see R3 of Guide 7.2).		
Keywords		
Assets: software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions		
Security properties: integrity, authenticity, availability		

Attack vectors: IIP1, III1, IIB1, IIA1, IIN1, IIC1, IIR1, III2, IID1, IIR2, IIT1, IIA2, IIS1 Status: active
Required Documentation
Description of the event logger mechanism. Description of the overflow protection. List of events that are counted.
Functional Checks
Trigger an event and check that it is recorded correctly by the event counter. Try to create an overflow of the event counter and check that this is prevented.

5.3 Inadmissible influence through software download

5.3.1 Solution: traced update (active)

Risk Class B	Risk Class C	Risk Class D
General		
The traced update allows to change the software in a verified device after which a subsequent verification is not necessary. The new software is checked for integrity and authenticity. If the software is transmitted to the device, see also *4.5* for possible acceptable solutions. After initiation, the update runs automatically, i.e., no human intervention is required. Depending on legislation, the user or owner might be required to initiate the update (see notes in Specific). During the update process, the device is inoperative and cannot perform measurements. Information regarding the update process and the result are recorded in the device for subsequent verification, surveillance, or inspection (see notes in Specific). An audit trail (see *5.1*) is a possible solution to record this information. After the update process, all assets are once again adequately protected regardless of the result of the update process.		
Specific		
If required by legislation, the device offers a feature for the owner or user to give their consent to an update, e.g., a switch or button. If the owner or user denies consent, the update is aborted. If the new software fails the integrity or authenticity check prior to installation, the update is aborted, and the previous version remains active. The update process impedes the measurement function only in an acceptable manner. For information about what is acceptable in this context, see the relevant documents. The number of update attempts is limited within a given time interval. The following information is recorded during and after the update process:		

- timestamp when the update procedure was started;
- result of the update procedure (success/failure);
- identification of the new software;
- identification of the previous software;
- timestamps for all recorded related events;
- if available, identification of the source of the update.

All evidence of an intervention is retained during the update procedure and is still available afterwards.

The update is not performed if information about the update process cannot be recorded or existing evidence of an intervention or information about previous updates would be deleted, for example due to insufficient storage capacity.

Variants

Instead of using the previous version of the software if the update process is aborted, the device is made inoperable. In this mode, it is only possible to restart the update process.

The software on the device is separated into fixed modules that cannot be updated and modules that can be updated. The fixed modules realize the administration of the update process.

For water meters, the duration of the installation of new software is limited to one minute or additional measures are implemented, e.g., the installation takes place at low energy consumption.

Conditions

-

Keywords

Assets:
software

Security properties:
integrity, authenticity, availability

Attack vectors:
IID1

Status:
active

Required Documentation

Description of how the integrity and authenticity of the new software is checked prior to installation.

Description of how the update process is performed automatically.

Description of how all events of the update process are recorded in the device. Including a description of how those events can be examined by a person, e.g., how they are indicated.

Description of how inadmissible influence on the metrological functions is prevented or minimized. Including a description of how time and processing resources are managed.

Description of how the assets are protected during and after the update if the

protection means are turned off during any point of the update process.

If the software is separated into fixed and variable modules, the following is required:

- a list of all fixed and variable software modules;
- a description of how the fixed modules administrate the update process.

Functional Checks

Initiate a download process with valid new software and check that the installation succeeds and all required information is recorded.

Initiate a download process with faulty (missing authenticity or integrity) new software and check that the installation is stopped and all required information is recorded.

Check the recorded information of the update process for consistency with the documentation.

If possible, check that an update is not performed if the required information cannot be recorded.

6 Instrument-specific solutions

6.1 Solution: fault recovery (active)

Risk Class B	Risk Class C	Risk Class D
General The software checks processed assets for faults and recovers to normal processing behavior.		
Variants A watchdog is sent heartbeats by the legally relevant software during normal operation. If heartbeats are not received for a certain time span, the watchdog resets the legally relevant software in an attempt to recover from faults.		
Conditions -		
Keywords Assets: - Security properties: - Attack vectors: - Status: active		
Required Documentation Description of the fault recovery mechanism and an explanation of how and when it is invoked. Description of the related tests carried out by the manufacturer. Description of fault recovery steps after an error, if this is required for software examination.		
Functional Checks Check that the implementation of fault recovery is appropriate. Check the correct execution of fault recovery in the presence of defined influencing quantities and provoked errors.		

