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

WELMEC Guide 7.1

Informative Document:
Risk-Based Approach to Software Examination

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

Risk-Based Approach to Software Examination

Contents

Foreword

The informative document in hand aims at explaining the guidance on the core requirements provided by WELMEC Software Guides based on a risk assessment. The essential requirements in question are the ones covering securing and protection for software-controlled components according to WELMEC Guide 8.8, sub-assemblies according to the MID [1] or measuring instruments under the NAWID [2] or MID. Additionally, this document provides information on how this has been implemented in WELMEC Guides 7.2, 7.3, 7.4 and 7.6 and outlines the motivation for doing so.

Please note that this informative document distinguishes between the following two kinds of requirements:

- **Essential Requirements** (as specified in annex I and the instrument-specific requirements of the MID or annex I and III of the NAWID).

Example (Article 8.3 of annex I of the MID):

Software that is critical for metrological characteristics shall be identified as such and shall be secured.

- **Requirements** (as stated in a guidance block of WELMEC Guide 7.2, i.e., what is required to fulfill the essential requirement).

Example (R1 of WELMEC Guide 7.2):

All assets (software, parameters, measurement data, measurement result, evidence of an intervention, and inscriptions) in the measuring instrument shall be adequately protected to ensure their integrity, authenticity and availability.

The title of this document therefore refers to what is required to fulfill the essential requirements on a technical level. It is not the objective of this document to develop or modify the essential requirements.

Non-automatic weighing instruments are also covered by this approach, considering that the software-related essential requirements of the NAWID can be fully covered by a subset of the software-related essential requirements of the MID, see *Annex I* for a mapping between these two directives.

While the essential requirements of the MID refer to securing and protection, the WELMEC Software Guides will only require the protection of assets. Securing is covered by a separate attack vector and, therefore, is automatically covered when protection is implemented. Protection, e.g., by means of modern communication protocols, usually also provides a securing mechanism.

The guidances in the specified WELMEC Software Guides only cover protection requirements and not the functional requirements, although software-controlled measuring instruments or components also need to comply with specific functional requirements. However, most of the functional requirements are instrument-specific and therefore fall under the scope of the technical WGs.

To assist the technical WGs with the drafting of these functional requirements, Annex IV provides some guidance regarding certain general functional requirements mostly derived from OIML D31 [3]. The technical WGs are invited to use this guidance to develop their own instrument-specific guidance on the functional requirements for software-controlled measuring instruments.

If instrument-specific annexes of the MID lay down essential requirements for sub-assemblies, then these sub-assemblies are legally relevant as well. They are treated as legally relevant physical parts of the measuring instrument.

The examples below in this Guide also apply to such sub-assemblies.

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 includes 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

A	risk assessment examination Guidance
C	check based on the documentation
D	required documentation
DR	design-specific requirements
F	functional check
FR	functional requirements
LR	legally relevant
MID	Measuring Instruments Directive
MQV	measured quantity value
N	specifying note
NAWI	non-automatic weighing instrument
NAWID	Non-Automatic Weighing Instruments Directive
OS	operating system
R	requirement
S	check based on the source code
SW	software
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.

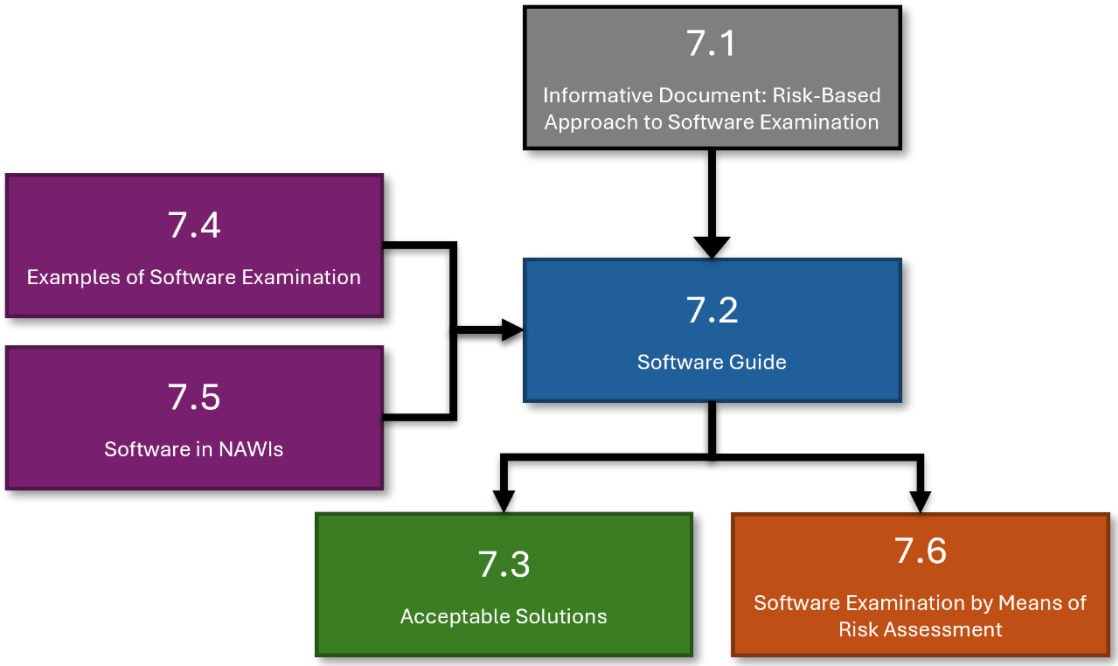

Figure 1: Relationship between the WELMEC Software Guides

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.

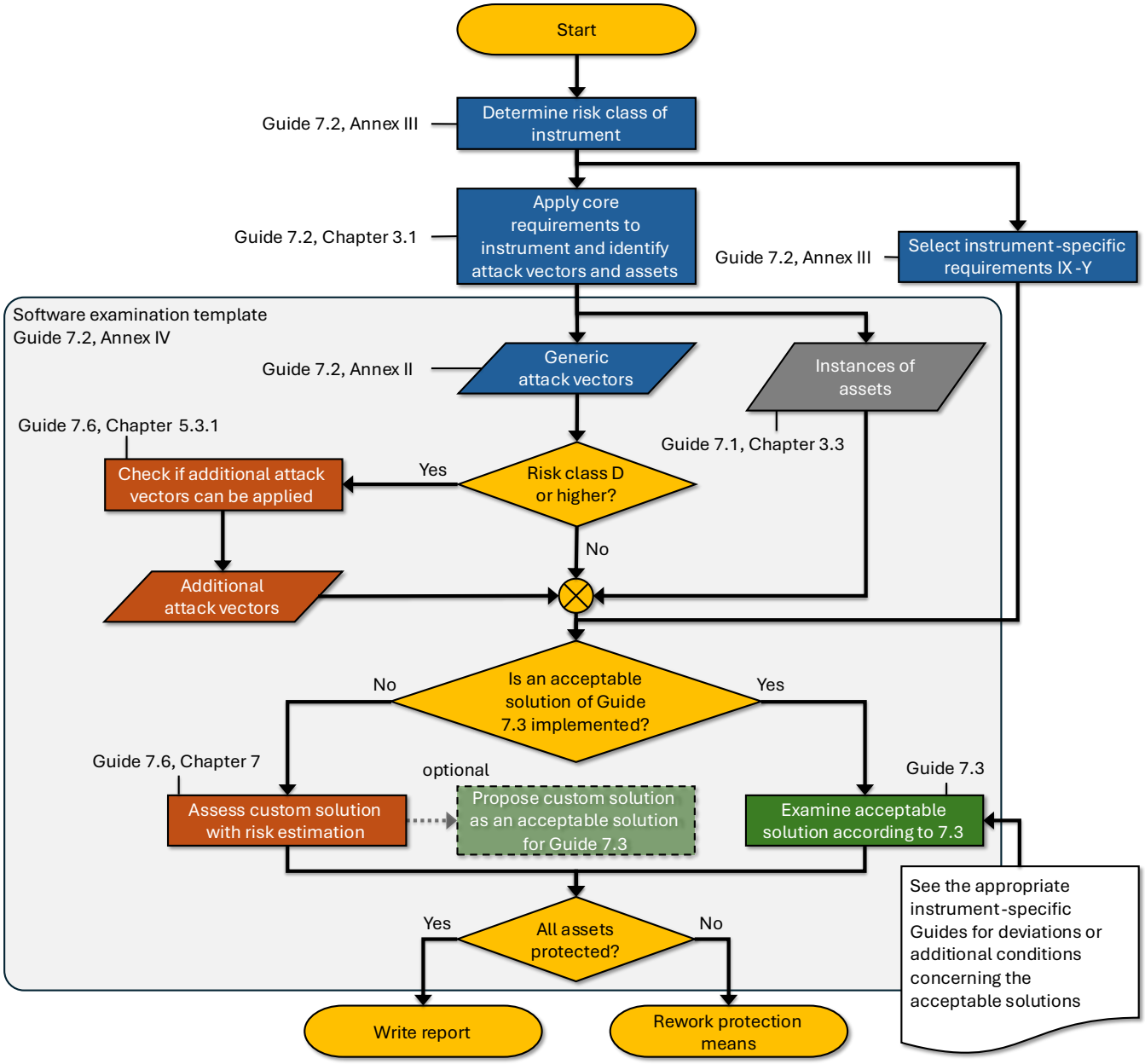

Figure 2: Workflow of the examination of the requirements using Guides 7.1, 7.2, 7.3, 7.6, and instrument-specific Guides (see the WELMEC website).

