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

WELMEC Guide 7.2

Software Guide

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

Software Guide

Contents

FOREWORD

The Guide in hand implements the core requirements applicable to software-equipped measuring instruments based on the essential requirements of the Measuring Instruments Directive (MID) [1] and Non-Automatic Weighing Instrument Directive (NAWID) [2]. See WELMEC Guide 7.1 for additional information.

This Guide gives requirements for measuring instruments, sub-assemblies, components, and software modules with regard to protection. It also provides examination guidance on how compliance with these requirements can be checked.

Although the Guide is oriented on measuring instruments included in the regulations of the MID and the Non-Automatic Weighing Instrument Directive (NAWID), the requirements are of a general nature and may be applied beyond, e.g., to measuring instruments under national regulation.

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

ADC	analog-to-digital converter
AVx	attack vector x
AVx/Fy	functional check y for attack vector x
AVx/Ny	specifying note y for attack vector x
EUT	equipment under test
EVCD	electric volume conversion device
GC	gas chromatograph
IIA1	inadmissible influence via the administration of the operating system
IIA2	inadmissible influence due to accidental modifications
IIB1	inadmissible influence via the boot process
IIC1	inadmissible influence by obtaining confidential information
IID1	inadmissible influence by downloading legally relevant software
III1	inadmissible influence via user interfaces
III2	inadmissible influence via hardware interfaces
IIN1	inadmissible influence via legally non-relevant software
IIP1	inadmissible influence on the measurement process by executing other functions
IIR1	inadmissible influence by replacing physical parts within the measuring instrument
IIR2	inadmissible influence by replacing or removing complete components
IIS1	inadmissible influence by incorrect software identification
IIT1	inadmissible influence by man-in-the-middle attacks
LNR	legally non-relevant
LR SW	legally relevant software
MID	Measuring Instruments Directive
MPE	maximum permissible error
NAWID	Non-Automatic Weighing Instruments Directive
OS	operating system
Rx	core requirement x
Rx/Ay	risk assessment examination guidance y for core requirement x
Rx/Dy	required documentation y for core requirement x
Rx/Fy	functional check y for core requirement x
Rx/Ny	specifying note y for core requirement x
Rx/Sy	check y based on the source code for core requirement x
Rx/Cy	check y based on the documentation for core requirement x
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.

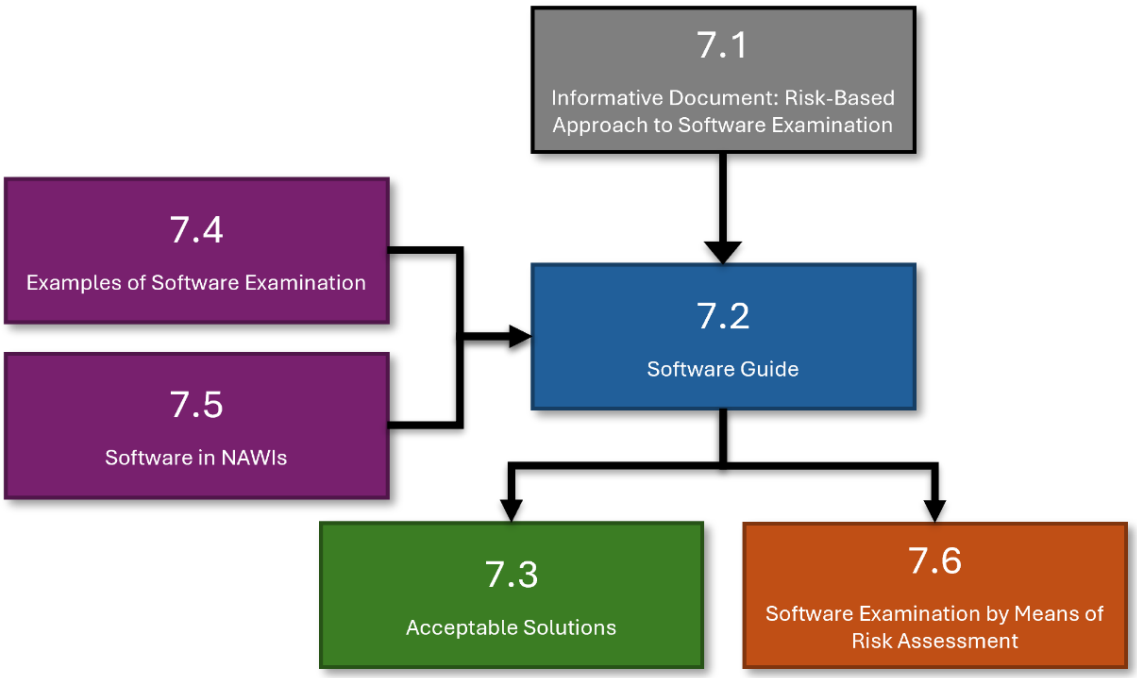

Figure 1: Relationship between the WELMEC Software Guides

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.

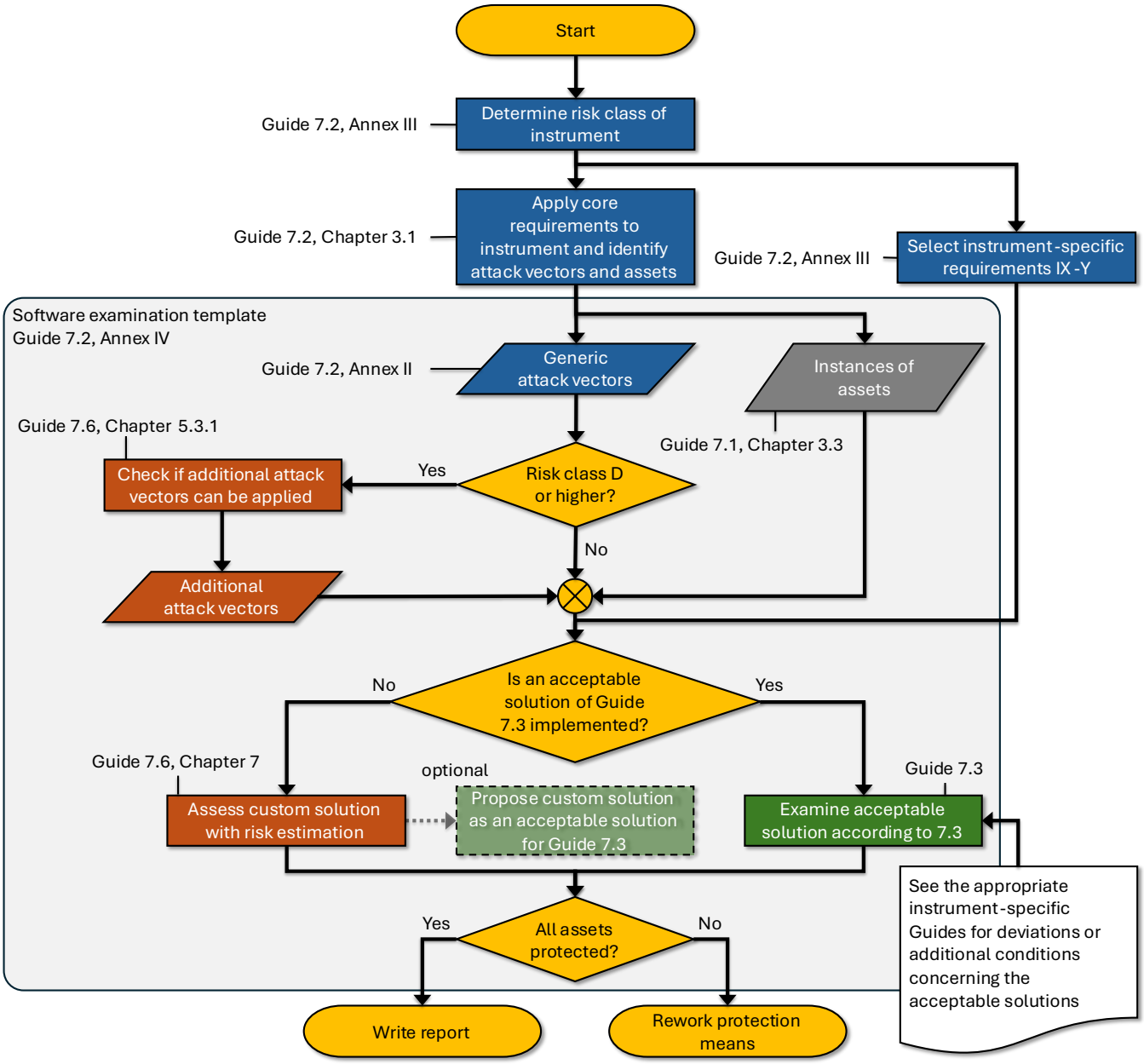

Figure 2: Workflow of the examination of the requirements using Guides 7.1, 7.2, 7.3, 7.6, and instrument-specific Guides (see the WELMEC website).

3 Core Requirements

3.1 R: Protection of Assets

Risk Class B	Risk Class C	Risk Class D	Risk Class E

R1 All assets (software, parameters, measurement data, measurement result, evidence of an intervention, and inscriptions)[1] in the measuring instrument shall be adequately protected to ensure their integrity, authenticity and availability.

R2 If assets are protected in such a way that any change leads to evidence of an intervention, then:

- R2.1 the evidence of an intervention shall contain sufficient information, and
- R2.2 shall be provided by the measuring instrument in a comprehensible manner for a reasonable period of time, and
- R2.3 checks shall be periodically carried out to ensure that no changes have occurred and, if the check fails, further appropriate action shall be taken, and
- R2.4 if a change has occurred in the software or parameters and that change is not expressly admissible (taking into account R3), inscriptions shall be marked as invalid or be deleted, indications of the measuring instrument shall be deactivated and measurement results shall either be marked as invalid or evidence of an intervention shall be provided indicating invalidity of measurement results.

R3 If a change to an asset is not intended to cause a subsequent verification, the resulting evidence of an intervention shall include appropriate information.

- R3.1 If parameters are changed, the evidence of an intervention shall at least include a time stamp and the identification of those parameters.
- R3.2 If the software is changed, the evidence of an intervention shall at least include a time stamp, the identification of the changed software prior to and after the change, and, if available, the source of the new software.

Specifying Notes

R1/N1 This includes all instances[2] of all assets, i.e., all assets in all components of the measuring instrument and during transmission.

R1/N2 Adequate protection against changes and inadmissible influence also means that the security and protection means cannot be bypassed, falsified, or otherwise manipulated.

[1] See WELMEC Guide 7.1, chapter 3.1.

[2] For an explanation of what an instance of an asset is, see WELMEC Guide 7.1, chapter 3.3.

R1/N3	Changes include accidental, unintentional, and intentional modification, substitution and deletion as expressed in the security properties integrity, authenticity and availability (see Guide 7.1). See also the generic attack vectors in Annex II, which express the most common inadmissible changes to assets. *Note 1:* Examples of accidental changes caused by physical effects are electromagnetic interference, temperature and vibration. Since such effects are typically dealt with by all currently used technological solutions, they are generally not subject to additional examination here. *Note 2:* An example of an unintentional change is the deletion of outdated stored datasets without prior confirmation. An example of an intentional modification is the manipulation of assets by an attacker.
R1/N4	If the measuring instrument is in risk class D[3] or higher, additional attack vectors in accordance with Guide 7.6, chapter 5.3.1, are to be considered.
R1/N5	Protection can be demonstrated either by means of an acceptable solution from Guide 7.3 or by means of a risk assessment in accordance with Guide 7.6.
R1/N6	The security property confidentiality is only required for secrets used to ensure these security properties, and is covered by **IIC1** in Annex II.
R2.1/N1	The information the evidence of an intervention shall contain can be found in the relevant documents.
R2.2/N1	How the evidence of an intervention shall be presented can be found in the relevant documents.
R2.2/N2	Information on the reasonable period of time within which the evidence of an intervention shall be available can be found in the relevant documents.
R2.2/N3	Whether a rolling log is acceptable, which reaction is acceptable when a log is full, etc. can be found in the relevant documents.
R2.3/N1	For hardware seals, it is the responsibility of the user to periodically perform a visual check to ensure that the seal is not broken. If the seal is broken, national legislation might require action, e.g., a subsequent verification.
R2.3/N2	How often the checks shall be performed, and what is considered an appropriate action if software means are used for protection can be found in the relevant documents.
R3.1/N1	If parameters require setting by the user, information regarding these parameters and any additional information required to be part of the evidence of an intervention can be found in the relevant documents.
R3.1/N2	If certain parameters require setting by the user, e.g., a parameter change is not intended to cause a subsequent verification, the resulting evidence of an intervention shall include at least the time stamp, the identification of the parameter that has been altered and, if required, any other information.