6.2 Solution: backup facility (active)

Risk Class B	Risk Class C	Risk Class D
General Measurement data are periodically backed up in non-volatile memory. **Specific** If the data stored within the backup facility are used for fault recovery, the minimum interval for the backup shall be calculated according to relevant documents. The backup procedure should take priority over most other legally relevant functions.		

Variants

Taximeter

- A voltage level detector is used to trigger the backup of measurement data.
- The voltage level detector fires a trigger signal when the voltage level drops for a period of 15 seconds. Subsequently, measurement data, state values, and other relevant data are stored in the backup facility.
- If the voltage level returns to normal, the data are restored and the instrument continues or stops, see MID, MI-007, 9.

Continuous and dynamic measurement of quantities of liquids other than water

- The measuring system must be equipped with a backup power source to ensure that all measuring functions are carried out in the event of a failure of the main power supply, or it must be equipped with means to preserve and display the data so that the ongoing transaction can be terminated.
- The storage interval must be short enough that the difference between current and stored cumulative measurement data is as small as possible.

Conditions

-

Keywords

Assets:

-

Security properties:

-

Attack vectors:

-

Status:

active

Required Documentation

Description of which measurement data are backed up and when the backup is performed.

Description of the calculation of the minimum interval for the backup according to relevant documents.

If cumulative measurement data are backed up, description of the calculation of the maximum error that can occur.

Functional Checks

Check that the backups are created in the documented intervals.

If possible, trigger a backup by causing an error during normal operation and check that a backup is performed.

6.3 Solution: number of digits (active)

Risk Class B	Risk Class C	Risk Class D

General

The display has a sufficient number of digits, see also relevant documents.

No special equipment or tools are necessary to verify a sufficient number of digits (via the display).

There is no ambiguity as to what the primary and correct display is and what content is indicated on the display.

Variants

Water meters

- ISO 4064-1 [3] contains requirements in relation to the number of digits.
- The number of digits is based on the flow Q3 as follows: four digits for Q3 ≤ 6.3, five digits for 6.3 < Q3 ≤ 63, six digits for 63 < Q3 ≤ 630, and seven digits for 630 < Q3 ≤ 6300.
- The subdivisions of the verification scale shall be small enough to ensure that the resolution error of the indicating device does not exceed 0.25 % for accuracy class 1 meters, and 0.5 % for accuracy class 2 meters, of the volume passed during 90 min at the minimum flow rate Q1.
- Additional verification elements may be used provided that the uncertainty of reading is not greater than 0.25 % of the test volume for accuracy class 1 meters and 0.5 % of the test volume for accuracy class 2 meters and that the correct functioning of the register is checked.
- If the maximum indicating range for volume totalization is reached, the indicating range will start again from zero cubic meter.
- A combination meter may have two indications, the sum of which provides the overall volume.
- The visual verification display may have either a continuous or a discontinuous movement.

Active electrical energy meter

- Typical values for three phase electricity meters are: Emax (4000h) = 3*60 A * 230 V * 4000h / 1000 = 165600 kWh. This requires a presentation of at least 6 digits.

Gas meters and volume conversion devices

- Typical values for domestic gas meters are: Q_{max} = 6 m^3/h. The required range is then 48000 m^3 requiring 5 digits to fit (currently mechanical and electronic gas meters display up to 99999 m^3 which is more than adequate for this size of meter).

Conditions

-

Keywords

Assets:

-

Security properties:

- Attack vectors: - Status: active
Required Documentation Description of the display and the display menu. Description of the verification display and a description of how a visual verification is initiated.
Functional Checks Check that the number of digits is appropriate. If possible, initiate a visual verification and • check that the resolution of the visual verification display is appropriate and • check that special equipment or software for this control is part of the instrument.