3 How to Derive Risk-Based Requirements

3.1 Assets

In legal metrology, an asset is an entity that has to fulfill and/or has an impact on the compliance with the

- essential requirements in annex I of the MID and the instrument-specific requirements of the MID, or
- essential requirements in annex I of the NAWID, or
- requirements from other harmonized standards or normative documents.

This chapter primarily deals with assets derived from the essential requirements of the MID. The essential requirements of the NAWID are covered by the essential requirements of the MID in full (see *Annex I*).

If an article of annex I of the MID or NAWID addresses an entity, it becomes an asset that needs to fulfill the essential requirements.

Example:

The MID has several essential requirements (see *Table 1*:) that address the measurement result:

1. Permissible errors
2. Reproducibility
3. Repeatability
4. Discrimination and Sensitivity
5. Durability

Therefore, since the essential requirements address the measurement result, the measurement result becomes an asset because inadmissible changes or influence on the measurement result might lead to a non-conformity, e.g., to an error larger than the permissible error.

In *Annex II* of this Guide, all essential requirements of annex I of the MID are discussed and mapped to assets with associated security properties.

The basic process of asset and requirement derivation, which forms the basis of the WELMEC Software Guides, is as follows:

- Step 1: Identify Assets
- Step 2: Define the asset properties that must be protected (= Security Properties)
- Step 3: Extend the asset definition to several instances
- Step 4: Identify the risks to the security properties of the assets
- Step 5: Derive requirements to minimize the risks to the security properties of the assets.

The resulting list of assets is shown in *Table 1*:.

Asset	Essential requirements of annex I of the MID
Software[1]	7.1, 7.2, 7.6, 8.1, 8.2, 8.3, 8.4
Parameters	7.1, 8.1, 8.2, 8.4
Measurement data	7.1, 8.1, 8.4
Measurement result	1, 2, 3, 4, 5, 10.1, 10.2, 11.1, 11.2
Evidence of an intervention	7.1, 8.2
Inscriptions[2]	9.1, 9.5, 9.7, 9.8

Table 1: Identified assets based on annex I of the MID

In many cases, the assets established in this way, when protected, result in further assets. Such indirectly established or deduced assets are, e.g., identification of assets, protection means for assets, and evidence of an intervention.

Example:

- If you have several selectable sets of calibration factors that are set by the user and belong to the assets of a measuring instrument, then the identification of each set is an asset, too.
- If a function computes the measurement result and is protected by a checksum, then the function calculating the checksum and the nominal value are assets, too.

If a change of a legally relevant parameter is written to a logbook for later check, then the logbook is an asset, too.

It is assumed that as long as annex I of the MID is not changed, there is no need for WELMEC to reevaluate whether all the assets are covered if new technology is used, and what functionality is considered legally relevant.

Functional design-specific requirements are discussed separately, see *Annex IV*.

3.2 Security properties

Taking into account the essential requirements of the MID and the NAWID, the following security properties have been defined for the assets: integrity, authenticity, and availability, see also *Annex II*.

Example:

- If a function computes the measurement result, it should not be changed once the measuring instrument is on the market, since the integrity of the function has to be kept.
- If several calibrated and non-calibrated sensors are used to produce a raw value, the authenticity of each raw value for the respective sensors is to be ensured.

If a function is protected by a checksum calculation, then the calculation must be available at any time.

[1] Protection means are interpreted as part of the software.
[2] As an example, the CE marking would be an inscription, but not an indication.

It is assumed that as long as annex I of the MID is not changed, the security properties need not be reevaluated when new technology is used.

Annex II contains the security properties for each of the essential requirements of the MID, and each of the assets, respectively.

It should be noted that availability of assets can be achieved by providing evidence of an intervention if an asset is no longer available.

3.3 Instances of assets

Assets can exist in a number of instances at any time and any place. For example, instances of measurement data could be present on one component and another instance may be transmitted to and, e.g., processed, stored, or indicated on a different component. It may happen that instances of assets appear more than once in a measuring instrument, e.g., one instance of measurement data is transmitted between sensor and computing unit, and a second instance of this data – now post-processed – is transmitted between computing unit and display.

Therefore, adequate protection has to be ensured for all instances of each individual asset at any time and any place during the operating time of the measuring instrument.

The assets and the essential requirements may be compressed to the statement “All assets must be protected” (R1). In combination with the respective documentation requirements, the so-called core requirements are established. These are listed in Guide 7.2.

3.4 Core requirements

The core requirements are formulated in an attempt to make them technologically independent, that is to say, the implementation of new technology should be possible without (re)formulating the core requirements.

The core requirement R2 specifies some details regarding the evidence of an intervention, e.g., what kind of information shall be provided, how it shall be provided, and that checks shall be periodically carried out to ensure that no changes have occurred and, if the check fails, that further appropriate action is taken.

In core requirement R3, additional requirements are given for parameters that are not intended to cause a subsequent verification.

Regarding the documentation, multiple requirements alongside the core requirements R1, R2 and R3 have been formulated, detailing the scope and content required.

Again, it is envisioned that these are the only requirements that apply with regard to the protection of the assets.

3.5 Legally relevant parts and properties of a measuring instrument

Not all parts and properties of a measuring instrument may contribute to fulfilling the essential and instrument-specific requirements, so not all parts and properties may be considered as being legally relevant.

Example:

A voltmeter shows the measured voltage and, for information of the user, current date and time. Date and time are not important for the voltmeter to fulfill its function. Voltage is considered a legally relevant measurement result, date and time are considered as being legally non-relevant.

All legally non-relevant parts and properties of the measuring instrument may be neglected in the examination.

MID and NAWID do not establish requirements for such legally non-relevant parts, with one exception: Essential requirement 7.6. of the MID states that “software which provides other functions” shall not inadmissibly influence the measuring function.

To find legally relevant and legally non-relevant parts and properties of a measuring instrument, one may imagine the “measurement chain”, i.e. the path between a physical quantity and its output as measurement result with value and unit. All parts and properties that contribute to this path (directly or indirectly) are legally relevant.

In Annex III, more explanation and some examples are given. Additional information can be found in relevant documents.

4 General Principle of Software Examination

For the application and examination of the risk-based requirements, it is required that the manufacturer lists all assets present in the measuring instrument or components. Furthermore, the manufacturer has to list the design features of his measuring instrument, such as storage devices, interfaces or operating systems.

For the conformity assessment, the manufacturer also has to supply a risk assessment report to demonstrate conformity of the measuring instrument with the essential requirements, see MID, annex II, Module B 3c and NAWID, annex II, Module B 1.3c.

Regarding software related requirements, this means that the report has to cover all attacks against all assets present and the proposed means (also called solutions) to mitigate those attack vectors through protection of the assets.

Protection aims to ensure that inadmissible influence on the assets is either impossible or an intervention is detected and acted upon, i.e., the integrity, authenticity, and availability of all assets have to be ensured at all times.

The examiner has to check for each asset present in a measuring instrument or component whether the solutions to mitigate the attack vectors either make inadmissible influence impossible or inadmissible influence is detected and acted upon.

Depending on the measuring instrument or component, certain assets might not be present.

Example:

On a storage device, only the measurement data and the legally relevant software are stored. The remaining assets parameters, evidence of an intervention, and/or inscriptions are not present. In that case, only adequate protection of the measurement data and of the legally relevant software has to be checked.

The adequacy of a solution might depend on the implemented technology and the actual assets that are involved.

Example:

For wireless transmission to a cloud storage device, a hardware seal to ensure authenticity is not adequate because wireless connections can be manipulated without accessing the hardware interfaces.

5 Implementation in WELMEC Guides 7.2, 7.3, and 7.6

The guidance in the different Guides is implemented through so-called guidance blocks.

Although the requirements apply to all measuring instruments, the adequacy of an acceptable solution depends on the risk level for a particular measuring instrument. Related to this are the documentation requirements which may differ for certain risk classes. To make this clear, measuring instruments are assigned to a risk class, and this is further highlighted in a guidance block.

Risk classes are explained in subchapter 5.2.

5.1 Guidance blocks

5.1.1 Types of guidance blocks

There are three types of guidance blocks:

1. A requirement block that addresses the core requirements, see Guide 7.2.
2. A solution block that addresses the acceptable solutions, see Guide 7.3.
3. An attack vector block that addresses the attacks, see Guide 7.2.

The basic structure of all three types of guidance blocks is similar but shows slight deviations. A detailed explanation of the requirement blocks is given in subchapter 5.1.2, of the solution blocks in subchapter 5.1.3, and of the attack vector blocks in subchapter 5.1.4.

5.1.2 Requirement block of guide 7.2

A requirement block in Guide 7.2 contains the actual guidance on how to comply with the requirements regarding protection and how compliance with the core requirements can be validated.

It consists of a defining text, explanatory specifying notes, the documentation to be provided, and an examination guidance containing checks based on the documentation, functional checks, the risk assessment examination guidance and checks based on the source code.

The content within a requirement block may be subdivided according to risk classes, see chapter *5.2*.