[3] For an explanation of risk classes, see WELMEC Guide 7.1, chapter 5.2.

Required Documentation

R1/D1	A general description of the measuring instrument and its intended operation, including but not limited to measuring instrument class, main measurement purpose, a list of all legally relevant functions, components, and software modules, a list of all assets and their instances in components or during transmission, a description of operating systems, libraries, interfaces.
R1/D2	The means that protect all instances of the assets against the generic attack vectors, see *Annex II*.
R1/D3	If the measuring instrument is in risk class D or higher, a risk assessment of additional attack vectors in accordance with Guide 7.6.
R1/D4	If an acceptable solution is applied: information as described in Guide 7.3 or a harmonized standard or normative document. Reference to the document and clause/chapter number shall be included.
R1/D5	If no acceptable solution is applied: an adequate analysis and assessment of the risks in accordance with Guide 7.6.
-	R1/D6 The source code of the measuring instrument
R2/D1	A description of the means implemented to provide evidence of an intervention, e.g., what kind of information and how this information is provided and for how long.
R2/D2	A description of the functionality of the checking facility, e.g., how often it will check, how it will act if the check fails, and a description of the detecting algorithm.
R2/D3	If access to the assets is secured, a description of the securing mechanism and how the assets can be accessed for functional testing.
-	R2/D4 The source code of the checking facility
R3/D1	A list of the parameters that can be set by the user and a description of the means implemented to secure and protect them.

Examination Guidance

Checks based on the documentation

R1/C1	Check that all instances of all assets are covered by the documentation, see also *Annex IV*.
R1/C2	Check that all assets have been protected.
R1/C3	Check that the documentation includes all information relevant for the software examination process.

R1/C4 Check that the documentation includes threats beyond the generic attack vectors mentioned in *Annex II* when the measuring instrument is in risk class D or higher.

R1/C5 If an acceptable solution is applied, check that the documentation contains the information required by the relevant documents, and that references to the relevant documents and clause/chapter numbers are included as well as the information required by Guide 7.3.

R1/C6 Check that the documentation provides all information relevant for the examination intelligibly, i.e., pages are numbered, documents are versioned, text is subdivided into chapters, and in a way that security and protection of all assets can be examined.

R2.1/C1 Check that the evidence of an intervention contains sufficient information.

R2.2/C1 Check that the evidence of an intervention is provided in a comprehensible manner for the longest expected period between at least two inspections/successive verifications of the measuring instrument in the field.

R2.3/C1 If software is used for protection, check that the checking facility periodically checks that no changes have occurred.

R2.3/C2 Check that the action taken by the checking facility in the event of a failed check is appropriate.

R2.4/C1 Check that when software or parameters are changed, evidence of an intervention is always provided.

R3.1/C1 Check that the evidence of an intervention for parameters that may be set by the user includes at least the time stamp, the identification of the parameter that has been altered, and any other information required by the relevant documents.

R3.2/C1 Check that the evidence of an intervention at least includes a time stamp, the identification of the changed software prior to and after the change, and, if applicable, the source of the new software.

Functional Checks

R1/F1 See the risk assessment procedure described in Guide 7.6.

R2/F1 Try to make changes to an asset by using the credentials in R2/D3 and, if changes can be made, check that

R2.1/F1 the evidence of an intervention contains sufficient information,

R2.2/F1 the evidence of an intervention is provided by the measuring instrument in a comprehensible manner for a reasonable period of time,

R2.3/F1 the action conforms with the documentation, and

R2.4/F1 the instrument reacts appropriately or provides evidence of an intervention as described in R2.4.

R3/F1 Change the parameters that require setting by the user and are not intended to cause a subsequent verification, and check that the evidence of

an intervention contains at least a time stamp, the identification of the parameters that have been altered, and the information required by the relevant documents.

Risk Assessment Examination Guidance

R1/A1 For an acceptable solution, Guide 7.3 shall be used to examine the correct implementation and to check that the acceptable solution meets the requirements.

R1/A2 If no acceptable solution is used, Guide 7.6 shall be used to assess the correct implementation of the protection means and to check that they are adequate.

Checks based on the source code

-	R1/S1 Check that means taken for detection of changes are implemented correctly.
	R1/S2 Check that the assets are completely covered by the protection means.

4 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.

Annex I. Checklist

Checklist of the core requirements in

R: Protection of Assets.

If the examination is executed in accordance with Guides 7.6 and 7.3 and their corresponding checklists or templates are used, it can be assumed that all core requirements are fulfilled.

Unless specified otherwise, a documentation check is performed for the different requirements as specified in this Guide.

Item	Guide(s) used for testing	Checks	Passed	Failed	Not applicable	Remarks
R1/D1		Does the documentation contain a general description of the measuring instrument and its intended operation, including but not limited to measuring instrument class, main measurement purpose?				
R1/D1		Does the documentation contain a list of all legally relevant functions, components, and software modules?				
R1/D1		Does the documentation contain a list of all assets and their instances in components or during transmission?				
R1/D1		Does the documentation contain a description of operating systems, libraries, interfaces?				
R1/D2		Does the documentation contain a list of all applied protection means per asset against generic attack vectors, if applicable?				
R1/D3		If the measuring instrument is in risk class D or higher, does the documentation contain a list of additional attack vectors that				

Item	Guide(s) used for testing		Checks	Passed	Failed	Not applicable	Remarks
			have been taken into account beyond the generic attack vectors covered in Guide 7.2, Annex II?				
R1/D4			If an acceptable solution is applied, does the documentation contain: • the information as required by Guide 7.3 or • the information as required by a harmonized standard or normative document?				
R1/D5			If no acceptable solution is applied, does the documentation contain an adequate analysis and assessment of the risks in accordance with Guide 7.6?				
R1/D6			Does the documentation contain the source code of the measuring instrument?				
R1	7.3	7.6	Are all assets protected against using system resources for other functions of the measuring instrument to ensure their availability? Is this adequate?				The typical assets and their instances are listed in Guide 7.1, chapter 3. If new technology is used, additional assets or instances can be included. This check addresses Annex II IIP1.

Item	Guide(s) used for testing		Checks	Passed	Failed	Not applicable	Remarks
R1	7.3	7.6	Are all assets, in particular the legally relevant software, including the operating system, protected against influence via the user interfaces to keep their integrity, authenticity and availability? Is this adequate?				This check addresses Annex II III1.
R1	7.3	7.6	Are all assets protected against influence via the user interfaces during establishment of the environment for the assets to keep their integrity, authenticity and availability? Is this adequate?				This check addresses Annex II IIB1.
R1	7.3	7.6	Are all assets protected against influence via the boot process to keep their integrity, authenticity and availability? Is this adequate?				This check addresses Annex II IIB1.
R1	7.3	7.6	For risk classes D and E, are all individual modules involved in the boot process up to the legally relevant application protected against influence to keep their integrity, authenticity and availability? Is this adequate?				This check addresses Annex II IIB1.
R1	7.3	7.6	Are all assets protected against influence via the user interfaces by using the operating system to keep their integrity, authenticity and availability? Is this adequate?				This check addresses Annex II IIA1.
R1	7.3	7.6	Are all assets protected against influence by executing functions of the legally non-relevant software to keep their integrity, authenticity and availability? Is this adequate?				This check addresses Annex II IIN1.

Item	Guide(s) used for testing		Checks	Passed	Failed	Not applicable	Remarks
R1	7.3	7.6	Are all assets protected against influence via functionalities of the legally non-relevant software to keep their integrity, authenticity and availability? Is this adequate?				This check addresses Annex II IIN1.
R1	7.3	7.6	Are all assets protected against influence by obtaining confidential information to keep their authenticity? Is this adequate?				This check addresses Annex II IIC1.
R1	7.3	7.6	Are all assets protected against introducing fake confidential information to keep their authenticity? Is this adequate?				This check addresses Annex II IIC1.
R1	7.3	7.6	Are all assets protected against influence by replacing physical parts within the complete measuring instrument or within a component to keep their integrity, authenticity and availability? Is this adequate?				This check addresses Annex II IIR1.
R1	7.3	7.6	Are all assets protected against influence via hardware interfaces by connecting legally non-relevant devices to the measuring instrument to keep their integrity, authenticity and availability? Is this adequate?				This check addresses Annex II III2.
R1	7.3	7.6	Are all assets protected against influence by downloading legally relevant software to keep their integrity, authenticity and availability? Is this adequate?				This check addresses Annex II IID1.

Item	Guide(s) used for testing		Checks	Passed	Failed	Not applicable	Remarks
R1	7.3	7.6	Are all assets protected against influence via replacement of complete components to keep their integrity, authenticity and availability? Is this adequate?				This includes replacing NLR sensors. This also includes using the output of a LR component, for example to spoof as LR indication. This check addresses Annex II IIR2.
R1	7.3	7.6	Are all assets protected against influence through removal of complete components to keep their integrity, authenticity and availability? Is this adequate?				This check addresses Annex II IIR2.
R1	7.3	7.6	Are all assets protected against influence during transmission within the measuring instrument to keep their integrity, authenticity and availability? Is this adequate?				This check addresses Annex II IIT1.
R1	7.3	7.6	Are all assets protected against influence due to accidental modification to keep their integrity, authenticity and availability? Is this adequate?				This check addresses Annex II IIA2.
R1	7.3	7.6	Is the software protected against influence through the use of an ambiguous or no software identification to keep its integrity, authenticity and availability? Is this adequate?				This check addresses Annex II IIS1.

Item	Guide(s) used for testing		Checks	Passed	Failed	Not applicable	Remarks
R1	7.3	7.6	Is the software protected against influence through the use of an identical software identifier for different versions of the same software to keep its integrity, authenticity and availability? Is this adequate?				This check addresses Annex II IIS1.
R1	7.6		For measuring instruments of risk class D or higher: Are the additional attack vectors assessed in accordance with Guide 7.6?				Please note in a separate sheet which additional attack vectors have been used, see Guide 7.6.
R2/D1			Does the documentation describe the means to provide evidence of an intervention, e.g., what kind of information and how this information is provided and for how long? Is this adequate?				
R2/D2			Does the documentation describe the functionality of the checking facility, e.g., how often it will check, how it will act if the check fails, and a description of the detecting algorithm? Is this adequate?				
R2/D3			If access to the assets is secured, does the documentation describe the securing mechanism and how the assets can be accessed for functional testing?				

Item	Guide(s) used for testing	Checks	Passed	Failed	Not applicable	Remarks
R3.1		If a parameter change is not intended to cause a subsequent verification, does the resulting evidence of an intervention contain at least a time stamp and the identification of the changed parameters?				
R3.2		If a software change is not intended to cause a subsequent verification, does the resulting evidence of an intervention contain at least a time stamp and the identification of the software prior to and after the change, and, if available, the source of the new software?				
R3/D1		Does the documentation list all parameters that can be set by the user?				
R3/D1		Does the documentation describe the means to secure and protect parameters that can be set by the user? Is this adequate?				

Annex II. Generic Attack Vectors

This annex lists generic attack vectors that are mirrored by corresponding acceptable solutions in chapter 4 of Guide 7.3.

The device to be assessed can either be a complete measuring instrument or a component (which can be tested separately). The examination focuses on attacks from both inside the measuring instrument and from outside.

All attack vectors are realizations of the threats foreseen by the essential requirements of annex I of the MID, e.g., intentional manipulation in essential requirement 8.4.

1. Inadmissible influence on assets via software or physical parts within the measuring instrument

1.1. IIP1: Inadmissible influence on the measurement process by executing other functions

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1	An attacker inadmissibly influences the assets and their security properties by using system resources for other functions of the measuring instrument.		
Specifying Notes			
AV1/N1	This covers functions of the legally relevant software (including the operating system).		
AV1/N2	Other functions of the measuring instrument are, for example: checking, durability and backup facilities, protection means, software updates and remote verifications.		
AV1/N3	Other functions of the operating system are, for example: cleaning-up storage, updating the operating system, or defragmenting.		
AV1/N4	This implies that there are enough resources for the operation of the legally relevant software.		
AV1/N5	The legally non-relevant software may influence the security property availability via resource consumption, but typically not integrity or authenticity.		
AV1/N6	This applies to all assets whether stored, processed or indicated, etc.		
Functional Checks			
AV1/F1	Try to access functions, e.g., from the user interfaces, that can indirectly influence the measurement process or have a negative impact on storage capacity, battery life or resources for the operation of the legally relevant software, and check that the assets are protected.		
AV1/F2	Perform spot checks by sequentially initiating several functions of the measuring instrument and check each function to ensure that it does not inadmissibly influence the measurement process, e.g., if a measurement can be performed, the result has to be within the MPE or critical change value.		