6.4 Solution: display test (active)

Risk Class B	Risk Class C	Risk Class D
General A display test can be performed to check the correct functioning of all segments in the display. **Specific** Depending on the type of display, different elements are displayed to verify that the display renders everything correctly.		
Variants -		
Conditions -		
Keywords Assets: - Security properties: - Attack vectors: - Status: active		
Required Documentation Description of how the display test is initiated and what happens in the test.		
Functional Checks Initiate the display test and check that the display works correctly.		

6.5 Solution: inhibit cumulative measurement data from resetting (active)

Risk Class B	Risk Class C	Risk Class D
General For utility measuring instruments, the display showing the total quantity supplied, or the displays from which this can be derived from, cannot be reset during use. A hardware seal can be used to protect the registers, see *4.4.3.1*. **Specific** Cumulative registers of a measuring instrument are reset prior to the applicable conformity assessment procedure. Totalizers of the cumulative registers of a measuring instrument are reset before the relevant conformity assessment procedure is completed. During a conformity assessment procedure in accordance with annex D, F or H1, the utility meters are fitted with all securing and protection means as specified by the TEC after which resetting the cumulative measurement data is not possible without evidence of an intervention being created.		
Variants -		
Conditions The measuring instrument is a utility measuring instrument.		
Keywords Assets: - Security properties: - Attack vectors: - Status: active		
Required Documentation Description of how a reset is inhibited.		
Functional Checks Check that resetting the cumulative measurement data is protected, i.e., it is either impossible or leaves evidence of an intervention.		

6.6 Solution: reading of measurement results (active)

Risk Class B	Risk Class C	Risk Class D
General The measurement results that serve as the basis for the price to pay may be the results of different registers that are activated by remote control, a clock or other means. Each register represents the total quantity, connected to one rate in the		

billing process. It is possible to show the results on different displays, periodically or on request via the user interface.

If a meter is designed to count quantities in different registers, the meter can display the total quantities of each register as well as the currently active rate register on the display by means of the user interface.

Specific

It is allowed to show the results on different displays, periodically or on request via the user interface. However, when displaying different measurement results, it is clear which display belongs to which register, there is no ambiguity in that respect. Additional inscriptions can be provided to clarify the different registers.

Variants

-

Conditions

-

Keywords

Assets:
-
Security properties:
-
Attack vectors:
-
Status:
active

Required Documentation

Description of how the measurement results are obtained that serve as the basis for the price to pay.

Functional Checks

Check that measurement results are handled correctly.

6.7 Solution: power source lifetime for gas meters (active)

Risk Class B	Risk Class C	Risk Class D

General

A dedicated power source offers an energy capacity equivalent to a lifetime of at least five years.

After 90% of its lifetime an appropriate visual warning is shown.

Specific

Changing the power source does not inadmissibly influence the assets.

Variants

-

Conditions

Only applies to gas meters.

Keywords Assets: - Security properties: - Attack vectors: - Status: active
Required Documentation Description of the power source capacity, maximum lifetime. Description of how to determine the consumed or available energy. Description of how the warnings are issued depending on the remaining energy.
Functional Checks Check that the documented power source is appropriate to guarantee a lifetime of at least five years. If possible, check that a warning is shown if the remaining lifetime is below 10%. If possible, check that exchanging the power source does not inadmissibly influence any of the assets.

6.8 Solution: test element for gas meters (active)

Risk Class B	Risk Class C	Risk Class D
General The gas meter is equipped with a test element that enables tests to be carried out in a reasonable amount of time. **Specific** Usually, the tests are performed prior to installation and normal operation. During the test, the same software and registers are used as during normal operation.		
Variants -		
Conditions Only applies to gas meters.		
Keywords Assets: - Security properties: - Attack vectors: - Status: active		

Required Documentation
Description of the test element and how the tests are initiated.
Functional Checks
Check that the tests with the test element can be completed in a reasonable amount of time.