Risk Class X	**Risk Class Y**	**Risk Class Z**	**Observations**
R1 Requirement 1 R2 Requirement 2			The starting point is the requirement
Specifying Notes R1/N1 Specifying note 1 for requirement 1 R2/N1 Specifying note 1 for requirement 2 R2/N2 Specifying note 2 for requirement 2			Specifying notes shall contain additional information concerning the main statement of requirements, i.e., scope of application, additional

<table>
<tr><td colspan="2"></td><td>explanations, exceptional cases, etc.
Specifying notes shall not contain requirements.
To highlight the correlation between requirements and specifying notes, the notes are numbered accordingly.</td></tr>
<tr><td colspan="2">Required Documentation
R1/D1 Required documentation 1 necessary to check for compliance with requirement 1
R2/D1 Required documentation 1 necessary to check for compliance with requirement 2
R2/D2 Required documentation 2 necessary to check for compliance with requirement 2</td><td>Documentation for each requirement and specifying note is needed, given that part of the conformity assessment is carried out by checking the documentation.
The numbering facilitates the assignment of the required documentation to the respective requirements.</td></tr>
<tr><td></td><td>R2/D3 Source Code</td><td>For certain higher risk classes, an examination based on the source code is required. Therefore, the required documentation is extended by the source code.</td></tr>
<tr><td>Examination Guidance
Checks Based on the Documentation
R1/C1 Examination guidance 1 to check for compliance with requirement 1
R2/C1 Examination guidance 1 to check for compliance with requirement 2
R2/C2 Examination guidance 2 to check for compliance with requirement 2</td><td></td><td>The examination guidance is given for checks based on the documentation, functional checks, risk assessment examination guidance, and, for the higher risk classes, checks based on the source code.
Checks based on the documentation are performed to verify that protection means have been implemented as required.</td></tr>
</table>

Functional Checks R1/F1 Functional check 1 for requirement 1 R2/F1 Functional check 1 for requirement 2			Functional checks are performed to verify that protection means are working as intended.
Risk Assessment Examination Guidance R1/A1 Examination guidance 1 for the risk assessment for requirement 1 R2/A1 Examination guidance 1 for the risk assessment for requirement 2 R2/A2 Examination guidance 2 for the risk assessment for requirement 2			The risk assessment examination guidance provides further details for how Guide 7.3 is used to check an acceptable solution, and how Guide 7.6 is used to check a risk assessment on the implemented risk mitigation means.
Checks Based on the Source Code			
-	R1/S1	Check 1 of the source code to check for compliance with requirement 1	For certain higher risk classes, an examination based on the source code is required. Therefore, the required examination guidance is extended by the source code.

Table 2: Structure of a requirement block of Guide 7.2. The following notation is used: R for requirement, N for specifying note, D for documentation, C for checks based on the documentation, F for functional checks, A for risk assessment examination guidance, S for checks based on the source code.

The content of the requirement blocks needs to be formulated in a certain way to

- maximize the readability and applicability, minimize the risk of contradictions between all items in a requirement block, i.e., between requirements, specifying notes, required documentation and examination guidance,
- minimize the risk that certain aspects, such as documentation or examination guidance, do not or not fully cover all the requirements and specifying notes or vice versa, that a documentation requirement or examination guidance does not originate from a requirement and/or specifying note.

For that purpose, the requirement block is divided into two parts.

The upper part contains:

- The requirement. This is the actual guidance concerning what is required to fulfill the essential requirements.
- The explanatory specifying notes:
  - They contain additional information concerning the main statement of the requirements, i.e., scope of application, additional explanations, exceptional cases, etc.
  - They do not contain additional requirements.
  - They are presented in such a way that the relation between requirement and specifying note is clear, i.e., by corresponding numbers. It could be that specifying notes contain multiple additional pieces of information about one requirement, this is visualized by adding levels to the numbering, i.e., R1/N1, R1/N2, R2/N1, R2/N2.

The lower part contains:

- The required documentation. This is presented in such a way that the relation between requirement and documentation is clear, i.e., by corresponding numbers.
  - The MID and NAWID require that the manufacturer submit technical documentation that render the design, manufacture, and operation of the measuring instrument intelligible[3].
  - The technical documentation shall make it possible to assess the measuring instrument's conformity with the applicable requirements of the respective directive and shall include an adequate analysis and assessment of the risk(s)[4].
- The examination guidance, which aims at different kinds of checks:
  a) **Based on documentation**: With the submitted documentation, the examiner can check whether the proposed solution is addressed adequately. It is therefore imperative that the documentation covers all requirements and that the examination guidance is covered by the required documents.
  b) **Functional checks**: With these checks, the examiner can actually test the practical implementation of the proposed solution.
  c) **Risk assessment examination guidance**: This guidance provides further details for how Guides 7.3 and 7.6 are used to check implemented risk mitigation means.
  d) **Checks based on the source code**: For risk class E, an examination based on the source code is required. Therefore, the required documentation is extended by the source code.
  Considering the general nature of this required documentation, this is the only documentation requirement not linked to a specific requirement or specifying note.

An implemented requirement block can be found in Guide 7.2, chapter 3.

[3] See MID, article 18, and NAWID, Annex II.

[4] See the relevant articles in modules B, G and H1 of the MID and the NAWID.

5.1.3 Solution block of guide 7.3

The solution blocks of Guide 7.3 follow the same principle as the requirement blocks, but with the focus on the acceptable solutions. Instead of specifying notes, the acceptable solution is described together with the conditions that must be present in the measuring instrument.

An acceptable solution may cover a requirement only in part, e.g.,

- it might cover all or multiple attack vectors or only a single attack vector, e.g., the communication interface;
- it can apply to all assets or only certain assets, for example only software and parameters;
- it can cover all security properties, or only a specific one, e.g., only integrity.

The solution block therefore describes the acceptable solution, the conditions that must be present in the measuring instrument, and which attack vectors, assets, and security properties are covered by the acceptable solution.

A generic solution block for Guide 7.3 is given in Table 3.

Examples of implemented solution blocks may be found in Guide 7.3, chapter 4.

Risk Class X	Risk Class Y	Risk Class Z
General The description of the acceptable solutions shall provide all details necessary to understand and implement a solution in a real-world measuring instrument. **Specific** Technical details and specific implementation details are listed here.		
Variants Variations of this solution that do not change any of the keyword characteristics.		
Conditions Design or technological conditions that have to be present in the measuring instrument for this solution to be implementable.		
Keywords Assets: all assets that are covered by the acceptable solution Security properties: all security properties of the assets that are covered by the acceptable solution Attack vectors: the identifiers of all attack vectors that are covered by the acceptable solution Status: the status of the solution shall be either “active” or “withdrawn”		
Required documentation The required documentation shall list all information necessary to show the correct implementation of the solution.		

Functional Checks
The functional checks shall list all information necessary to functionally test the correct implementation of the solution.

Table 3: Structure of a solution block of Guide 7.3.

5.1.4 Attack vector block of Guide 7.2

The attack vector blocks in Annex II of Guide 7.2 follow the same principle described above, but with the focus on generic attack vectors derived from MID, annex I. The attack vectors in Annex II of Guide 7.2 do not include the required documentation because this is already covered by the guidance block(s) in chapter 3 of Guide 7.2, “Core Requirements”.

The guidance blocks given in Annex II of Guide 7.2 may serve as examples of implemented attack vector blocks.

5.2 Risk classes

5.2.1 General principle

The contents of Guides 7.2, 7.3, 7.4 and 7.6 are differentiated according to risk classes. In these Guides, risks are related to software and not to any other risks associated with a measuring instrument, e.g., electrical safety.

Each measuring instrument, component or module shall be assigned to a risk class because the guidance is tailored to the risk class the measuring instrument belongs to. Instrument-specific WGs shall assign individual risk classes to specific types of measuring instruments, components or modules. The attacker motivation score described in Guide 7.6 can provide WGs some aid when deciding on the applicable risk class.

Risks addressed by the Guides are derived from three factors: adequate level of protection of assets, adequate level of examination of software, and appropriate level of conformity to type.

A risk class is a combination of levels of these factors where the definition of levels is indirectly made by the correspondingly necessary countermeasure. Three levels of adequate countermeasures, low, middle, and high, are introduced for each of the factors. The higher the appropriate level is assumed, the higher the level of a countermeasure.

5.2.2 Description of levels of countermeasures for the risk factors

The following definitions are used for the corresponding levels:

Protection levels

Low: No particular protection means against intentional changes are required.

Middle: The software is protected against intentional changes made by using easily available and simple common software tools (e.g., text editors).

High: The software is protected against intentional changes made by using sophisticated software tools (debuggers and hard disc editors, software development tools, etc.).

Software examination levels

Low: Standard type examination including functional testing of the measuring instrument is performed. No extra software testing is required.

Middle: In addition to the conformity level “low”, the software is examined based on its documentation. The documentation includes the description of the software functions, parameters, etc. Practical tests of the software-supported functions (spot checks) may be carried out to check the plausibility of the documentation and the effectiveness of protection means.

High: In addition to the conformity level “middle”, an in-depth examination of the software is carried out, usually based on the source code.

Software conformity levels

Low: The legally relevant software of individual measuring instruments is considered to conform to the legally relevant software of the type under examination if the functionality of the software corresponds to the technical documentation of the type. The binary code of the software itself does not need to be identical to the software of the type.

Middle: In addition to the conformity level “low”, the binary code of legally relevant software of individual measuring instruments is identical to the software of the type under examination (or re-examination).

High: The binary code of all the software implemented in the individual measuring instruments is identical to the software of the type under examination.