AV1/F3	Initiate several functions of the legally relevant software, including the operating system, so that they run simultaneously and check that there is no inadmissible influence on the measurement process, e.g., if a measurement can be performed, the result has to be within the MPE or critical change value.
Keywords	
Assets:	software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions
Security properties: availability	

1.2. III1: Inadmissible influence via user interfaces

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1	An attacker inadmissibly influences the assets and their security properties directly via the user interfaces.		
Specifying Notes			
AV1/N1	This includes all user interfaces that can in some way influence the assets, in particular the legally relevant software, including the operating system.		
AV1/N2	This includes the inadmissible influence on the assets by trying to modify, remove or replace assets, including software modules of the legally relevant software, which the operating system can be a part of.		
AV1/N3	This applies to all assets whether stored, processed or indicated, etc.		
Functional Checks			
AV1/F1	Try some combinations of inputs and check that they do not inadmissibly influence the assets and their security properties.		
AV1/F2	Try some undocumented standard commands to check that they are not accepted.		
Keywords			
Assets:	software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions		
Security properties: integrity, authenticity, availability			

1.3. IIB1: Inadmissible influence via the boot process

Risk Class B		Risk Class C	Risk Class D		Risk Class E
AV1	An attacker inadmissibly influences the assets and their security properties via the user interfaces during the establishment of the environment for the assets (boot process).				
AV2	An attacker inadmissibly influences the assets and their security properties via the boot process.		AV2	An attacker inadmissibly influences the individual modules involved in the boot process up to the legally relevant application.	

Specifying Notes	
AV1/N1	This implies that the boot process of the operating system is unambiguous and reproducible.
AV1/N2	This implies that any module involved in establishing the environment (boot process) is legally relevant.
Functional Checks	
AV1/F1	Check that it is impossible to interrupt the boot process via the user interfaces, this includes settings in the bootloader, BIOS or UEFI.
Keywords	
Assets:	software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions
Security properties: integrity, authenticity, availability	

1.4. IIA1: Inadmissible influence via the administration of the operating system

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1	An attacker inadmissibly influences the assets and their security properties via the user interfaces by using the operating system.		
Specifying Notes			
AV1/N1	This includes basic tasks such as file, memory and process management, handling input and output, and controlling peripheral devices such as disk drives and printers.		
AV1/N2	This includes influence via protection means realized by the operating system.		
Functional Checks			
AV1/F1	Try to access the administrator account and check that access is secured.		
AV1/F2	Use the administrator account and check that any changes in the administration settings produce evidence of an intervention.		
-		AV1/F3	Check that user and group privileges as well as the administrator account are configured correctly.
		AV1/F4	Check that the configuration of the application control is configured correctly.
		AV1/F5	Check that mounted storage media, partitions and media with access attributes are configured correctly.
		AV1/F6	Check that policies for storage media and auxiliary devices

	correspond to the information contained in the documentation and are configured correctly.

Keywords

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

Security properties: integrity, authenticity, availability

1.5. IIN1: Inadmissible influence via legally non-relevant software

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1	An attacker inadmissibly influences the assets and their security properties by executing functions of the legally non-relevant software.		
AV2	An attacker inadmissibly influences the assets and their security properties directly via the functionalities of the legally non-relevant software.		

Specifying Notes

AV1/N1	This includes direct influence by the legally non-relevant software on any security property.
AV1/N2	This includes inadmissible influence via software interfaces between legally relevant and legally non-relevant software.
AV1/N3	This implies that there are enough resources for the operation of the legally relevant application.
AV1/N4	This includes inadmissible influence on the assets and their security properties via scheduling and runtime of the legally non-relevant software.
AV1/N5	This includes modification of the access rules realized by the implemented securing means for all assets.
AV1/N6	This includes modification of the implemented protection means without evidence of an intervention.
AV1/N7	This includes the use of measurement data by the legally non-relevant software to spoof legally relevant software.
AV1/N8	This applies to all assets whether stored, processed or indicated, etc.
AV2/N1	This includes the update procedure for legally non-relevant software.

Functional Checks

AV1/F1	Perform spot checks by using functions of any known legally non-relevant software and check that there is no inadmissible influence on the assets, e.g., if a measurement can be performed, the result has to be within the MPE or the critical change value.
AV1/F2	Check each interface that can be used for exchanging legally non-relevant software to ensure that an exchange does not inadmissibly influence any of the assets.

AV2/F1	Try to influence the assets by using simple software, e.g. a text editor, to modify, delete or replace assets.	AV2/F1	Try to influence the assets by using sophisticated software tools to modify, delete or replace assets.

Keywords

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

Security properties: integrity, authenticity, availability

1.6. IIC1: Inadmissible influence by obtaining confidential information

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1	An attacker inadmissibly influences the assets by obtaining confidential information.		
AV2	An attacker introduces fake confidential information into the measuring instrument.		

Specifying Notes

AV1/N1	Depending on the protection means, confidential information may consist of keys, generator polynomials, initial vectors / start values, seeds, etc.
AV1/N2	This includes access to stored cryptographic material during processing, e.g., access to the storage of cryptographic material in volatile memory.
AV1/N3	This includes side-channel attacks.

Functional Checks

AV1/F1	Check that it is impossible to retrieve the confidential information via any interfaces or by using legally non-relevant software.
AV2/F1	Check that it is impossible to introduce fake confidential information, e.g., via the user interfaces or by using legally non-relevant software.

Keywords

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

Security properties: authenticity

1.7. IIR1: Inadmissible influence by replacing physical parts within the measuring instrument

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1	An attacker inadmissibly influences the assets by replacing physical parts.		

Specifying Notes

AV1/N1	This includes physical parts within a complete measuring instrument or within a component.

AV1/N2	This includes memory chips that contain software or parameters, ADC and amplifiers, displays, etc.
AV1/N3	The replacement may result in different effects, from complete stop of operation to a slight distortion of the measurement result.
AV1/N4	This applies to all assets whether stored, processed or indicated, etc.
Functional Checks	
AV1/F1	Try to replace physical parts within the measuring instrument or component and check that this leads to evidence of an intervention and, if software is used to protect such parts from being replaced, that the replacement is detected and acted upon.
Keywords	
Assets:	software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions
Security properties: integrity, authenticity, availability	

2. Inadmissible influence on assets via external influence on the equipment under test

2.1. III2: Inadmissible influence via hardware interfaces

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1	An attacker inadmissibly influences the assets and their security properties via hardware interfaces by connecting legally non-relevant devices to the measuring instrument.		
Specifying Notes			
AV1/N1	Hardware interfaces include direct memory access, open interfaces and communication interfaces.		
AV1/N2	This includes the influence on operating system functions accessible via open interfaces.		
AV1/N3	This includes the influence via the connection of auxiliary devices, such as exchangeable media.		
AV1/N4	This includes modification of any access rules realized by the implemented securing means for all assets.		
AV1/N5	This includes modification of the implemented protection means without evidence of an intervention.		
AV1/N6	This includes influence via exchanging legally non-relevant software by connecting a storage device or by connecting to a network.		
AV1/N7	This applies to all assets whether stored, processed or indicated, etc.		
Functional Checks			
AV1/F1	Perform spot checks by, e.g., connecting a peripheral device and trying to influence the assets and their security properties.		
Keywords			
Assets:	software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions		
Security properties: integrity, authenticity, availability			

2.2. IID1: Inadmissible influence by downloading legally relevant software

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1	An attacker inadmissibly influences the assets and their security properties by downloading legally relevant software.		
Specifying Notes			
AV1/N1	This includes modifications of existing evidence of an intervention and parameters during, or as the result of, a software download.		
AV1/N2	This includes preventing evidence of an intervention from being generated during the download process.		

Functional Checks	
AV1/F1	Check that it is impossible to modify existing evidence of an intervention and parameters during a software download.
AV1/F2	Perform an update of legally relevant software and check that evidence of an intervention is generated correctly.
Keywords	
Assets:	software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions
Security properties: integrity, authenticity, availability	

2.3. IIR2: Inadmissible influence by replacing or removing complete components

Risk Class B	**Risk Class C**	**Risk Class D**	**Risk Class E**
AV1	An attacker inadmissibly influences the assets by replacing or removing complete components.		
Specifying Notes			
AV1/N1	This includes the replacement of sensors.		
AV1/N2	This includes the replacement of components with the intention to fake the measurement result.		
AV1/N3	This includes the removal of mandatory peripheral components. These components include, for example, printers and data storage devices for storing measurement results.		
AV1/N4	Typically, the removal of components that are routinely involved in continuous measurements is to be detected and appropriately acted upon.		
AV1/N5	This applies to all assets whether stored, processed or indicated, etc.		
Functional Checks			
AV1/F1	Try to replace individual components and check that this leads to evidence of an intervention and, if software is used to protect authenticity, check that the replacement is detected and acted upon.		
AV1/F2	Try to remove individual legally relevant components and check that the replacement is detected and acted upon.		
Keywords			
Assets:	software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions		
Security properties: integrity, authenticity, availability			

2.4. IIT1: Inadmissible influence by man-in-the-middle attacks

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1	An attacker inadmissibly influences the assets and their security properties during transmission within the measuring instrument.		
Specifying Notes			
AV1/N1	This includes capture, deletion, delay, modification, replacement, or disturbance of assets.		
AV1/N2	This includes capture-replay attacks.		
Functional Checks			
AV1/F1	Attempt to modify assets during transmission and check that this is detected and acted upon.		
AV1/F2	Attempt to interrupt or prevent the transmission of assets and check that this is detected and acted upon.		
AV1/F3	Attempt to introduce fraudulent assets into the transmission and check that these are detected and discarded.		
AV1/F4	Attempt to introduce copies of assets into the transmission and check that these are detected and discarded.		
Keywords			
Assets:	software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions		
Security properties: integrity, authenticity, availability			

2.5. IIA2: Inadmissible influence due to accidental modification

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1	The assets and their security properties are influenced due to accidental modification.		
Specifying Notes			
AV1/N1	This attack vector requires, most likely, some form of user interface that enables a person, e.g., a user, to modify assets.		
AV1/N2	Admissible access to the assets that might lead to unintentional modifications should be restricted, e.g., by a securing means such as a password, to enable intentional and authenticated modification. This includes deleting measurement data after a transaction is completed or changing restricted parameters.		
AV1/N3	The assets must be protected against accidental modification at any place or time, e.g., during processing on the main component or transmission to a storage component or during indication.		
Functional Checks			
AV1/F1	Check that it is impossible to modify an asset without authentication.		

Keywords	
Assets:	software, parameters, measurement data, measurement result, evidence of an intervention, inscriptions
Security properties: integrity, authenticity, availability	

2.6. IIS1: Inadmissible influence by incorrect software identification

Risk Class B	**Risk Class C**	**Risk Class D**	**Risk Class E**
AV1	An attacker inadmissibly influences the software by providing an ambiguous or no software identification.		
AV2	An attacker inadmissibly influences the software by providing an identical software identifier for different versions of the same software.		
Specifying Notes			
AV1/N1	This includes a software identifier that is used for multiple purposes where the identifier is not clearly distinguishable.		
AV1/N2	This includes software identifiers for legally relevant modules and the legally non-relevant modules that cannot be distinguished.		
AV1/N3	This includes software identifiers for modules in all components.		
AV1/N4	This includes software identifiers for an operating system, drivers and/or modules of that operating system and those that are specifically programmed for a legally relevant task.		
AV1/N5	This includes software identifiers for a specific legally relevant configuration of the operating system.		
Functional Checks			
AV1/F1	Check the software identification for completeness and comprehensibility.		
Keywords			
Assets:	software		
Security properties: integrity, authenticity, availability			

Annex III. Instrument-Specific Requirements

This annex is intended to complement the general software requirements of the previous chapters and cannot be considered isolated from the core requirements (see chapter 2). It reflects the existence of instrument-specific MID annexes MI-x and contains specific aspects and requirements for measuring instruments or systems (or sub-assemblies). These requirements do not, however, go beyond the requirements of the MID. If reference is made to OIML recommendations or ISO/IEC standards, this is done only if these can be considered as normative documents in the sense of the MID, and if this supports a harmonized interpretation of the MID requirements.