6.9 Solution: electronic conversion device for gas meters (active)

Risk Class B	Risk Class C	Risk Class D
General		
An electronic conversion device is capable to detect if the device is no longer within the operating range stated by the manufacturer. If not within the specified operating range, the conversion device shall stop integrating the converted quantity. Instead, it may totalize the converted quantity separately for the time it is operating outside the operating range.		
Specific		
If not within the specified operating range, a visual warning is shown.		
Variants		
There is only one cumulating register but the start and end date, time and register values of the out-of-range period are recorded in an audit trail, see *5.1*. Both quantities are indicated and the user can clearly identify and distinguish the regular and the failure indication by means of a status indication.		
Conditions		
Only applies to gas meters.		
Keywords		
Assets: - Security properties: - Attack vectors: - Status: active		
Required Documentation		
Description of the different registers for converted quantity and failure quantity.		
Functional Checks		
If possible, check that the device detects if it is no longer within the specified operating range and that the behavior matches the documentation.		

6.10 Solution: detecting fraudulent alterations for taximeters (active)

Risk Class B	Risk Class C	Risk Class D
General A facility checks the plausibility of the measured distance. **Specific** The output of the distance signal generator is continuously checked on its defined characteristics regarding voltage level, pulse width and the relation of speed and frequency (stability of the signal).		
Variants -		
Conditions Only applies to taximeters.		
Keywords Assets: - Security properties: - Attack vectors: - Status: active		
Required Documentation Description of how the plausibility of the measured distance is checked.		
Functional Checks If possible, invoke errors in the measured distance and check that they are detected.		

6.11 Solution: long-term storage on power loss for taximeters (active)

Risk Class B	Risk Class C	Risk Class D
General A facility automatically stores the totalized measurement data if the device is disconnected from power by means of a voltage detector that detects if the voltage drops. The data are stored before the internal voltage drops below the operating voltage. **Specific** The totalized measurement data are usually stored in non-volatile storage. Data storage takes appropriate priority over other legally relevant functions.		
Variants The totalized measurement data are stored continuously or in an appropriate interval that covers the time between the detection of a power loss until the (internal) voltage drops below the operating voltage.		

Conditions
Only applies to taximeters.
Keywords Assets: - Security properties: - Attack vectors: - Status: active
Required Documentation
Description of what data are stored and at which time they are stored.
Functional Checks
If possible, disconnect the device from power and check that all totalized measurement data are stored.

7 Currently not assigned solutions

7.1 Solution: no measurements during remote verification for measuring instruments other than utility meters (active)

Risk Class B	Risk Class C	Risk Class D
General During a remote verification for a measuring instrument other than utility meters, the measuring function is made inoperative, so that there is no possibility to display, print, store, or transmit measurement data except to the remote verification software.		
Variants -		
Conditions This solution does not apply to utility meters.		
Keywords Assets: - Security properties: - Attack vectors: - Status: active		
Required Documentation Description of how the remote verification is implemented.		
Functional Checks Start the remote verification procedure and check that the measuring function is made inoperative.		

7.2 Solution: plausibility check for data from outside the scope of the MID (active)

Risk Class B	Risk Class C	Risk Class D
General This solution only applies to legally relevant components that are outside the scope of the MID, e.g., the distance signal generator of a taximeter, see MID, MI-007, article 19. All data coming from outside the measuring instrument are checked for plausibility before they are processed. This includes inputs from a user via user interfaces. For digital inputs, the data are checked against valid interval and frequency, if applicable. For analog inputs, the data are checked as described in relevant documents.		

Variants
-
Conditions
This solution does not apply to utility meters.
Keywords
Assets: measurement data Security properties: integrity, authenticity Attack vectors: IIP1 Status: active
Required Documentation
Description of the module that checks the output signal of the legally relevant component outside the scope of the MID.
Functional Checks
Attempt to disrupt the output signal or replace the legally relevant component outside the scope of the MID and check for an appropriate reaction.

8 References

[1] „Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments”, Official Journal of the European Union L 96/149, 29.3.2014

[2] „Directive 2014/31/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of non-automatic weighing instruments”, Official Journal of the European Union L 96/107, 29.3.2014

[3] “ISO 4064-1:2024 Water meters for cold potable water and hot water - Part 1: Metrological and technical requirements”, Geneva, CH, Standard