5.2.3 Derivation of risk classes

Out of the 27 theoretically possible level combinations, only 3 or at the utmost 6 are of practical interest (risk classes B, C, D and possibly A, E and F). They cover all of the measuring instrument classes regulated by the MID and are listed in *Table 4.*

Moreover, they provide a sufficient window of opportunity should risk evaluations change. The risk classes are defined in the table below. The table shall be interpreted in such a way that a certain risk class is defined by the corresponding combination of levels of necessary countermeasures.

In addition, the corresponding maximum risk score for the risk assessment described in Guide 7.6 is given in the rightmost column of the table.

Risk Class	Software Protection	Software Examination	Software Conformity	Risk score
A	low	low	low	≤ 5
B	middle	middle	low	≤ 4
C	middle	middle	middle	≤ 3
D	high	middle	middle	≤ 2
E	high	high	middle	1
F	high	high	high	1

Table 4: Most common and practical risk classes.

5.2.4 Interpretation of risk classes

Risk class A: It is the lowest risk class of all. No particular means against intentional changes of software are required. Examination of software is part of the functional testing of the device. Conformity is required on the level of documentation. It is not expected that any measuring instrument will be classified as a risk class A measuring instrument. However, by introducing this class, this possibility is kept open.

Risk class B: In comparison to risk class A, the protection of software level is raised to “middle”. Correspondingly, the examination level is raised to “middle” as well. The conformity remains unchanged in comparison to risk class A.

The software examination is carried out based on the documentation. In consequence, the type examination certificate allows for different implementations with respect to the same documentation when placing the measuring instruments on the market[5].

Risk class C: In comparison to risk class B, the conformity level is raised to “middle”. This means, the binary code of the legally relevant software of individual measuring instruments is identical to the software of the type under examination. The levels of protection and examination remain unchanged in comparison to risk class B.

Risk class D: The significant difference in comparison to risk class C is the upgrade of the protection level to “high”. The examination level remains unaffected at “middle”, therefore sufficiently informative documentation shall be provided to show that the protection means taken are appropriate. The conformity level remains unchanged in comparison to risk class C.

Risk class E: In comparison to risk class D, the examination level is raised to “high”. The levels of protection and conformity remain unchanged.

Risk class F: The levels with respect to all aspects (protection, examination and conformity) are set to “high”. The difference to risk class E is that there is not any legally non-relevant software anymore.

Unless specified otherwise in the relevant documents, all measuring instruments are assigned to risk class C by default.

5.3 Adding acceptable solutions to Guide 7.3

Guide 7.3 contains acceptable solutions that are considered to be adequate to ensure the availability, and/or integrity, and/or authenticity of the assets. Acceptable solutions are not mandatory, a manufacturer can use his own solution, in which case the adequacy is examined in accordance with Guide 7.6.

If a solution is adequate, a notified body or the manufacturer himself can ask WG7 if the specific solution can be included as an acceptable solution in Guide 7.3. Note that the notified body first has to ask the manufacturer for permission. If permission is granted, the following steps have to be followed:

[5] After having placed the measuring instrument on the market, the permission to change software depends on national legislation.

- The request to implement this specific solution as an acceptable solution in Guide 7.3 has to contain:
  - a description of the acceptable solution, together with a solution block that contains:
    - the technical conditions that must be present in the measuring instrument for the solution to be implementable, e.g., the operating system;
    - covered security properties;
    - covered attack vectors.
  - The evaluation by the notified body.
  - The risk analysis performed by the manufacturer that shows the attack vectors that have been taken into consideration for this solution and explains how these are mitigated.
- The request can then be discussed within WG7 to decide on further steps.
- It might be necessary to have the solution evaluated by other notified bodies (second opinion).
- If WG7 agrees with the solution, it implements it in Guide 7.3.

Acceptable solutions are implemented in Guide 7.3 accompanied by the year they were included in the document.

This provides the opportunity to withdraw an acceptable solution if it no longer applies or is updated with a newer version, taking into consideration that this might not affect measuring instruments in the field.

In the rare event that an acceptable solution proves to not be adequate, measures have to be taken to correct this, see MID, chapter 2.

The above necessitates that the status of the acceptable solution is stated in Guide 7.3 together with the reason of withdrawal to evaluate the impact on the measuring instruments in use.

6 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 (recast) Text with EEA relevance, OJ L 96, 29.3.2014, p. 149–250.

[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 (recast) Text with EEA relevance, OJ L 96, 29.3.2014.

[3] "OIML D31 General requirements for software-controlled measuring instruments," *International Organization of Legal Metrology, Paris, France, Tech. Rep.*, October 2023. [Online]. Available: https://www.oiml.org/en/publications/documents/en/files/pdf_d/d031-e23.pdf

Annex I. Mapping between the NAWID and the MID

The mapping provided in this document is based on the 17th resolution of the 33rd WELMEC Committee meeting 2017. There, the WELMEC Committee emphasized the fact that the software-related essential requirements of the NAWID could be fully covered by a subset of the software-related essential requirements of the MID.

In the present mapping, the MID requirements are mapped to the NAWID requirements. In some cases, different MID requirements map to the same NAWID requirement. The NAWID essential requirements are taken from either annex I or annex III, the MID essential requirements from annex I.

The table also notes the following:

- Some MID requirements that do not apply to NAWIs.
- Some NAWID requirements that are considered instrument-specific requirements.
- Some NAWID requirements that are specific for NAWIs and are not covered by annex I of the MID.

NAWID	Wording	MID	Wording	Remarks
1	The units of mass used shall be the legal units within the meaning of Council Directive 80/181/EEC of 20 December 1979 on the approximation of the laws of the Member States relating to units of measurement.	**9.5**	The unit of measurement or its symbol shall be shown close to the numerical value.	-
1.1	Those instruments shall bear visibly, legibly, and indelibly the following inscriptions	**8.4**	Measurement data, software that is critical for measurement characteristics and metrologically important parameters stored or transmitted shall be adequately protected against accidental or intentional corruption.	-

1.2	Those instruments shall have adequate facilities for the affixing of the conformity marking and inscriptions. These shall be such that it shall be impossible to remove the conformity marking and inscriptions without damaging them, and that the conformity marking and inscriptions shall be visible when the instrument is in its regular operating position.	**9.6**	A material measure shall be marked with a nominal value or a scale, accompanied by the unit of measurement used.	-
8.1	Design and construction of the instruments shall be such that the instruments will preserve their metrological qualities when properly used and installed and when used in an environment for which they are intended.	**7.6**	The test procedure shall be described in the operation manual.	This is dealt with in instrument-specific Guides. See the WELMEC website for the appropriate WELMEC Guide that deals with this subject.
8.1	The value of the mass must be indicated.	**9.7**	The units of measurement used and their symbols shall be in accordance with the provisions of Union legislation on units of measurement and their symbols.	For NAWIs, it is not possible to only print or record the measurement result. The measurement result shall be indicated.
8.1	Design and construction of the instruments shall be such that the instruments will preserve their metrological qualities when properly used and installed and when used in an environment for which they are intended.	**6**	A measuring instrument shall be designed to reduce as far as possible the effect of a defect that would lead to an inaccurate measurement result, unless the presence of such a defect is obvious.	-

8.2	When exposed to disturbances, electronic instruments shall not display the effects of significant faults or shall automatically detect and indicate them. Upon automatic detection of a significant fault, electronic instruments shall provide a visual or audible alarm that shall continue until the user takes corrective action or the fault disappears.	**7.1**	A measuring instrument shall have no feature likely to facilitate fraudulent use, whereas possibilities for unintentional misuse shall be minimal.	-
8.3	Digital electronic devices shall always exercise adequate control of the correct operation of the measuring process, of the indicating device, and of all data storage and data transfer.	**8.3**	Software that is critical for metrological characteristics shall be identified as such and shall be secured.	In the context of this Guide, securing that provides evidence of an intervention is considered protection.
8.3	The requirements of points 8.1 and 8.2 shall be met on a lasting basis during a period of time that is normal in view of the intended use of such instruments. Upon automatic detection of a significant durability error, electronic instruments shall provide a visual or audible alarm that shall continue until the user takes corrective action or the error disappears.	**7.3**	The errors of a utility measuring instrument at flows or currents outside the controlled range shall not be unduly biased.	-
8.4	When external equipment is connected to an electronic instrument through an appropriate interface the metrological qualities of the instrument shall not be adversely influenced.	**8.1**	The metrological characteristics of a measuring instrument shall not be influenced in any inadmissible way by the connection to it of another device, by any feature of the connected device itself or by any remote device that communicates with the measuring instrument.	-

8.5	The instruments shall have no characteristics likely to facilitate fraudulent use, whereas possibilities for unintentional misuse shall be minimal.	**7.4**	Where a measuring instrument is designed for the measurement of values of the measurand that are constant over time, the measuring instrument shall be insensitive to small fluctuations of the value of the measurand, or shall take appropriate action.	-
8.5	The instruments shall have no characteristics likely to facilitate fraudulent use, whereas possibilities for unintentional misuse shall be minimal.	**7.5**	A measuring instrument shall be robust and its materials of construction shall be suitable for the conditions in which it is intended to be used.	-
8.5	The instruments shall have no characteristics likely to facilitate fraudulent use, whereas possibilities for unintentional misuse shall be minimal.	**7.6**	and shall not be inadmissibly influenced by the associated software.	-
8.5	Components that may not be dismantled or adjusted by the user shall be secured against such actions.	**8.2**	A hardware component that is critical for metrological characteristics shall be designed so that it can be secured.	In the context of this Guide, securing that provides evidence of an intervention is considered protection.
8.5	The instruments shall have no characteristics likely to facilitate fraudulent use, whereas possibilities for unintentional misuse shall be minimal.	**8.3**	Software identification shall be easily provided by the measuring instrument.	In the context of this Guide, securing that provides evidence of an intervention is considered protection.
8.6	Instruments shall be designed to permit ready execution of the statutory controls laid down by this Directive.	-	-	-