Besides instrument-specific software aspects and requirements, this annex contains the instrument (or category) specific assignment of risk classes which ensures a harmonized level of software examination, software protection and software conformity.

For the present, this annex is intended to be an initial draft to be completed by the respective WELMEC Working Group that has the corresponding specific knowledge. Therefore, Extension I has an "open structure", i.e., it provides a skeleton that is - besides the initial assignment of risk classes - filled-in only partly (e.g., for utility meters and automatic weighing instruments). It may be used for other MID (or non-MID) instruments, too, according to the experiences gained and decisions taken by the responsible WELMEC Working Groups.

1. Structure

There are different instrument-specific software aspects that might need consideration for a certain type of measuring instrument. These aspects should be treated in a systematic manner as follows: Each instrument-specific sub-chapter should be subdivided into the following categories.

1.1. Specific regulations, standards and other normative documents

Here, instrument (or category) specific regulations, standards and other normative documents (e.g., OIML recommendations) or WELMEC Guides should be mentioned that may help to develop instrument (or category) specific software requirements as an interpretation of the requirements of the MID Annex I and its instrument-specific annexes.

Normally, the specific software requirements apply in addition to the general ones in the previous chapters. Otherwise, it should be clearly stated whether a specific software requirement replaces one or more general software requirements, or whether one or more general software requirements are not applicable, and the reason why.

1.2. Technical description

In this section, examples of most common specific technical configurations, the application of the core requirements and attack vectors to these examples, and useful (instrument-specific) checklists for both the manufacturer and the examiner may be given. The description should mention:

- the measuring principle (cumulative measurement or single independent measurement; repeatable or non-repeatable measurement; static or dynamic measurement);
- the fault detection and reaction; two cases are possible:
  - the presence of a defect is obvious or can be checked easily, or there are hardware means for fault detection;

  - the presence of a defect is not obvious and cannot be checked easily, and there are no hardware means for fault detection. In this case, fault detection and reaction requires appropriate software means and hence appropriate software requirements.
- the hardware configuration (at least the following issues should be addressed):
  - Is there a modular, general-purpose computer-based system or a dedicated instrument with an embedded system subject to legal control?
  - Does the computer system stand-alone, or is it part of a closed network, e.g., Ethernet, token-ring LAN, or part of an open network, e.g., Internet?
  - Is the sensor separated (separate housing and separate power supply) from the main measuring system or is it partly or completely integrated into it?
  - Is the user interface always under legal control or can it be switched to an operating mode which is not under legal control?
  - Is long-term data storage foreseen? If yes, is the storage local (e.g., hard disk) or remote (e.g., file server)?
  - Is the storage medium fixed (e.g., internal ROM) or removable (e.g., floppy disc, CD-RW, smart-media card, memory stick)?
- the software configuration and environment; at least the following issues should be addressed:
  - Which operating system is used or can be used?
  - Do other software applications reside on the system besides the legally relevant software?
  - Is there software not subject to legal control that is intended to be freely modified after approval?

1.3. Specific software requirements

In this section, the specific software requirements should be listed using the same format as in chapter *3*.

1.4. Examples of legally relevant parameters, functions, and data

In this section, examples of the following may be given:

- device-specific parameters (e.g., individual configuration and calibration parameters of a specific measuring instrument),
- type-specific parameters (e.g., specific parameters that are fixed at type examination), or
- legally relevant, specific functions.

1.5. Other aspects

In this section, further aspects (e.g., specific documentation required for type (software) examination), specific descriptions, and instructions to be supplied in type examination certificates, or other aspects (e.g., requirements concerning the testability) may be mentioned.

1.6. Assignment of risk class

In this section, the appropriate risk class for instruments of the respective type should be defined. This can be done

- generally, or
- depending on the field of application, or category, or other aspects if these exist.

2. Water Meters

2.1. Specific regulations, standards and other normative documents

Member states may – in accordance with MID Article 2 – prescribe water meters in residential, commercial and light industrial use to be subject to the regulations in the MID. The specific requirements of this chapter are based on Annex III (MI-001) of the MID only.

2.2. Technical description

Hardware configuration

The water meter is an instrument intended to measure continuously, memorize, and display the volume of water passing through the measurement transducer at metering conditions. A water meter includes at least a measurement transducer, a calculator (including adjustment or correction devices, if present) and an indicating device. These three devices can be in different housings.

Note: Volume means in sense of accumulated amounts of volume over a time period.

Software Configuration

This is specific to each manufacturer who would normally be expected to follow the recommendations given in the main body of this guide.

Measuring Principle

Water meters continually cumulate the volume consumed. The cumulative volume is displayed at the instrument. Various principles are employed. The volume measurement typically cannot be repeated.

Fault Detection and Reaction

Requirement 7.1.2 in Annex III (MI-001) deals with electromagnetic disturbances. There is a need to interpret this requirement for software-controlled instruments because detection of a disturbance and recovery is only possible by co-operation of specific hardware components and specific modules. From the software point of view, it makes no difference what the reason for a disturbance was (electromagnetic, electrical, mechanical, etc.): the recovery procedures are all the same.

After undergoing an electromagnetic disturbance, the water meter shall

- recover to operate within MPE, and
- have all measurement functions safeguarded, and
- allow recovery of all measurement data present just before the disturbance.

See ISO 4064-1:2014 A3, A5 and OIML R 49:2024-1 A3, A5.

2.3. Specific software requirements

2.3.1. Fault recovery

Risk Class B	Risk Class C	Risk Class D
I1-1	The software shall recover from a disturbance to normal processing.	
Specifying Notes		
I1-1/N1	Date-stamped flags should be raised to help logging of periods of faulty operation.	
Required Documentation		
I1-1/D1	A brief description of the fault recovery mechanisms and an explanation of how and when it is invoked.	
I1-1/D2	A brief description of the related tests carried out by the manufacturer.	
I1-1/D3	A brief description of SW recovery mechanism steps after an error (from the manufacturer of the meter), if this is required for SW examination.	
Examination Guidance		
Checks based on the documentation		
I1-1/C1	Check if the realization of fault recovery is appropriate.	
Functional Checks		
I1-1/F1	Confirm correct functioning in the presence of defined influencing quantities and provoked errors.	

2.3.2. Back-up facilities

Risk Class B	Risk Class C	Risk Class D
I1-2	There shall be a back-up facility that periodically backs up measurement data, such as measurement values and the current status of the process. This back-up shall be stored in a non-volatile storage.	
Specifying Notes		
I1-2/N1	If the back-up facility is used for fault recovery, the minimum interval for the back-up shall be calculated to ensure the critical change value is not exceeded.	
Required Documentation		
I1-2/D1	A brief description of which data is backed up and when this occurs.	
I1-2/D2	Calculation of the minimum interval for the back-up to ensure that the critical change value is not exceeded.	

Examination Guidance

Checks based on the documentation

I1-2/C1 Check that the back-up is stored on a non-volatile storage and that it can be recovered.

Functional Checks

I1-2/F1 Confirm correct functioning in the presence of defined influencing quantities and provoked errors.

2.3.3. Inhibit resetting of cumulative data

Risk Class B	Risk Class C	Risk Class D

I1-3 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.

Specifying Notes

I1-3/N1 Cumulative registers of a measuring instrument shall be reset prior to the applicable conformity assessment procedure. During a conformity assessment procedure in accordance with annex D, F or H1, the water meters shall be fitted with all securing and protective means as specified by the TEC after which resetting of the cumulative measurement data shall not be possible without evidence of an intervention.

I1-3/N2 Totalizers of the cumulative registers of a measuring instrument shall be reset before the relevant conformity assessment procedure is completed. During the conformity assessment procedure in accordance with Annex D, F or H1, the water meters shall be equipped with all the safety provisions set out in the TEC, that shall ensure evidence of an intervention into the meter registers after resetting the cumulative measurement data.

Note: Cumulative registers are not allowed to be reset during use in distribution network.

Required Documentation

I1-3/D1 Documentation of protection means against resetting the volume registers.

Examination Guidance

Checks based on the documentation

I1-3/C1 Check that the reset operation of the cumulative legally relevant measurement data is secured and that the protective means foreseen shall provide for evidence of an intervention.

Functional Checks

I1-3/F1 Confirm correct functioning of the protective means foreseen, see also III1: Inadmissible influence via user interfaces and III2: Inadmissible influence via hardware interfaces.

2.3.4. Reading of measurement results

Risk Class B	Risk Class C	Risk Class D
I1-4	The measurement results that serve as the basis for the price to pay may be the results of different registers which are activated by remote control, a clock or other means. Each register represents the total quantity, connected to one rate in the billing process. It should be possible to show the results on different displays, periodically or on request, via the user interface.	
Specifying Notes		
I1-4/N1	Cumulative registers or totalized registers of the water meter may be reset prior to the applicable conformity assessment procedure. During a conformity assessment procedure in accordance with annex D, F or H1, the utility meters shall be fitted with all protective means as specified by the TEC by the manufacturer after which resetting of the cumulative measurement data shall not be possible without evidence of an intervention, see 2.3.3.	
I1-4/N2	When the maximum indicating range of the volume totalization is reached, the indicating range will continue measuring starting from zero cubic meter, see also 0.	
Required Documentation		
I1-4/D1	Documentation of how the obtained measurement results serve as the basis for the price to pay.	
Examination Guidance		
Checks based on the documentation		
I1-4/C1	Check the correct handling of the measurement result.	
Functional Checks		
I1-4/F1	Confirm correct functioning of the handling of the measurement results.	

2.3.5. Number of digits

Risk Class B	Risk Class C	Risk Class D
I1-5	The display of total quantity shall have sufficient numbers of digits.	
Specifying Notes		
I1-5/N1	A combination meter may have two indicating devices, the sum of which provides the indicated volume.	
I1-5/N2	Every indicating device shall provide means for visual, non-ambiguous verification testing and calibration.	
Required Documentation		
I1-5/D1	A description of the display and display menu.	

I1-5/D2	A description of the visual verification display and an explanation on how to initiate the visual verification display.

Examination Guidance

Checks based on the documentation

-

Functional Checks

I1-5/F1	Check that the displays of the total quantity have sufficient numbers of digits.
I1-5/F2	Initiate the visual verification display and check that the resolution of the visual verification display fulfills the requirements.
I1-5/F3	Initiate the visual verification display and check ithat special equipment or software for this control is part of the instrument (if relevant).

2.3.6. Display Test

Risk Class B	Risk Class C	Risk Class D
I1-5	To verify the correct function of all segments of the display, a display test shall be possible to be executed.	

Specifying Notes

-

Required Documentation

I1-5/D1	A description of the display and display menu.
I1-5/D2	A description of the visual verification display and an explanation of how to initiate visual verification display.

Examination Guidance

Checks based on the documentation

-

Functional Checks

I1-5/F1	Check that the displays of the total quantity have sufficient numbers of digits.
I1-5/F2	Initiate the visual verification display and check that the resolution of the visual verification display fulfills the requirements.
I1-5/F3	Initiate the visual verification display and check ithat special equipment or software for this control is part of the instrument (if relevant).

2.4. Examples of legally relevant parameters, functions, and data

Access to means for modification of software, settings and/or parameters that influence the determination of the results of measurements shall be secured.[4]

Parameter	Pro-tected	Setta-ble	Com-ment
Calibration factor	x		
Linearization factor	x		
Legally relevant configuration of registers	x		
Settings, for example: Correction devices Curve fitting	x		
Other relevant parameters that can or might influence the measurement result	x		
Software download of the legally relevant software	x		

2.5. Assignment of risk class

Risk class C is considered appropriate and should be applied.

[4] With respect to securing a water meter, additional guidance is given in WELMEC Guide 13.3.

3. Gas Meters and Volume Conversion Devices

3.1. Specific regulations, standards and other normative documents

The specific requirements of this chapter are based on MID, Annex IV Gas meters and Volume Conversion Devices (MI-002).

With respect to securing gas meters and volume conversion devices, guidance can also be found in WELMEC Guide 11.3.

Specific guidance in relation to the gas chromatograph connected as a live sensor to an EVCD can be found in WELMEC Guide 11.1.

Additional guidance or updates on specific guidance for gas meters and volume conversion devices can be found on the WELMEC website.

National legislation concerning additional functionality, OIML recommendations, (EN) harmonized standards and (IEC) standards have not been taken into consideration.

3.2. Technical Description

Hardware configuration

Gas meters and conversion devices are usually separate hardware components.