8.6	Instruments shall be designed to permit ready execution of the statutory controls laid down by this Directive.	**8.2**	Security measures foreseen shall provide for evidence of an intervention.	-
-	-	**8.3**	Software that is critical for metrological characteristics shall be identified as such	Does not apply to NAWIs.
-	-	**8.3**	Evidence of an intervention shall be available for a reasonable period of time.	Does not apply to NAWIs.
-	-	**9.1**	A measuring instrument shall bear certain inscriptions.	Does not apply to NAWIs.
9	The indication of the weighing results and other weight values shall be accurate, unambiguous and non-misleading	**9.8**	All marks and inscriptions required under any requirement shall be clear, non-erasable, unambiguous and non-transferable.	-
		10.1	Indication of the result shall be by means of a display or hard copy.	-

9	and the indicating device shall permit easy reading of the indication under normal conditions of use. Secondary indications may be shown, provided that they cannot be mistaken for primary indications. Indication shall be impossible above the maximum capacity (Max), increased by 9 e. An auxiliary indicating device is permitted only to the right of the decimal mark. An extended indicating device may be used only temporarily, and printing shall be inhibited during its functioning.	**10.2**	The indication of any result shall be clear and unambiguous and accompanied by such marks and inscriptions necessary to inform the user of the significance of the result. Easy reading of the presented result shall be permitted under normal conditions of use. Additional indications may be shown provided they cannot be confused with the metrologically controlled indications.	- - These NAWID requirements are considered instrument-specific and are not part of the “general” software requirements of Guide 7.2.
10	Printed results shall be correct, suitably identified and unambiguous. The printing shall be clear, legible, non-erasable and durable.	-	-	The preliminary observation mentions that a NAWI can record the weighing result.
14	Instruments for direct sale to the public shall show all essential information about the weighing operation and, in the case of price-indicating instruments, shall clearly show the customer the price calculation of the product to be purchased.	-	-	-
14	Instruments for direct sales to the public shall safeguard customers against incorrect sales transactions due to their malfunctioning.	**7.2**	A measuring instrument shall be suitable for its intended use taking account of the practical working conditions and shall not require unreasonable demands of the user in order to obtain a correct measurement result.	-

14	Price-computing instruments shall display the essential indications long enough for the customer to read them properly.	**10.3**	In the case of a hard copy, the print or record shall also be easily legible and non-erasable.	-
14	Instruments shall bear no characteristics that can cause, directly or indirectly, indications the interpretation of which is not easy or straightforward.	**10.4**	A measuring instrument for direct sales trading transactions shall be designed to present the measurement result to both parties in the transaction when installed as intended.	-
14	The price to pay, if indicated, shall be accurate.	**10.2**	Easy reading of the presented result shall be permitted under normal conditions of use.	This is considered an instrument-specific requirement. MID measuring instruments with price to pay have a similar requirement in the instrument-specific annexes.
14	Price-computing instruments may perform functions other than per-article weighing and price computation only if all indications related to all transactions are printed clearly and unambiguously and are conveniently arranged on a ticket or label for the customer.	**10.2**	The indication of any result shall be clear and unambiguous	This is NAWI-specific.
14	Auxiliary indicating devices and extended indicating devices are not permitted.	-	-	This is NAWI-specific.
14	Supplementary devices are permitted only if they cannot lead to fraudulent use.	-	-	This is NAWI-specific.

14	Instruments similar to those normally used for direct sales to the public which do not satisfy the requirements of this Section must carry near to the display the indelible marking 'Not to be used for direct sale to the public'.	-	-	This is NAWI-specific but not software-related.
-	-	**10.4**	When critical in case of direct sales, any ticket provided to the consumer by an ancillary device not complying with the appropriate requirements of this Directive shall bear appropriate restrictive information.	The preliminary observation mentions that a NAWI can record the weighing result although no requirements are given for storage. The EN45501 that gives presumption of conformity for the NAWID, addresses storage of measurement data as well, see WELMEC Guide 7.5.
-	-	**10.5**	Whether or not a measuring instrument intended for utility measurement purposes can be remotely read, it shall in any case be fitted with a metrologically controlled display accessible without tools to the consumer. The reading of this display is the measurement result that serves as the basis for the price to pay.	For a NAWI, it is typically considered that a print-out provides the durable proof. However, this is not always required. See requirement 10 of annex I of the NAWID.

14	Price-computing instruments may perform functions other than per-article weighing and price computation only if all indications related to all transactions are printed clearly and unambiguously and are conveniently arranged on a ticket or label for the customer.	**11.1**	A measuring instrument other than a utility measuring instrument shall record by a durable means the measurement result accompanied by information to identify the particular transaction, when: • the measurement is non-repeatable; and • the measuring instrument is normally intended for use in the absence of one of the trading parties.	This is NAWI-specific.
15	Price labelling instruments shall meet the requirements of price indicating instruments for direct sale to the public, as far as applicable to the instrument in question. The printing of a price label shall be impossible below a minimum capacity.	**11.2**	Additionally, a durable proof of the measurement result and the information to identify the transaction shall be available on request at the time the measurement is concluded.	This is considered an instrument-specific requirement. For automatic weight price labelers, it is stated in the instrument-specific annex VIII (MI-006) of the MID that any result outside the measurement range shall be identified as such, where a printout is possible.
-	-	**12**	A measuring instrument shall be designed so as to allow ready evaluation of its conformity with the appropriate requirements of this Directive.	

Table 5: Mapping of NAWID and MID essential requirements.

Annex II. Assets and Security Properties in Legal Metrology

The identified assets and security properties based on the essential requirements in annex I of the MID, are listed in the table in this Annex.

For each requirement, the identified assets and security properties are listed. Sometimes, the description of the requirement has been modified to suit the purpose of this Annex. The column “MID Requirement” in the table refers to the respective essential requirement in annex I of the MID.

MID Requirement	***Wording***	***Observations***	***Asset***	***Security Property***
1	Allowable errors	These requirements are established to get a correct and reliable measurement result, so the measurement result is the asset. It needs to be protected against changes to keep the conformity of the measuring instrument.	measurement result	integrity
2	Reproducibility			
3	Repeatability			
4	Discrimination and Sensitivity			
5	Durability			
6	A measuring instrument shall be designed to reduce as far as possible the effect of a defect that would lead to an inaccurate measurement result unless the presence of such a defect is obvious.	This is a general requirement that addresses software, parameters, measurement data, inscriptions, indications, and evidence of an intervention, i.e., they need to be protected against defects, e.g., accidental or unintentional changes. See also MID requirement 7.2.	software, parameters, measurement data, inscriptions, evidence of an intervention	integrity, availability[6]

[6] If a defect destroys a measurement result or the software, the presence of the defect would be obvious, and the requirement would be met.

7.1	A measuring instrument shall have no feature likely to facilitate fraudulent use, whereas possibilities for unintentional misuse shall be minimal.	This is a general requirement that addresses software, parameters, measurement data, inscriptions, indication, and evidence of an intervention, they need to be protected so any change (admissible or inadmissible) must generate evidence of an intervention. Securing to avoid unintentional misuse addresses software, parameters, measurement data, inscriptions, indications, and evidence of an intervention.	software, parameters, measurement data, inscriptions, evidence of an intervention	integrity, authenticity
7.2	A measuring instrument shall be suitable for its intended use taking account of the practical working conditions and shall not require unreasonable demands of the user in order to obtain a correct measurement result.	This is a general requirement that addresses software, specifically, the user interfaces. See also MID requirement 6.	software	availability

7.3	The errors of a utility measuring instrument at flows or currents outside the controlled range shall not be unduly biased.	This is dealt with in instrument-specific Guides developed by the WGs 11 and 13. See the *WELMEC website* for the appropriate WELMEC Guide that deals with this subject.	-[7]	-
7.4	Where a measuring instrument is designed for the measurement of values of the measurand that are constant over time, the measuring instrument shall be insensitive to small fluctuations of the value of the measurand or shall take appropriate action.	This is dealt with in instrument-specific Guides. See the *WELMEC website* for the appropriate WELMEC Guide that deals with this subject.	-	-
7.5	A measuring instrument shall be robust, and its materials of construction shall be suitable for the conditions in which it is intended to be used.	This is dealt with in instrument-specific Guides. See the *WELMEC website* for the appropriate WELMEC Guide that deals with this subject.	-	-
7.6	A measuring instrument shall be designed so as to allow the control of the measuring tasks after the instrument has been placed on the market and put into use.	This is a feature of the measuring instrument that addresses all the assets, i.e., it needs to be possible to evaluate whether the assets meet the essential requirements. It is related to requirement 12 of annex I of the MID.	software, parameters, measurement data, inscriptions, evidence of an intervention	-

[7] This concerns protection means that check for correct operational conditions. These means must be present and unchanged. They are interpreted as being part of the software.

If necessary, special equipment or software for this control shall be part of the instrument.	This addresses a module of the software that enables control of the measuring instrument after it has been placed on the market and put into use. This is a protection means, and the module is considered part of the legally relevant software.	software	integrity, availability, authenticity
The test procedure shall be described in the operation manual.	This is related to the required documentation. This means that test procedures, such as remote verification, need to be described in the operation manual.	Software identification is covered by attack vector IIS1 in Guide 7.2, Annex II.	availability, authenticity
When a measuring instrument has associated software which provides other functions besides the measuring function, the software that is critical for the metrological characteristics shall be identifiable	This requirement is related to a measuring instrument that has both legally relevant software modules and legally non-relevant software modules. The LR SW needs to be identifiable. The identifier is considered a part of the software, see also MID requirement 8.3.	Software identification is covered by attack vector IIS1 in Guide 7.2, Annex II	availability, authenticity
and shall not be inadmissibly influenced by the associated software.	This addresses the protection of software. The legally non-relevant software shall not inadmissibly influence the LR SW.	software	integrity, availability, authenticity

8.1	The metrological characteristics of a measuring instrument shall not be influenced in any inadmissible way by the connection to it of another device, by any feature of the connected device itself or by any remote device that communicates with the measuring instrument.	With respect to Guide 7.2, this addresses the protection of the software, parameters, measurement data, inscriptions, indications, and evidence of an intervention against external influence through another device.	software, parameters, measurement data, inscriptions, evidence of an intervention	integrity, availability, authenticity
8.2	A hardware component that is critical for metrological characteristics shall be designed so that it can be secured.	It could be that the legally relevant software, parameters, measurement data, identifications, logbooks, or credentials are stored on a hard disk that needs to be protected. It may be protected by using hardware as well as software seals.	software, parameters, measurement data, inscriptions, evidence of an intervention	integrity, availability, authenticity
	Security measures foreseen shall provide for evidence of an intervention.	The text addresses security/protection means as well as evidence of an intervention.	software, evidence of an intervention	integrity, availability, authenticity
8.3	Software that is critical for metrological characteristics shall be identified as such.	This addresses the software identification. See also MID requirement 7.6.	Software identification is covered by attack vector IIS1 in Guide 7.2, Annex II.	integrity, authenticity
	Software identification shall be easily provided by the measuring instrument.	This addresses the software identification. See also MID requirement 7.6.	Software identification is covered by attack vector IIS1 in Guide 7.2, Annex II.	availability
	Software shall be secured.	The text addresses software and security/protection means.	software	integrity, availability, authenticity

	Evidence of an intervention shall be available for a reasonable period of time.	The text addresses evidence of an intervention (e.g. event counter protocols, audit trails) directly, as well as their capacity.	evidence of an intervention	integrity, availability
8.4	Measurement data, software that is critical for measurement characteristics and metrologically important parameters stored or transmitted shall be adequately protected against accidental or intentional corruption	This addresses the protection of measurement data, software and parameters during storage and transmission which was covered by Extensions L, T and D in WELMEC Guide 7.2:2025.	software, parameters, measurement data	integrity, authenticity, availability
8.5	For utility measuring instruments, the display of the total quantity supplied or the displays from which the total quantity supplied can be derived, whole or partial reference to which is the basis for payment, shall not be able to be reset during use.	This is covered in the instrument-specific annexes of Guide 7.2 because it only applies to utility meters.	measurement data	integrity, availability
9.1	A measuring instrument shall bear certain inscriptions. It is up to the working groups to decide which inscriptions can be shown in the display.	Inscriptions shown in the display are considered an asset because they need to comply with the requirements listed under number 9, see below. Specifically, special attention should be paid to requirement 9.8 with regard to authenticity and integrity.	inscriptions	availability

9.2	An instrument of dimensions too small or of too sensitive a composition to allow it to bear the relevant information shall have its packaging, if any, and the accompanying documents required by the provisions of this Directive suitably marked.	Not software-related.	-	-
9.3	The instrument shall be accompanied by information on its operation unless the simplicity of the measuring instrument makes this unnecessary.	This only has consequences for the documentation.	-	-
9.4	Groups of identical measuring instruments used in the same location or used for utility measurements do not necessarily require individual instruction manuals.	This only has consequences for the instruction manual.	-	-
9.5	The unit of measurement or its symbol shall be shown close to the numerical value.	The unit of measurement is part of the required inscriptions.	inscription	availability
9.6	A material measure shall be marked with a nominal value or a scale, accompanied by the unit of measurement used.	Not software-related.	-	-

9.7	The units of measurement used, and their symbols shall be in accordance with the provisions of Union legislation on units of measurement and their symbols.	The units of measurement are part of the required inscriptions.	inscriptions	availability
9.8	All marks and inscriptions required under any requirement shall be clear, non-erasable, unambiguous, and non-transferable.	The general consensus is that marks need to be put on the measuring instrument or on a data plate of the measuring instrument. However, the WGs may decide that some inscriptions may be displayed.	inscriptions	integrity, availability
10.1	Indication of the result shall be by means of a display or hard copy.	This addresses the indication which is covered by attack vectors in Guide 7.2, Annex II. This addresses a hard copy which is covered under stored measurement data, see also MID requirement 10.3.	evidence of an intervention	availability
10.2	The indication of any result shall be clear and unambiguous	This has to do with the readability of the indications. Guide 7.2 does not specifically deal with this requirement. This is dealt with in instrument-specific Guides. See the *WELMEC website* for the appropriate WELMEC Guide that deals with this subject.	-	-

	and accompanied by such marks and inscriptions necessary to inform the user of the significance of the result.	The inscriptions to inform the user of the significance of the result is considered to be measurement result relevant data and part of the measurement data. This addresses the indications and measurement data.	measurement data	availability
	Easy reading of the presented result shall be permitted under normal conditions of use.	This has to do with the readability of the indications. Guide 7.2 does not specifically deal with this requirement. This is dealt with in instrument-specific Guides. See the *WELMEC website* for the appropriate WELMEC Guide that deals with this subject.		-
	Additional indications may be shown provided they cannot be confused with the metrologically controlled indications.	This has to do with legally relevant indications and legally non-relevant indications.	Is dealt with by relevant attack vectors of Guide 7.2, Annex II.	integrity, authenticity
10.3	In the case of hard copy the print or record shall also be easily legible and non-erasable	Printing is covered by indications. This addresses both indications and stored measurement data. Legibility is not specifically dealt with in Guide 7.2.	measurement data,	availability

10.4	A measuring instrument for direct sales trading transactions shall be designed to present the measurement result to both parties in the transaction when installed as intended.	This is related to the indication of the measurement result. This also addresses measurement data needed to construct the measurement result for indication.	measurement data	availability
	When critical in case of direct sales, any ticket provided to the consumer by an ancillary device not complying with the appropriate requirements of this Directive shall bear appropriate restrictive information.	Guide 7.2 does not specifically deal with this requirement. This is dealt with in instrument-specific Guides. See the *WELMEC website* for the appropriate WELMEC Guide that deals with this subject.	-	-
10.5	Whether or not a measuring instrument intended for utility measurement purposes can be remotely read it shall in any case be fitted with a metrologically controlled display accessible without tools to the consumer. The reading of this display is the measurement result that serves as the basis for the price to pay.	This clause is only valid for gas meters, electricity meters, water meters and heat meters. These are dealt with in instrument-specific Guides. See the *WELMEC website* for the appropriate WELMEC Guide that deals with this subject.	measurement data	availability

11.1	A measuring instrument other than a utility measuring instrument shall record by a durable means the measurement result accompanied by information to identify the particular transaction, when: the measurement is non-repeatable; and the measuring instrument is normally intended for use in the absence of one of the trading parties.	This address measurement data, especially stored measurement data.	measurement data	integrity, availability
11.2	Additionally, a durable proof of the measurement result and the information to identify the transaction shall be available on request at the time the measurement is concluded.	This addresses measurement result and identifying information, esp. when stored in a special, durable form (e.g. as printout or archive file).	measurement data	integrity, availability
12	A measuring instrument shall be designed so as to allow ready evaluation of its conformity with the appropriate requirements of this Directive.	This is related to requirement 7.6. This is a feature of the measuring instrument that applies to all the assets, i.e., that it shall be possible to evaluate if these assets meet the essential requirements. To make evaluation possible, each asset should be protected against changes, should be available, and should be authentic.	software, parameters, measurement data, inscriptions, evidence of an intervention	integrity, availability, authenticity

Table 6: The identified assets and security properties, based on the essential requirements of annex I of the MID.

Annex III. Legally Relevant

Legally relevant: required to fulfill the essential requirements and/or having an impact on the compliance with the essential requirements of the MID, annex I, and the instrument-specific requirements of the MID and/or the essential requirements of the NAWID, annex I and III.

With the definition above, one can determine whether software modules, parameters, data, inscriptions, or other items are legally relevant with regard to the MID and NAWID.

Below, some examples are given demonstrating the application of the definition.