Indicators or calculators of gas meters and of volume conversion devices may have one or more interfaces to connect external sensor units.

In case a gas chromatograph is connected as a live sensor to an EVCD, the GC influences the measuring result (base volume) of the EVCD and should therefore be a part of the conformity assessment procedure.

Software Configuration

This is specific to each type of meter but would normally be expected to follow the recommendations given in the main body of this Guide.

Measuring Principle

Gas meters continually cumulate the volume or mass flow through the meter. A volume conversion device may be used to calculate the volume at base conditions.

The volume measurement is a non-repeatable measurement.

Fault Detection and Reaction

The requirement in MID, Annex IV Gas meters and Volume Conversion Devices (MI-002), article 3.1 deals with the permissible effect of disturbances. From the software point of view, it makes no difference what the reason for a disturbance was (electromagnetic, electrical, mechanical, etcetera): the recovery procedures are all the same.

After undergoing a disturbance, the gas meter shall:

- recover to operate within MPE, and
- have all measurement functions safeguarded, and
- allow recovery of all measurement data present just before the disturbance.

See article 3.1.2 of the MID, Annex IV Gas meters and Volume Conversion Devices (MI-002).

- An electronic conversion device shall be capable of detecting when it is operating outside the operating range(s) stated by the manufacturer for parameters that are relevant for measurement accuracy. In such a case, the conversion

device must stop integrating the converted quantity and may totalize separately the converted quantity for the time it is operating outside the operating range(s).

See article 9.1 of the MID, Annex IV Gas meters and Volume Conversion Devices (MI-002).

3.3. Specific software requirements

3.3.1. Fault recovery

Risk Class B	Risk Class C	Risk Class D
I2-1	The software shall recover from a disturbance to normal processing.	
Specifying Notes		
I2-1/N1	Date-stamped flags should be raised to help logging of periods of faulty operation.	
Required Documentation		
I2-1/D1	A brief description of the fault recovery mechanisms and an explanation of how and when it is invoked.	
Examination Guidance		
Checks based on the documentation		
I2-1/C1	Check that the realization of fault recovery is appropriate.	
Functional Checks		
I2-1/F1	Confirm correct functioning in the presence of defined influencing quantities and provoked errors.	

3.3.2. Back-up facilities

Risk Class B	Risk Class C	Risk Class D
I2-2	There shall be a back-up facility that periodically backs up measurement data, such as measurement values and the current status of the process. This back-up shall be stored in a non-volatile storage.	
Specifying Notes		
I2-2/N1	If the back-up facility is used for fault recovery, the minimum interval for the back-up shall be calculated to ensure the critical change value is not exceeded.	
Required Documentation		
I2-2/D1	A brief description of which data is backed up and when this occurs.	
I2-2/D2	Calculation of the minimum interval for the back-up to ensure that the critical change value is not exceeded.	

Examination Guidance	
Checks based on the documentation	
I2-2/C1	Check if the back-up is stored on a non-volatile storage and can if it can be recovered.
Functional Checks	
I2-2/F1	Confirm correct functioning in the presence of defined influencing quantities and provoked errors.

3.3.3. Inhibit resetting of cumulative measurement data

Risk Class B	**Risk Class C**	**Risk Class D**
I2-3	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.	
Specifying Notes		
I2-3/N1	During a conformity assessment procedure in accordance with annex D, F or H1, the water meters shall be fitted with all securing and protective means as specified by the TEC after which resetting of the cumulative measurement data shall not be possible without evidence of an intervention.	
I2-3/N2	For gas meters, the register for the total measured volume has to be protected by hardware metrological seals	
I2-3/N3	For conversion devices the volume at base conditions has to be protected by hardware metrological seals.	
Required Documentation		
I2-3/D1	Documentation of protection means against resetting the volume registers.	
Examination Guidance		
Checks based on the documentation:		
I2-3/C1	Check that the reset operation of the cumulative legally relevant measurement data is secured and that the protective means foreseen shall provide for evidence of an intervention.	
Functional Checks		
I2-3/F1	Confirm correct functioning of the protective means foreseen, see also III1: Inadmissible influence via user interfaces and III2: Inadmissible influence via hardware interfaces.	

3.3.4. Reading of measurement results

Risk Class B	Risk Class C	Risk Class D
I2-4	The measurement results, that serve as the basis for the price to pay, may be the results of different registers, which are activated by remote control, a clock or other means. Each register represents the total quantity, connected to one rate in the billing process. It should be possible to show the results on different displays, periodically or on request, via the user interface.	
Specifying Notes		
I2-4/N1	Cumulative registers of the measuring instrument may be reset prior to applicable conformity assessment procedure. During a conformity assessment procedure according to annex D, F or H1 the utility meters shall be fitted with all protective means as specified by the TEC by the manufacturer after which resetting of the cumulative measurement data shall not be possible without evidence of an intervention, see 2.3.3.	
Required Documentation		
I2-4/D1	Documentation of how the obtained measurement results serve as the basis for the price to pay.	
Examination Guidance		
Checks based on the documentation		
I2-4/C1	Check the correct handling of the measurement result.	
Functional Checks		
I2-4/F1	Confirm correct functioning of the handling of the measurement results.	

3.3.5. Number of digits

Risk Class B	Risk Class C	Risk Class D
I2-5	The display of total quantity shall have sufficient numbers of digits to ensure that when the meter is operated for 8000 hours at Q_{max}, the indication does not return to its initial value.	
Specifying Notes		
-		
Required Documentation		
I2-5/D1	Description of the internal representation of the register.	
Examination Guidance		
Checks based on the documentation		
I2-5/C1	Check that the number of digits is sufficient after 8000 hours of flow.	
Functional Checks		
-		

3.3.6. Power source lifetime

Risk Class B	Risk Class C	Risk Class D
I2-6	A dedicated power source shall have a lifetime of at least five years. After 90% of its lifetime an appropriate warning shall be shown.	
Specifying Notes		
I2-6/N1	Lifetime is used here in the sense of available energy capacity.	
I2-6/N2	If the power source can be changed in the field, parameters and measurement data shall not be corrupted during the changeover.	
I2-6/N3	Additional warnings before the 90% threshold is reached, is allowed provided that these warnings are not confusing.	
Required Documentation		
I2-6/D1	Documentation of the power source capacity, maximum lifetime (independent of energy consumption), measures to determine the consumed or available energy, description of the means for the warning of low available energy and of the battery exchange process.	
Examination Guidance		
Checks based on the documentation		
I2-6/C1	Check if the measures taken are appropriate for the surveillance of the energy available.	
Functional Checks -		

3.3.7. Test element

Risk Class B	Risk Class C	Risk Class D
I2-7	The gas meter shall have a test element, which shall enable tests to be carried out in a reasonable time.	
Specifying Notes		
I2-7/N1	The test element for accelerating time consuming test procedures is normally used for testing before installation and normal operation.	
I2-7/N2	During the test mode the same registers and software parts shall be used as during standard operating mode.	
Required Documentation		
I2-7/D1	Documentation of the test element and instructions for activating the test mode.	

Examination Guidance
Checks based on the documentation I2-7/C1 Check if all time consuming test procedures of the gas meter can be completed by means of the test element. Functional Checks -

3.3.8. Electronic conversion device

Risk Class B	**Risk Class C**	**Risk Class D**
I2-8	An electronic conversion device shall be capable of detecting when it is outside the specific field of measurement stated by the manufacturer, for parameters that are relevant for measurement accuracy. In such a case, the 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).	
Specifying Notes		
I2-8/N1	There shall be a display indication of the failure state.	
Required Documentation		
I2-8/D1	Documentation of the different registers for converted quantity and failure quantity.	
Examination Guidance		
Checks based on the documentation I2-8/C1 Check if the measures taken are appropriate for the management of unusual operating conditions. Functional Checks -		

3.3.9. Recalculation of the conversion factor

Risk Class B	**Risk Class C**	**Risk Class D**
I2-9	In electronic gas volume conversion devices, the conversion factor shall be recalculated at intervals not exceeding 1 min for a temperature conversion device and at intervals not exceeding 30 s for other types of gas volume conversion devices. However, when no volume signal has been received from the gas meter for over 1 min for a temperature conversion device, or over 30 s for other types, recalculation is not required until the next volume signal is received.	
Specifying Notes		
-		

Required Documentation
I2-9/D1 Documentation of the recalculating sequence.
Examination Guidance
Checks based on the documentation I2-9/C1 Check if the measures taken are. Functional Checks -

3.4. Examples of legally relevant parameters, functions, and data

Access to means for modification of legally relevant software, settings and/or parameters that influence the determination of the results of measurements shall be secured.[5]

For Gas meters for example but not limited to:

Parameter	**Protected**	**Settable**	**Comment**
Calibration factor	x		
Linearization factor	x		
Legally relevant configuration of registers	x		
Setting of for example: correction devices curve fitting pulse number minimum flow rate cut off setting of ultrasonic sensors transducers geometry in ultrasonic gas meters	x		
Other relevant parameters that can or might influence the measurement result	x		
Software download of the legally relevant software	x		

For Conversion devices for example but not limited to:

Parameter	**Protected**	**Settable**	**Comment**
Calibration factor	x		
Linearization factor	x		
Legally relevant configuration of registers	x		

[5] The manufacturer should always take into account the national requirements concerning additional functionality. With respect to interval metering additional guidance is given in WELMEC Guide 11.2.

Setting of for example: Legally relevant parameters of a correction device, such as parameters based on the error curve of a gas meter Pulse value of a gas meter Gas composition and parameters for compressibility calculation	x		
Other relevant parameters that can or might influence the measurement result	x		
Software download of the legally relevant software	x		

3.5. Assignment of risk class

Risk class C is considered appropriate and should be applied.

4. Active Electrical Energy Meters

4.1. Specific regulations, standards and other normative documents

The specific requirements of this chapter are based on MID, Annex V Active Electrical Energy Meters (MI-003).
With respect to securing Active Electrical Energy Meters guidance can also be found in WELMEC Guide 11.3.
Additional guidance or updates on specific guidance for Active Electrical Energy Meters is found on the WELMEC website.
National legislation concerning additional functionality, OIML recommendations, (EN) harmonized standards and (IEC) standards have not been taken into consideration.

4.2. Technical Description

Hardware configuration

Active electrical energy meters take voltages and currents measurements as inputs, derive the active electrical power from them, and integrate this with respect to time to give the energy consumed.

Active electrical energy meters may be used in combination with external instrument transformers.

Software Configuration

This is specific to each type of meter but would normally be expected to follow the recommendations given in the main body of this guide.

Measuring Principle

Active electrical energy meters continuously cumulate the energy consumed in a circuit. The cumulative consumed energy value is displayed by the instrument.

The measurement is a non-repeatable measurement.

Fault Detection and Reaction

The requirement in MID, Annex V Active Electrical Energy Meters (MI-003), article 4.3.1, deals with the permissible effect of disturbances. From the software point of view, it makes no difference what the reason for a disturbance was (electromagnetic, electrical, mechanical etc.) the recovery procedures are all the same.

After undergoing a disturbance, the meter shall:

- recover to operate within MPE, and
- have all measurement functions safeguarded, and
- allow recovery of all measurement data present just before the disturbance and
- not indicate a change in the registered energy of more than the critical change value.

4.3. Specific software requirements

4.3.1. Fault recovery

Risk Class B	Risk Class C	Risk Class D
I3-1	The software shall recover from a disturbance to normal processing.	
Specifying Notes		
I3-1/N1	Date stamped flags should be raised to help logging of periods of faulty operation.	
Required Documentation		
I3-1/D1	A brief description of the fault recovery mechanisms and an explanation of how and when it is invoked.	
I3-1/D2	A brief description of the related tests carried out by the manufacturer.	
Examination Guidance		
Checks based on the documentation		
I3-1/C1	Check if the realization of fault recovery is appropriate.	
Functional Checks		
I3-1/F1	Confirm correct functioning in the presence of defined influencing quantities and provoked errors.	

4.3.2. Back-up facility

Risk Class B	Risk Class C	Risk Class D
I3-2	There shall be a back-up facility that periodically backs up measurement data, such as measurement values and the current status of the process. This back-up shall be stored in a non-volatile storage.	
Specifying Notes		
I3-2/N1	If the back-up facility is used for fault recovery, the minimum interval for the back-up shall be calculated to ensure the critical change value is not exceeded.	
Required Documentation		
I3-2/D1	A brief description of which data is backed up and when this occurs.	
I3-2/D2	Calculation of the minimum interval for the back-up to ensure that the critical change value is not exceeded.	
Examination Guidance		
Checks based on the documentation		
I3-2/C1	Check if the back-up is stored on a non-volatile storage and can if it can be recovered.	
Functional Checks		
I3-2/F1	Confirm correct functioning in the presence of defined influencing quantities and provoked errors.	