- A measuring instrument put under legal control has to comply with essential requirements, see article 6 of the MID and article 4 of the NAWID, therefore, according to the definition of that term, that measuring instrument is legally relevant.
- Any module or component that is part of the measurement chain between sensor and (primary) indication is legally relevant.
- The markings and inscriptions that have to fulfill the essential requirements are legally relevant according to the definition.
- The protection features used to protect the measuring instrument and assets have to fulfill the essential requirements and are therefore legally relevant.
- Data, whether stored, transmitted, and/or indicated, or used to construct the measurement result have to fulfill the essential requirements and are therefore legally relevant. Legally relevant data are called measurement data in this Guide.
- If a component or module is used to construct, store, retrieve, transmit, and/or receive measurement data and/or evidence of an intervention of a protection measure and/or indicate the measuring result, then that component might influence the measurement result or the protection requirements and therefore have an influence on the compliance with the requirements and is therefore legally relevant.
    - Components to construct the measurement data include, for example, the sensor, analog data processing unit and digital data processing unit.
    - Components to store or transmit measurement data include, for example, a hard disk and network interface card.
    - Components to indicate the measurement results include display and printer.
- Evidence of an intervention generated by a protection means includes, for example, data of an audit trail and event counter.
- Modules used to protect evidence of an intervention or stored measurement data, and modules that are used to check the integrity and authenticity of evidence of an intervention or stored measurement data are considered legally relevant because these have an influence on the compliance with the essential requirements.
- If a module has a function or algorithm that determines or influences the measured quantity value (MQV) and/or has parameters that have an influence on the MQV and/or processes the measurement data needed to construct the MQV, i.e., the intermediate MQV from the sensor, then that module has an influence on the measurement result and thus on the compliance with the essential requirements and is therefore legally relevant.
- If a module or component has functions that use the MQV or that process measurement data, then they might influence the measurement result and thus the conformity with the essential requirements and are therefore legally relevant.

- Parameters that influence the measurement result or the metrological characteristics of the measuring instrument or are necessary to construct the measurement result or are used to give access to certain functionalities or are used as part of a software seal are legally relevant.
    - Examples of parameters that influence the measurement result are calibration parameters (e.g., span adjustment or other adjustments or corrections).
    - Examples of parameters that influence the metrological characteristics of the measuring instrument are configuration parameters (e.g., maximum value, minimum value, unit of measurement, etc.).
    - Examples of parameters that are needed to construct the measurement result are the unique identifier of the data source (identification of the sensor if multiple sensors use a common display) and the time and date settings.
    - Examples of parameters that give access to certain functionality are the parameters that enable/disable the remote verification procedure, or a verified or traced update.
    - Examples of parameters that are part of the software seal are pairing parameters that prevent exchanging components or modules.
- The configurable part of the software that has an influence on the legally relevant measurement process or the protection means is legally relevant.
- Any software modules with other functions that cannot influence compliance with the essential requirements are legally non-relevant.

Annex IV. Conformity Assessment and Functional Design-Specific Requirements (informative)

This annex only covers functional requirements that may be considered by the WGs. They shall be used in conjunction with Guide 7.2 regarding the protection of software-controlled measuring instruments or components.

1. Conformity Assessment

Regarding the documentation of the protection means against inadmissible influence on the assets, see WELMEC Guide 7.2.

CA1 Information for verification

CA1.1 Information necessary for verification shall be provided by the measuring instrument to the verifier and, if applicable, to the remote verification software.

Note 1: This could include a test element that enables tests to be carried out in a reasonable time, for example by accelerating time-consuming test procedures for gas meters.

Note 2: This could include the measured quantity value with a scale interval smaller than the verification scale interval, parameters, evidence of an intervention, checksum values, software identification, or the result of checking and durability protection facilities.

Note 3: This could also include records of events, records of evidence of an intervention, etc.

Note 4: Access to this information might be restricted, e.g., if it influences compliance with other requirements, such as:

- requirements on battery life,
- on resources, or
- delays in the measurement process.

CA1.2 If separate modules are present, a filled-in form for the compatibility checks as specified in the instrument-specific WELMEC Guides, harmonized standards or normative documents, together with the data that is used to fill in the form, shall be made available by the manufacturer for a conformity assessment procedure in accordance with module B, module D or module F.

CA2 Information to be included in the certificate

CA2.1 Regarding software-controlled measuring instruments or components, at least the following information shall be included in the certificate:

- general description of the LR functions of the software;
- the risk class for the LR software;
- software identification of all approved software versions;
- method to display the current software identification on the approved measuring instrument in use;
- protection means as well as means to provide evidence of an intervention and the method to check them (e.g. hardware seals, event counters, audit trails, see WELMEC Guide 7.2);

- software modules under legal control, including whether or not the measuring instrument is equipped with a remote verification procedure or a traced update procedure;
- if applicable:
  - means of integrity protection checking;
  - software operating environment;
  - test items with their unique identification used for the remote verification procedure.
- Short description of the software environment:
  - software operating environment necessary to operate the software (e.g., operating system);
  - modules under legal control (if software separation is implemented);
  - hardware and software interfaces (e.g., infrared, Bluetooth, wireless LAN…);
  - components and their locations in the measuring instrument including its protection, if needed, see also WELMEC Guide 7.2.
- Short description of the legally relevant design functions, e.g., storage and/or transmission.
- If remote verification is supported:
  - which information is made available and in what manner;
  - a description of the remote verification procedure for accessing/reading remote verification data and for executing remote verification procedures with an explanation of how a certain test item can be used to evaluate whether a certain requirement is fulfilled;
  - description of the access rights to the measuring instrument for remote verification and a description of how test items can be obtained (and made available to relevant authorities depending on national legislation).

2. Functional Requirements

FR1 Deletion of the measurement result

Note: Unless otherwise specified, it is assumed that measurement data will be stored indefinitely.

FR1.1 For measuring instruments other than utility meters, the measurement result may be deleted if

- the transaction is settled, or
- these data are printed by a printing device subject to legal control or transmitted to the other party involved in the transaction.

FR1.2 For utility measuring instruments, the display of the total quantity supplied or the displays from which the total quantity supplied can be derived, and which form the basis for payment in whole or in part, shall not be able to be reset during use.

Note: Cumulative registers of a measuring instrument shall be reset prior to applicable conformity assessment procedures. For a conformity assessment procedure in accordance with annex D, F or H1, the utility meter is fitted with all protection means by the manufacturer as specified in the type examination certificate. After the assessment procedure, it is not possible to reset the cumulative measurement data without evidence of an intervention being generated. See also WELMEC Guide 7.2.

FR2 Deletion of evidence of an intervention

Note: Unless otherwise specified, it is assumed that evidence of an intervention will be stored indefinitely.

FR2.1 Evidence of an intervention shall be available for a certain period of time, defined by the WGs.

Note 1: This could be related to verification periods or other considerations.

Note 2: Regarding the indication of evidence of an intervention, see R2.2 and R2.4 in WELMEC Guide 7.2.

3. Design-specific Requirements

The instrument-specific requirements of the MID, WELMEC Guides, normative documents, or harmonized standards may require specific design facilities, such as checking facilities, time stamps or automatic storage.

In any case, the manufacturer can provide these functions even if they are not mandatory. This also includes the voluntary designs of software separation, software updates and dynamic modules.

However, if these specific designs are implemented, they have to fulfill certain requirements.

DR1 Diagnostics and fault recovery

DR1.1 General diagnostics and fault recovery requirements

DR1.1.1 For remote verification, the use of diagnostics, detection of significant defects and durability protection are required, and the data containing the results shall be made available to the remote verification software.

DR1.1.2 Regarding the automatic storage of these events, see *DR4*.

DR1.1.3 If the manufacturer of a measuring instrument implements detection functions for significant defects and/or durability protection, he shall implement checking facilities into the software modules or hardware components or provide means by which the hardware components can be supported by the software modules of the measuring instrument.

DR1.2 Detection of significant defects

DR1.2.1 If software is involved in the detection of significant defects, it shall carry out the relevant checks in the required timeframe and appropriately act upon any detected defect.

Note: The WGs need to decide on the timeframe and what reaction is appropriate in this context.

DR1.2.2 The documentation to be submitted for type examination shall contain a list of the significant defects that will be detected by the software, information about the timeframe in which a check is carried out, how the software will act upon these defects and, if needed for understanding its operation, a description of the detecting algorithm.

Note 1: This could include the detection of available energy in a battery, e.g., if the available energy in a battery is below 90%, a warning is shown.

Note 2: This could include detecting when a measuring instrument is outside the specific field of measurement specified by the manufacturer for parameters that are relevant for measurement accuracy, and taking appropriate action if this is the case.

Examples:

1) The documentation shall show the power source capacity, maximum lifetime (regardless of energy consumption), means to determine the energy consumed or available, description of how a low battery warning is provided and of the battery exchange process. If the power source can be changed in the field, parameters and measurement data shall not be corrupted during the exchange.

2) A volume conversion device shall stop integrating the converted quantity and may totalize separately the converted quantity for the time it is operating outside the operating range(s).

DR1.3 Durability protection

DR1.3.1 If software is involved in durability protection, it shall carry out the relevant checks in the required timeframe and appropriately act upon any detected durability error.

DR1.3.2 The documentation to be submitted for type examination shall contain a list of the durability errors that will be detected by the software, information about the timeframe in which a check is carried out, how the software will act upon detected errors and, if needed for understanding its operation, a description of the detecting algorithm.

DR1.4 Back-up facilities

DR1.4.1 For non-repeatable measurements, the measuring system shall be equipped with a backup power source to ensure that all measuring functions are carried out even if the main power supply fails, or it shall be equipped with a backup facility to store and display the data so that the ongoing transaction can be terminated.

DR1.4.2 For non-repeatable measurements, there shall be a facility that provides for periodic back-up of measurement data, such as measurement values and the current status of the process, to prevent loss of data in the event of a significant defect.

DR1.4.3 The minimum interval for the back-up shall ensure that the critical change value is not exceeded.

DR1.4.4 This data shall be stored in a non-volatile storage.

DR1.4.5 The documentation shall contain a description of which data is backed-up, the time interval for the back-ups, and the calculation of the minimum interval for the back-up to ensure that the critical change value is not exceeded.