4.3.3. Inhibit resetting of cumulative measurement data

Risk Class B	Risk Class C	Risk Class D
I3-3	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.	
Specifying Notes		
I3-3/N1	Cumulative registers of a measuring instrument shall be reset prior to applicable conformity assessment procedure.	
I3-3/N2	During a conformity assessment procedure according to annex D, F or H1 the utility meters shall be fitted with all securing and protective means as specified by the TEC after which resetting of the cumulative measurement data shall not be possible without evidence of an intervention.	
Required Documentation		
I3-3/D1	Documentation of protection means against resetting the energy registers.	
Examination Guidance		
Checks based on the documentation		
I3-3/C1	Check that the reset operation of the cumulative legally relevant measurement data is secured and that the protective means foreseen shall provide for evidence of an intervention.	
Functional Checks		
I3-3/F1	Confirm correct functioning of the protective means foreseen, see also III1: Inadmissible influence via user interfaces and III2: Inadmissible influence via hardware interfaces.	

4.3.4. Reading of measurement results

Risk Class B	Risk Class C	Risk Class D
I3-4	The measurement results, that serve as the basis for the price to pay, may be the results of different registers, which are activated by remote control, a clock or other means. Each register represents the total quantity, connected to one rate in the billing process. It should be possible to show the results on different displays, periodically or on request, via the user interface.	
Specifying Notes		
I3-4/N1	Cumulative registers of the measuring instrument may be reset prior to applicable conformity assessment procedure. During a conformity assessment procedure according to annex D, F or H1 the utility meters shall be fitted with all protective means as specified by the TEC by the manufacturer after which resetting of the cumulative measurement data shall not be possible without evidence of an intervention, see 2.3.3.	

Required Documentation	
I3-4/D1	Documentation of how the obtained measurement results serve as the basis for the price to pay.
Examination Guidance	
Checks based on the documentation	
I3-4/C1	Check the correct handling of the measurement result.
Functional Checks	
I3-4/F1	Confirm correct functioning of the handling of the measurement results.

4.3.5. Number of digits

Risk Class B	**Risk Class C**	**Risk Class D**
I3-5	The display of total quantity shall have sufficient numbers of digits to ensure that when the meter is operated for 4000 hours at full load ($I=I_{max}$, $U=U_n$ and PF=1), the indication does not return to its initial value.	
Specifying Notes		
-		
Required Documentation		
I3-5/D1	Description of the internal representation of the electrical energy register and auxiliary quantities.	
Examination Guidance		
Checks based on the documentation		
I3-5/C1	Check whether the number of digits is sufficient (internal and on display).	
Functional Checks		
-		

4.4. Examples of legally relevant parameters, functions, and data

Access to means for modification of software, settings and/or parameters that influence the determination of the results of measurements shall be secured.[6]

Parameter	**Protected**	**Settable**	**Comment**
Calibration factor	x		
Linearization factor	x		
Legally relevant configuration of registers	x		

[6] The manufacturer should always take into account the national requirements concerning additional functionality.

Setting of for example: legally relevant parameters of a correction devices, such as parameters based on curve fitting of an active electrical energy mete transformer ratio	x		
Other relevant parameters that can or might influence the measurement result	x		
Software download of the legally relevant software	x		

4.5. Assignment of risk class

Risk class C is considered appropriate and should be applied.

5. Thermal Energy Meters

5.1. Specific regulations, standards and other normative documents

Member states may – in accordance with MID Article 2 – prescribe Thermal energy meters in residential, commercial and light industrial use to be subject to regulations in the MID. The specific requirements of this chapter are based on Annex VI (MI-004) of the MID only.

5.2. Technical Description

Hardware configuration

The thermal energy meters are instruments for measuring thermal energy transferred by the heat-transfer medium. A thermal energy meter is either a complete instrument or a combined instrument consisting of the sub-assemblies (modular approach), e.g., flow sensor, temperature sensor pair, and calculator, as defined in MID Article 4(b). A thermal energy meter can be a combination of both. Separate assemblies of thermal energy meters, which has an evaluation unit (contain software) shall be to the subject of the examination process also.

Software Configuration

This is specific to each manufacturer who would normally be expected to follow the recommendations given in the main body of this guide.

Measuring Principle

Thermal energy meters continually cumulate the energy consumed in a heating circuit. The cumulated thermal energy is displayed at the instrument. Various principles are employed. The energy measurement may not be repeated.

Fault Detection and Reaction

The requirement VI (MI-004), 4.1 and 4.2 deal with electromagnetic disturbances. There is a need to interpret these requirements for software-controlled instruments because detection of a disturbance and recovery is only possible by co-operation of specific hardware parts and specific software. From the software point of view, it makes no difference what the reason for a disturbance was (electromagnetic, electrical, mechanical, etc): the recovery procedures are all the same.

After undergoing an electromagnetic disturbance, the thermal energy meter shall

- recover to operate within MPE, and
- have all measurement functions safeguarded, and
- allow recovery of all measurement data present just before the disturbance.

See EN 1434-4:2015 chapter 7.

5.3. Specific software requirements

5.3.1. Fault recovery

Risk Class B	Risk Class C	Risk Class D
I4-1	The software shall recover from a disturbance to normal processing.	
Specifying Notes		
I4-1/N1	Date stamped flags should be raised to help logging of periods of faulty operation.	
Required Documentation		
I4-1/D1	A brief description of the fault recovery mechanisms and an explanation of how and when it is invoked.	
I4-1/D2	A brief description of the related tests carried out by the manufacturer.	
Examination Guidance		
Checks based on the documentation		
I4-1/C1	Check if the realization of fault recovery is appropriate.	
Functional Checks		
I4-1/F1	Confirm correct functioning in the presence of defined influencing quantities and provoked errors.	

5.3.2. Back-up facility

Risk Class B	Risk Class C	Risk Class D
I4-2	There shall be a back-up facility that periodically backs up measurement data, such as measurement values and the current status of the process. This back-up shall be stored in a non-volatile storage.	
Specifying Notes		
I4-2/N1	If the back-up facility is used for fault recovery, the minimum interval for the back-up shall be calculated to ensure the critical change value is not exceeded.	
Required Documentation		
I4-2/D1	A brief description of which data is backed up and when this occurs.	
I4-2/D2	Calculation of the minimum interval for the back-up to ensure that the critical change value is not exceeded.	
Examination Guidance		
Checks based on the documentation		
I4-2/C1	Check if the back-up is stored on a non-volatile storage and can if it can be recovered.	
Functional Checks		
I4-2/F1	Confirm correct functioning in the presence of defined influencing quantities and provoked errors.	

5.3.3. Inhibit resetting of cumulative measurement data

Risk Class B	Risk Class C	Risk Class D
I4-3	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.	
Specifying Notes		
I4-3/N1	Cumulative registers of a measuring instrument shall be reset prior to applicable conformity assessment procedure. During a conformity assessment procedure according to annex D, F or H1 the thermal energy meters shall be fitted with all securing and protective means as specified by the TEC by the manufacturer after which resetting of the cumulative measurement data shall not be possible without evidence of an intervention.	
I4-3/N2	Totalizers of the cumulative registers of a measuring instrument shall be reset before the relevant conformity assessment procedure is completed. During the conformity assessment procedure according to Annex D, F or H1, the thermal energy meters shall be equipped with all the safety provisions set out in the TEC, that shall ensure evidence of an intervention into the meter registers after resetting the cumulative measurement data.	
I4-3/N3	Cumulative registers are not allowed to be reset during use in distribution network.	
Required Documentation		
I4-3/D1	Documentation of protection means against resetting the energy registers.	
Examination Guidance		
Checks based on the documentation		
I4-3/C1	Check that the reset operation of the cumulative legally relevant measurement data is secured and that the protective means foreseen shall provide for evidence of an intervention.	
Functional Checks		
I4-3/F1	Confirm correct functioning of the protective means foreseen, see also III1: Inadmissible influence via user interfaces and III2: Inadmissible influence via hardware interfaces.	

5.3.4. Reading of measurement results

Risk Class B	Risk Class C	Risk Class D
I4-4	The measurement results, that serve as the basis for the price to pay, may be the results of different registers, which are activated by remote control, a clock or other means. Each register represents the total quantity, connected to one rate in the billing process. It should be possible to show the results on different displays, periodically or on request, via the user interface.	

Specifying Notes	
I4-4/N1	Cumulative registers of the measuring instrument may be reset prior to applicable conformity assessment procedure. During a conformity assessment procedure according to annex D, F or H1 the utility meters shall be fitted with all protective means as specified by the TEC by the manufacturer after which resetting of the cumulative measurement data shall not be possible without evidence of an intervention, see 2.3.3.
I4-4/N2	When the maximum indicating range of the totalization of the quantity of heat is reached, the indicating range will continue measuring starting from zero cubic meter, see also 5.3.5.
Required Documentation	
I4-4/D1	Documentation of how the obtained measurement results serve as the basis for the price to pay.
Examination Guidance	
Checks based on the documentation	
I4-4/C1	Check the correct handling of the measurement result.
Functional Checks	
I4-4/F1	Confirm correct functioning of the handling of the measurement results.

5.3.5. Number of digits

Risk Class B	Risk Class C	Risk Class D
I4-5	The display indicating the quantity of heat shall be able to register, without overflow, a quantity of heat at least equal to the transfer of energy, which corresponds to a continuous operation for 3000 hours at the upper limit of the thermal power of the heat meter. The quantity of heat, measured by a heat meter, operating at the upper limit of the thermal power for 1 hour shall correspond to at least one digit of lowest significance of the display.	
Specifying Notes		
I4-5/N1	The test signal output shall be according to EN1434-2 paragraph 5.3.	
I4-5/N2	The indicating device of a heat meter shall provide an easily read, reliable, and unambiguous visual indication of the indicated volume. A combination meter may have two indicating devices, the sum of which provides the indicated volume.	
I4-5/N3	Every indicating device shall provide means for visual, non-ambiguous verification testing and calibration.	
I4-5/N4	The visual verification display may have either a continuous or a discontinuous movement.	

Required Documentation	
I3-5/D1	Documentation of the internal representation of the calculator of energy, temperature sensor, and flowmeters.
I3-5/D2	A description of the display and display menu.
I3-5/D3	A description of the visual verification display and an explanation on how to initiate visual verification display.
Examination Guidance	
Checks based on the documentation	
I4-5/C1	Check if the number of digits is sufficient (internal and on display).
Functional Checks	
I4-5/F1	Check if the display of total quantity has sufficient numbers of digits.
I4-5/F2	Initiate the visual verification display and check if the resolution of the visual verification display fulfils the requirements and check if special equipment or software for this control is part of the instrument (if relevant).

5.3.6. Display test

Risk Class B	Risk Class C	Risk Class D
I4-6	For verifying the correct function of all segments of the electronic display, a display test shall be possible to be executed.	
Specifying Notes		
I4-6/N1	The meter shall provide visual checking of the entire display which shall have the following sequence: for seven segment type displaying all the elements (e.g. an “eights” test), for seven segment type blanking all the elements (a “blanks” test), or graphical displays an equivalent test to demonstrate that display faults cannot result in any digit being misinterpreted.	
I4-6/N2	Each step of the sequence shall last at least 1 second.	
Required Documentation		
I4-5/D1	Description of the electronic display test and an explanation on how to initiate such a test.	
Examination Guidance		
Checks based on the documentation		
-		
Functional Checks		
I4-6/F1	Initiate the display test and check if visual checking of the entire display is possible.	

5.4. Examples of legally relevant parameters, functions, and data

Access to means for modification of software, settings and/or parameters that influence the determination of the results of measurements shall be secured.[7]

Parameter	Protected	Settable	Comment
Calibration factor	x		
Linearization factor	x		
Legally relevant configuration of registers	x		
Other relevant parameters that can or might influence the measurement result - unit of measuring energy (MWh, GJ), installation sensor of flow (supply, return branch of the thermal circuit).	x		
Software download of the legally relevant software	x		

5.5. Assignment of risk class

Risk class C is considered appropriate and should be applied.

[7] The manufacturer should always take into account the national requirements concerning additional functionality. With respect to interval metering additional guidance is given in WELMEC Guide 13.3.

6. Measuring Systems for the Continuous and Dynamic Measurement of Quantities of Liquids Other than Water

Measuring systems for the continuous and dynamic measurement of quantities of liquids other than water are subject to the requirements of the MID. The specific requirements of this chapter are based on Annex I and Annex VII (MI-005) only.

6.1. Specific regulations, standards and other normative documents

The specific requirements of this chapter are based on MID, Annex VII and OIML R117-1 edition 2019.

6.2. Technical Description

Hardware configuration

The smallest possible measuring system shall include:

- a meter,
- a transfer point, and
- a hydraulic path.

For correct operation, it is often necessary to add:

- a gas elimination device,
- a filter,
- a pump, and
- correction devices

The measuring system may be provided with other ancillary and additional devices.

Ancillary and additional devices can be:

- zero-setting device;
- repeating indicating device;
- printing device;
- memory device;
- price indicating device;
- totalizing indicating device;
- correction device;
- conversion device;
- pre-setting device;
- self-service arrangement; and
- self-service device.

If ancillary and additional devices is/are part(s) of Measuring Systems for continuous and dynamic measurement of quantities of liquids other than water as separate device/s which can be disconnected without breaking the seal(s) and contains legally relevant software, then IIT1 must be considered.

If several meters are intended for a single measuring operation, the meters are considered to form a single measuring system.

If several meters intended for separate measuring operations have common elements (calculator, filter, gas elimination device, conversion devices, etc.), each meter is considered to form a separate measuring system, sharing the common elements.

Software Configuration

This is specific to each manufacturer but would normally be expected to follow the recommendations given in the main body of this guide.

Measuring Principle

The quantity of the liquid is measured by means of measuring sensor of a volume or mass flow sensor which can operate on different principles. The measured quantity is converted into a signal (e.g. pulses) in the transmitter and sent to the calculator and indicating device. They together form a meter. Further auxiliary measuring devices for measuring liquid characteristic can be connected to the meter. E.g. temperature sensor, pressure sensor. The measured quantity can be converted to the base conditions, e.g., using an ATC (Automatic Temperature Compensation) function for conversion to 15 °C. The measured quantity must be indicated in millilitres, cubic centimetres, litters, cubic meters, grams, kilograms or tons.

Fault Detection and Reaction

The requirement of Annex VII (MI-005), Article 3.1 deals with electromagnetic interference. This requirement must be interpreted in relation to software-controlled devices since interference detection and error correction are not possible without the interoperability of specific hardware components and modules. In terms of software the type of interference does not matter, e.g.: electromagnetic, electrical or mechanical interference, as recovery procedures are always the same.

6.3. Specific software requirements

6.3.1. Fault recovery

Risk Class B	Risk Class C	Risk Class D
I5-1.1 The software shall recover from a disturbance to normal processing. Interruptible electronic measuring systems shall be designed and manufactured such that when they are exposed to the disturbances either: a) the indication of the measurement result shows a momentary variation that cannot be interpreted, memorized or transmitted as a measuring result. Furthermore, in the case of an interruptible system, this can also mean the impossibility to perform any measurement; or b) the change in the measurement result is greater than the critical change value, in which case the measuring system shall permit the retrieval of the measuring result just before the critical change value occurred and cut off the flow.		
Additional requirement is stated in OIML R117-1:2019 section A.1.5 regarding fault generation parameters.		
Specifying Notes		
I5-1/N1 For non-interruptible measuring systems the detection by the checking facilities of incorrectness in the generation, transmission, processing and/or indication of measurement data shall result in the following actions: automatic correction of the malfunction; or stopping only the faulty device when the measuring system without that device continues to comply with the regulations.		

I5-1/N2	If the checking facilities of an interruptible electronic measuring systems detect significant defects or any incorrectness in the generation, transmission, processing, or indication of the measurement data they shall act by either automatic correction of the malfunction; or stopping only the faulty device, when the measuring system without that device continues to comply with the regulations; or the measuring system shall permit the retrieval of the measuring result just before the critical change value occurred and cut off the flow.
Required Documentation	
I5-1/D1	A brief description of what is checked, what is required to trigger the fault detection process, what action is taken on the detection of a fault.
I5-1/D2	A list of parameters and their valid and controlled ranges which may generate faults and which will be detected by the software including the expected reaction and, if necessary for understanding the detection algorithm, its description.
Examination Guidance	
Checks based on the documentation	
I5-1/C1	Check if the realisation of fault recovery is appropriate.
Functional Checks	
I5-1/F1	Confirm correct functioning in the presence of defined influencing quantities and provoked errors.

6.3.2. Back-up facility

Risk Class B	Risk Class C	Risk Class D
I5-2	There shall be a back-up facility that periodically backs up measurement data, such as measurement values and the current status of the process. This back-up shall be stored in a non-volatile storage.	
Specifying Notes		
I5-2/N1	If the back-up facility is used for fault recovery, the minimum interval for the back-up shall be calculated to ensure the critical change value is not exceeded.	
Required Documentation		
I5-2/D1	A brief description of which data is backed up and when this occurs.	
I5-2/D2	Calculation of the minimum interval for the back-up to ensure that the critical change value is not exceeded.	
Examination Guidance		
Checks based on the documentation		
I5-2/C1	Check if the back-up is stored on a non-volatile storage and can if it can be recovered.	

Functional Checks	
I5-2/F1	Confirm correct functioning in the presence of defined influencing quantities and provoked errors.

6.4. Examples of legally relevant parameters, functions, and data

Access to means for modification of software, settings and/or parameters that influence the determination of the results of measurements shall be secured.[8]

Parameter	Protected	Settable	Comment
Calibration factor	x		
Linearization factor	x		
Legally relevant configuration of registers	x		
Other relevant parameters that can or might influence the measurement result, for example but not limited to: Number of decimal places for quantity indication Low flow cut off Service commands (Saving of peripheral unit IDs, Resetting of electronic totals, complete initialization of memory - electronic summaries, statistics and history, and transition of parameters to factory settings) Value measured by mass meter - setting L / kg Suppression of the dispensing hose dilation - setting the hidden amount at the start of dispensing Correction factor of the meter Measuring time after hanging the nozzle pulse / L, pulse / kg Activating of the automatic temperature compensation for individual nozzles (ATC) and calibration of temperature sensors Fuel type or density Assignment of temperature sensors to individual nozzles Configuration of the mass meter Setting the zero point of the mass meter	x		
Software download of the legally relevant software	x		
Software setting/configuration in case of pulse signals	x		
Software setting/configuration in case of digital data	x		

[8] See also WELMEC Guide 10.6: Guide for securing of Fuel Dispensers.

6.5. Assignment of risk class

Risk class C is considered appropriate and should be applied.

7. Weighing Instruments

Weighing instruments are divided into two main categories:

- Non-automatic weighing instruments (NAWIs), and
- Automatic weighing instruments (AWIs).

While most AWIs are governed by the MID, NAWIs are not; they are governed by the European Directive 2014/31/EU. Therefore, the WELMEC Guide 7.5 applies to NAWIs, whereas this software guide applies to AWIs.

The specific requirements of this chapter are based on Annex MI-006 and the normative documents mentioned in 10.6.1 as far as they support the interpretation of MID requirements.

7.1. Specific regulations, standards and other normative documents

Five categories of automatic weighing instruments (AWIs) are subject to regulations in MID Annex MI-006:

- Automatic catchweighers (R51)
- Automatic gravimetric filling instruments (R61)
- Discontinuous totalizers (R107)
- Continuous totalizers (belt weighers) (R50)
- Automatic rail weighbridges (R106)

The numbers in brackets refer to the respective OIML recommendations that are normative documents in the sense of the MID. In addition, WELMEC has issued the WELMEC Guide 2.6 that supports the testing of automatic catchweighers.

There is one category of AWIs that is not governed by the MID:

- Automatic instruments for weighing road vehicles in motion (R134)

However, of these six categories, only **discontinuous totalizers** and **continuous totalizers** (belt weighers) have been identified as requiring instrument-specific software requirements (see 10.6.3). The reason is that the measurement is cumulative over a relatively long period of time and cannot be repeated if a significant defect occurs.

7.2. Technical Description

Hardware configuration

A discontinuous totalizer is a totalizing hopper weigher that determines the mass of a bulk product (e.g. grain) by dividing it into discrete loads. The system usually comprises of one or more hoppers supported on load cells, power supply, electronic controls and indicating device.

A continuous totalizer is a belt weigher that measures the mass of a product as the belt passes over a load cell. The system usually comprises of a conveyor belt, rollers, load receptor supported on load cells, power supply, electronic controls and indicating device. There will be a means for adjusting the tension of the belt.

Software Configuration

This is specific to each manufacturer but would normally expect to follow the recommendations given in the main body of this guide.

Measuring Principle

In the case of a discontinuous totaliser the bulk product is fed into a hopper and weighed. The mass of each discrete load is determined in sequence and summed. Each discrete load is then delivered to bulk.

In the case of a continuous totaliser the mass is continually measured as the product passes over the load receptor. Measurements are made in discrete units of time that depend on the belt speed and the force on the load receptor. There is no deliberate subdivision of the product or interruption of the conveyor belt as with a discontinuous totaliser. The total mass is an integration of the discrete samples. It should be noted that the load receptor could use strain gauge load cells or other technologies such as vibrating wire.

Fault Detection and Reaction

Joints in the belt may generate shock effects, which can lead to erroneous results when zeroing. In the case of discontinuous totalisers, single or all weighing results of discrete loads may get lost before being summed up.

7.3. Specific software requirements

MID Annex MI-006, Chapter IV, Section 8, and Chapter V, Section 6 deals with electromagnetic disturbances. There is a need to interpret these requirements for software-controlled instruments because the detection of a disturbance (fault) and subsequent recovery are only possible through the co-operation of specific hardware parts and specific software. From the software point of view, it makes no difference what the reason of a disturbance was (electromagnetic, electrical, mechanical etc); the recovery procedures are all the same.

7.3.1. Fault detection

Risk Class B		Risk Class C	Risk Class D
I6-1	The software shall detect if normal processing is disturbed. On detection of a fault, the cumulative measurement and other relevant legal data shall be automatically saved to non-volatile storage (see 7.3.1), and the hopper weigher or belt weigher shall be stopped automatically, or a visible or audible alarm signal shall be given (see Required Documentation)		
Specifying Notes			
-			
Required Documentation			
I6-1/D1	A brief description of what is checked, what is required to trigger the fault detection process, what action is taken on the detection of a fault.		
I6-1/D2	If, on detection of a fault, it is not possible to stop the transportation system automatically without delay (e.g., due to safety reasons) the documentation shall include a description of how the non-measured material is treated or properly taken into account.		
Examination Guidance			
Checks based on the documentation			
I6-1/C1	Check if the realization of fault detection is appropriate.		

Functional Checks	
I6-1/F1	If possible: simulate certain hardware faults and check if they are detected and reacted upon by the software as described in the documentation.

7.3.2. Back-up facility

Risk Class B	Risk Class C	Risk Class D
I6-2	There shall be a back-up facility that periodically backs up measurement data, such as measurement values and the current status of the process. This back-up shall be stored in a non-volatile storage.	
Specifying Notes		
I6-2/N1	The state characteristics and important data are included in the back-up.	
I6-2/N2	This requirement normally implies a controlled storage facility providing automatic back-up in case of a disturbance. Periodic backing up is acceptable only if a controlled storage facility is not available due to hardware or functional constraints. In that exceptional case the storage intervals shall be sufficiently small, i.e., the maximum possible discrepancy between the current and saved measurement data shall be within a defined fraction of the maximum permissible error (see Required Documentation)	
I6-2/N3	The back-up facilities should normally include appropriate wake-up facilities in order that the weighing system, including its software, does not get into an indefinite state by a disturbance.	
Required Documentation		
I6-2/D1	A brief description of the back-up mechanism and the data that are backed up, and when this occurs.	
I6-2/D2	Specification or calculation of the maximum error that can occur for cumulative measurement data if a cyclical (periodic) back-up is realized.	
Examination Guidance		
Checks based on the documentation		
I6-2/C1	Check if the back-up is stored on a non-volatile storage and can if it can be recovered.	
Functional Checks		
I6-2/F1	Confirm correct functioning in the presence of defined influencing quantities and provoked errors.	

7.4. Examples of legally relevant parameters, functions, and data

Examples of legally relevant, device-specific and type-specific functions and data (DF, DD, TF, TD) for AWIs in comparison with those of non-automatic weighing instruments (R76) are listed in the table below. VV indicates variable values.