DR1.5 Fault recovery

DR1.5.1 The software shall automatically recover from a disturbance to normal processing.

DR1.5.2 The fault recovery facilities shall include appropriate wake-up facilities so that the measuring instrument, including its software, does not get into an indefinite state.

DR1.5.3 If the back-up facility is used for fault recovery, the minimum interval for the back-up shall be defined to ensure the critical change value is not exceeded.

DR2 Time stamps

DR2.1 If a measuring instrument uses timestamps, it shall contain an internal clock that shall be used to create the timestamp.

DR2.2 Time stamps are mandatory if an audit trail is used or if they are part of the measurement result relevant data, e.g., to determine tariffs or fines based on a time slot or, together with the date, to provide traceability to the transaction. In

that case, the timestamp shall be read from the clock of the measuring instrument.

DR2.3 The timestamp shall be in a consistent format, allowing for easy comparison of two timestamps and tracking progress over time.

DR2.4 Depending on the kind of measuring instrument or on the field of application, setting the clock may be legally relevant and appropriate protection means shall be taken in accordance with the risk level to be applied (see WELMEC Guide 7.2).

DR2.5 Automatic setting of the time shall only be possible if legal time according to national regulations is used as a time base in an authenticated manner. If an internal clock is synchronized with legal time, the synchronization method and traceability to legal time shall be described.

DR3 Completeness of measurement data

DR3.1 Measurement data shall include all relevant data necessary for the legally relevant purpose.

Note 1: In the event of an irregularity, the measurement data is not to be used for further legally relevant purposes. They need to be registered as invalid. This register is considered measurement result relevant data.

Note 2: If multiple sensors contribute data to the measurement data, the measurement data contains an identification of the respective sensors.

DR3.2 The following shall be considered:

- The measurement result contains all measurement result relevant data to enable the examination of the correctness of and traceability to the transaction.
  - For non-repeatable measurements, the identification of the measuring instrument shall be included in the measurement result relevant data.
  - For durable proof, the invoice shall state where the measurement result is located, for example on which data storage device, website (web storage), or printout.
- Measurement data used for the construction of the measurement result contains all measurement result relevant data.
- If a checking facility is used for the detection of significant defects or for durability protection, the evidence of an intervention contains the nature of the failures or significant defects and, for remote verification, a time stamp.
- If dynamic modules are present, the measurement data contains information regarding the use of these modules in the measurement process.
- If assets are protected in such a way that changes lead to evidence of an intervention, the evidence of an intervention contains sufficient information:
  - For an event counter:
    - a non-resettable counter that increments each time an event occurs to provide evidence of an intervention for each parameter change;
    - the value of the event counter after (subsequent) verification shall be marked on the measuring instrument.

- For audit trails:
  - In all cases:
    - a time stamp of the event with the date and time of the event.
  - In addition:
    - In the event of a software update:
      - if permission of the user or owner is required, the identification of the operator that initiated the update procedure;
      - success/failure of the update procedure;
      - software identification of the installed version, including the number of the TEC;
      - software identification of the previously installed version;
      - identification of the uploading party, i.e., the source of the update.
    - In the event of a parameter change:
      - identification of the changed parameter;
      - the old and new value of the changed parameter;
      - the source of the parameter change, e.g., for dynamic modules (e.g., the learning facility) or instrument-specific requirements.
    - In the event of inadmissible influence on an asset:
      - the asset involved.

DR3.3 Measurement results shall be presented on demand when required to finalize the transaction or to facilitate verification or inspection.

DR4 Automatic storage

DR4.1 Evidence of an intervention shall be stored automatically.

DR4.2 If storage of the measurement result is required, measurement results shall be stored automatically.

Note: If a decision is required from the operator whether or not to accept a measurement result, the measurement data needs to be stored automatically upon acceptance.

DR4.3 When the data necessary for the calculation of the measurement result are relevant for legal purposes, all measurement result relevant data included in the calculation shall be automatically stored with the final value.

DR4.4 A checking facility shall check the availability and the capacity of the storage.

DR4.5 The information on the capacity of the storage shall be made available.

DR4.6 If the storage is not available or full, an appropriate response is required.

Note: The WGs need to decide which response is required.

DR4.7 If data storage is mandatory, no measurement shall be possible if the storage device is not available.

DR4.8 There shall be sufficient memory storage for the intended application.

Note: The WGs shall decide which action shall be taken if the memory limit is reached, e.g., disabling further measurements or deleting the oldest evidence of an intervention.

DR4.9 See *FR1* for the conditions under which the measurement result may be deleted.

DR5 Dynamic modules

DR5.1 Where measuring instruments or systems incorporate or are dependent upon dynamic modules of legally relevant software, this information shall be indicated and made available to all parties interested in the measurement result(s) produced by that measuring instrument or system.

DR5.2 Where a measurement result is the product of a measurement process that incorporates or is dependent upon dynamic modules of legally relevant software, the indication of the measurement result shall include information regarding the use of those modules in the measurement process. This may be achieved by using a short statement, clearly understood markings, symbols or other indications.

DR6 Remote verification

DR6.1 General requirements for remote verification

Note: Depending on national legislation, remote verification may be possible even for devices that are not on site.

DR6.1.1 If the measuring instrument facilitates remote verification, there shall be a description of the remote verification procedure, how to access and read the remote verification data and how to execute remote verification procedures.

DR6.1.2 Access rights to the measuring instrument for remote verification shall be described in the documentation and made available to the relevant authorities depending on national legislation.

DR6.1.3 If not in compliance with national legislation, the manufacturer shall disable the remote verification functionality.

DR6.1.4 The modules involved in the remote verification are part of the legally relevant software and shall fulfill the relevant requirements.

DR6.2 Required functionality for remote verification

DR6.2.1 The remote verification procedure shall meet the following requirements:

- It shall always be possible to establish the integrity of the measuring instrument to be verified. When checking software integrity, the integrity measure (checksum, hash) shall be calculated immediately before it is transmitted to the remote verification software.
- It shall always be possible to establish the authenticity of the measuring instrument, i.e., the measuring instrument shall be uniquely identified and other means shall be provided to ensure authenticity.
- For remote verification, the measuring instrument shall
  - use timestamps,
  - provide evidence of an intervention regarding software, parameters, and stored measurement data by means of an audit trail,
  - have a facility for detection of significant defects and faults,
  - store logging data, events, audit trails, and
  - make these available for remote verification purposes.

- Relevant test items identified by the WGs shall be available depending on the specific requirement to be tested and the measuring instrument type (e.g. type approval number, serial number, legally relevant parameters, verification information and status, software version identification, software integrity, audit trails, change logs, event logs, etc.).
- Test items shall be uniquely identified. The test items obtained shall be unambiguously linked to the measuring instrument to be verified.
- There shall be a legally relevant interface for data extraction for remote verification purposes. Interfaces for remote verification shall be protected.
- Provisions shall be made to securely store the result of the remote verification in the measuring instrument. These data shall be protected. Securing means shall ensure that only the remote verification software has write permissions.

DR6.2.2 Access to the verification procedures, specific test items or commands shall be available but can be restricted if these influence the compliance with other requirements, such as:

- requirements on battery life,
- on resources or
- delays in the measurement process.

DR6.2.3 The result of the remote verification shall contain, at least, a unique ID (at least identifying the verification authority) and the date of the verification.

Note 1: Depending on the measuring instrument type or the application, additional data could be required by national legislation.

Note 2: The recognition of a verification mark and the data it contains are subject to national requirements.

DR6.2.4 In the event of a non-compliance, it shall be possible to take appropriate action.

Note: National legislation needs to be consulted for information about what an appropriate action is in the event of a non-compliance, e.g., a displayed warning that the measuring instrument shall not be used for legal purposes or a disqualification mark.

Annex V. Main Differences between Recast and Guide 7.2: 2025

The approach used in the recast Guide 7.2 may seem comparable to the use of extensions in Guide 7.2: 2025, however, special care has to be taken, for example:

- Guide 7.2: 2025 limits the application of extension L to long term storage of measurement data. This limitation has been removed in the recast Guide 7.2 to address the storage of other assets, such as software, parameters, logs, events, but also the storage of measurement data in components used to construct the measurement result. Therefore, stored assets are instances of the overall identified assets and must be adequately protected.
- Guide 7.2: 2025 limits the application of extension T to measurement data and parameters. Comparable to stored measurement data, this limitation has been removed in the recast Guide 7.2, considering that, for example, parameters might also be transmitted from one component to another. Therefore, transmitted assets are instances of the overall identified assets and must be adequately protected.
- In subchapter 4.1, Guide 7.2: 2025 specifies that the requirements for extension O do not apply if the operating system fulfills certain conditions. With the recast of Guide 7.2, this exception no longer applies. Inadmissible influence through the OS shall always be prevented.
  However, a possible solution might be that the OS (or subsystems) is setup and configured in accordance with the conditions mentioned in subchapter 4.1 in Guide 7.2: 2025, e.g., it is ensured that all communication is under control of the legally relevant software, the OS does not allow loading or changing modules, parameters, data or running programs, the OS does not allow to change the environment of the legally relevant application. This includes that the access prevention shall be preset and not the result of a respective subsequent configuration of these subsystems. In that case, those attack vectors addressing inadmissible influence through the operating system do not need to be examined further by the examiner. Only proper implementation of the solution has to be checked.
- In the recast version of Guide 7.2, modifications of user-changeable legally relevant parameters are now required to produce evidence of an intervention.