Parameter	Type	OIML Recommendation No.						
		50	51 (X)	51 (Y)	61	76	106	107
Weight calculation	TF, TD	X	X	X	X	X	X	X
Stability analysis	TF, TD		X	X	X	X	X	X
Price calculation	TF, TD			X		X		
Rounding algorithm for price	TF, TD			X		X		
Span (sensitivity)	DD	X	X	X	X	X	X	X
Corrections for non-linearity	DD (TD)	X	X	X	X	X	X	X
Max, Min, e, d	DD (TD)	X	X	X	X	X	X	X
Units of measurement (e.g., g, kg)	DD (TD)	X	X	X	X	X	X	X
Weight value as displayed (rounded to multiples of e or d)	W	X		X		X	X	X
Tare, preset tare	W		X	X	X	X	X	
Unit price, price to pay	W			X		X		X
Weight value in internal resolution	W	X	X	X	X	X	X	X
Status signals (e.g., zero indication, stability of equilibrium)	TF	X	X	X	X	X	X	X
Comparison of actual weight vs. preset value	TF		X		X			
Automatic printout release, e.g., at interruption of automatic operation	TF	X						X
Warm-up time	TF (TD)	X	X	X	X	X	X	X
Interlock between functions	TF		X	X				
e.g., zero setting/tare	TF		X	X	X	X		

automatic/non-automatic operation	TF						X	
zero-setting/totalizing	TF	X						X
Record of access to dynamic setting	TF (W)		X	X				
Maximum rate of operation/range of operating speeds (dynamic weighing)	DD (TD)	X	X	X	X		X	X
(Product)-Parameters for dynamic weight calculation	W		X	X			X	
Preset weight value	W		X		X			
Width of adjustment range	DD (TD)		X	X				
Criterion for automatic zero-setting (e.g., time interval, end of weighing cycle)	DD (TD)		X	X	X		X	X
Minimum discharge, rated minimum fill	DD				X			X
Limiting value of significant defect (if not 1e or 1d)	DD (TD)	X			X			
Limiting value of battery power	DD (TD)	X	X	X	X	X	X	X

The marked functions and parameters are likely to occur on the various types of weighing instruments. If one of them is present, it has then to be treated as “legally relevant”. The table is, however, not meant as an obligatory list indicating that any function or parameter mentioned has to be realized in each instrument.

7.5. Assignment of risk class

For the present, according to the decision of the responsible WELMEC Working Group (24th WG 2 meeting, 22/23 January 2004) risk class "B" shall be generally applied to all categories of AWIs.

However, as a result of the WG 7 questionnaire (2004), the following differentiation seems appropriate:

- Risk class B for embedded systems (except totalizers),
- Risk class C for all other systems.

The embedded IT system is characterized as follows:

- The software is exclusively constructed for the measuring purpose. Additional functions for securing software and data, for transmitting data and for downloading software are considered constructed for the measuring purpose.

- The user interface is dedicated to the measuring purpose, i.e., it is normally in an operating mode subject to legal control. Switching to an operating mode not subject to legal control is possible.
- An operating system (OS) or subsystems of it may be included
    - if all communication is under control of legally relevant software,
    - it does not allow loading or changing modules, parameters or data or running programs,
    - it does not allow to change the environment of the legally relevant application, etc.
- This includes that the access prevention shall be preset and not the result of a respective subsequent configuration of these components.
- The software environment is invariable and there are no internal or external means for programming or changing the software in its embedded status.
- Software download is allowed if implemented according to this guide, see also generic attack vector IID1.

8. Taximeters

Taximeters are subject to regulations in MID. The specific requirements are in Annex MI-007. These specific requirements, the normative document OIML R 21 (2007) and WELMEC CT-007 (corresponding table) have been taken into consideration.

8.1. Specific regulations, standards and other normative documents

OIML Recommendation R 21 on taximeters is a normative document in the sense of the MID. WELMEC CT-007 about taximeters shows the correspondence between the essential requirements of MID and OIML R 21. WELMEC 12.1 gives specific interpretations of MID and corresponding clauses of OIML R 21.

8.2. Technical Description

A taximeter as defined in MID measures the time, the distance (using the output of a distance signal generator not covered by MID) and calculates the fare for a trip based on the applicable tariffs.

Taximeters can use an embedded architecture, which means built-for-purpose instruments or an architecture using universal devices with an operating system.

Hardware configuration

-

Software Configuration

-

Measuring Principle

-

Fault Detection and Reaction

-

8.3. Specific software requirements

MID Annex IX, 4:

A taximeter shall be able to supply the following data through an appropriate protected interface(s):

- operation position: ‘For Hire’, ‘Hired’ or ‘Stopped’;
- totaliser data according to paragraph 15.1 of MID;
- general information: constant of the distance signal generator, date of securing, taxi identifier, real time, identification of the tariff;
- fare information for a trip: total charged, fare, calculation of the fare, supplement charge, date, start time, finish time, distance travelled;
- tariff(s) information: parameters of tariff(s).

National legislation may require certain devices to be connected to the interface(s) of a taximeter. Where such a device is required; it shall be possible, by secured setting, to inhibit automatically the operation of the taximeter for reasons of the non-presence or improper functioning of the required device.

MID Annex IX, 9:

In case of a reduction of the voltage supply to a value below the lower operating limit as specified by the manufacturer, the taximeter shall:

- continue to work correctly or resume its correct functioning without loss of data available before the voltage drop if the voltage drop is temporary, i.e. due to restarting the engine,
- abort an existing measurement and return to the position "For Hire" if the voltage drop is for a longer period.

MID Annex IX, 15.2:

- If disconnected from power, a taximeter shall allow the totalised values to be stored for one year for the purpose of reading out the values from the taximeter to another medium.

MID Annex IX, 19:

A taximeter and its installation instructions specified by the manufacturer shall be such that, if installed according to the manufacturer's instructions, fraudulent alterations of the measurement signal representing the distance travelled are sufficiently excluded.

8.3.1. Back-up facility

Risk Class B		Risk Class C	Risk Class D
I7-1	There shall be a back-up facility that periodically backs up measurement data, such as measurement values and the current status of the process. This back-up shall be stored in a non-volatile storage.		
Specifying Notes			
I7-1/N1	A voltage level detector to detect when to store measurement data is necessary.		
I7-1/N2	The back-up facilities shall include appropriate wake-up facilities in order that the taximeter, including its software, does not get into an indefinite state.		
Required Documentation			
I7-1/D1	A brief description of which data is backed up and when this occurs.		
Examination Guidance			
Checks based on the documentation			
I7-1/C1	Check if the back-up is stored on a non-volatile storage and can if it can be recovered.		
Functional Checks			
I7-1/F1	Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		

8.3.2. Long-term storage

Risk Class B	Risk Class C	Risk Class D
I7-2	There shall be a facility that automatically stores the totalised measurement data if disconnected from power.	
Specifying Notes		
I7-2/N1	The totalized measurement data should normally be stored in non-volatile storage	
I7-2/N2	The facility shall store the totalized measurement data continuously or with an update rate covering the time to detect power down until the (internal) voltage drops below the operating voltage.	
Required Documentation		
I7-2/D1	A brief description of which data is stored and when this occurs.	
Examination Guidance		
Checks based on the documentation:		
I7-2/C1	Check whether all totalized measurement data are saved in case disconnection from power.	
Functional Checks		
I7-2/F1	Confirm correct functioning in the presence of defined influencing quantities and provoked errors.	

8.3.3. Fraudulent alterations

Risk Class B	Risk Class C	Risk Class D
I7-3	There shall be a facility that checks the plausibility of the distance measurement signals.	
Specifying Notes		
I7-3/N1	The facility shall include appropriate routines to check that the pulses or information received are plausible.	
Required Documentation		
I7-3/D1	A brief description of how the routines check the plausibility.	
Examination Guidance		
Checks based on the documentation		
I7-3/C1	Check if the routines check the plausibility and how.	
Functional Checks		
I7-3/F1	Confirm correct functioning in the presence of provoked errors.	

8.4. Examples of legally relevant parameters, functions, and data

In addition to the functions mentioned in 778.2, the following typical parameters of taximeters can be considered.

Parameter	Protected	Settable	Comment
Taximeter constant *k*	x		Impulses per km
Time / date	x	x	
Tariffs (including the parameters for automatic change of tariffs)	x	x	Currency Unit/km, Currency Unit/h
Country/region specific	x	x	Currency Unit, calculation mode S / D, wording/language, etc
Interface parameters		x	Baud-rate, etc

At least the tariffs have to be separately secured.

Also the following data can be considered.

Data	Comment
Interface parameters	Baud-rate, etc
Operation position	'For Hire', 'Hired' or 'Stopped'
Totaliser data	according to point 15.1, (Currency Unit, km, h)
General information	constant of the distance signal generator, (impulses/km) date of securing, (ddmmyyyy) taxi identifier, (license plate number) real time, (hh:mm) identification of the tariff (checksum)
Fare information for a trip	total charged, (Currency Unit) fare, (Currency Unit) calculation of the fare, (Currency Unit, km, h) supplement charge, (Currency Unit) date, (ddmmyyyy) start time, (hh:mm) finish time, (hh:mm) distance travelled (km)
Tariff(s) information	parameters of tariff(s), (Currency Unit/km, Currency Unit/h)

8.5. Assignment of risk class

For the present, according to the result of the WELMEC WG 7 questionnaire (2004) and confirmed by the responsible WELMEC WG12 taximeters, the following risk class shall be applied if software examinations based on this guide are carried out for (software-controlled) taximeters:

- Risk class C for embedded systems
- Risk class D for all other systems and totalisers

The embedded IT system is characterised as follows:

- The software is exclusively constructed for the measuring purpose. Additional functions for securing software and data, for transmitting data and for downloading software are considered constructed for the measuring purpose.
- The user interface is dedicated to the measuring purpose, i.e., it is normally in an operating mode subject to legal control. Switching to an operating mode not subject to legal control is possible.
- An operating system (OS) or subsystems of it may be included
    - if all communication is under control of legally relevant software,
    - it does not allow loading or changing modules, parameters or data or running programs,
    - it does not allow to change the environment of the legally relevant application, etc.
- This includes that the access prevention shall be preset and not the result of a respective subsequent configuration of these components.
- The software environment is invariable and there are no internal or external means for programming or changing the software in its embedded status.
- Software download is allowed if implemented according to this guide, see also generic attack vector IID1.

9. Material Measures

Material measures are subject to regulations in MID. The specific requirements are in Annex MI-008.

Subject to future developments and decisions material measures in the sense of MID Annex MI-008 are not considered to be software-controlled measuring instruments. Thus, for the present, this software guide does not apply to material measures.

10. Dimensional Measuring Instruments

Dimensional Measuring Instruments are subject to regulations in MID. The specific requirements are in Annex MI-009. Neither these specific requirements nor any normative documents have yet been taken into consideration.

Missing clauses will be filled in if considered necessary in the future.

10.1. Assignment of risk class

For the present, according to the result of the WELMEC WG 7 questionnaire (2004) and subject to future decisions of the responsible WELMEC Working Group, the following risk class should be applied if software examinations based on this guide are carried out for (software-controlled) dimensional measuring instruments:

- Risk class B for embedded systems
- Risk class C for all other systems and totalizers

The embedded IT system is characterized as follows:

- The software is exclusively constructed for the measuring purpose. Additional functions for securing software and data, for transmitting data and for downloading software are considered constructed for the measuring purpose.
- The user interface is dedicated to the measuring purpose, i.e., it is normally in an operating mode subject to legal control. Switching to an operating mode not subject to legal control is possible.
- An operating system (OS) or subsystems of it may be included
    - if all communication is under control of legally relevant software,
    - it does not allow loading or changing modules, parameters or data or running programs,
    - it does not allow to change the environment of the legally relevant application, etc.
- This includes that the access prevention shall be preset and not the result of a respective subsequent configuration of these components.
- The software environment is invariable and there are no internal or external means for programming or changing the software in its embedded status.
- Software download is allowed if implemented according to this guide, see also generic attack vector IID1.

11. Exhaust Gas Analyzers

Exhaust Gas Analyzers are subject to regulations in MID. The specific requirements are in Annex MI-010. Neither these specific requirements nor any normative documents have yet been taken into consideration.

Missing clauses will be filled in if considered necessary in the future.

11.1. Assignment of risk class

For the present, according to the result of the WELMEC WG 7 questionnaire (2004) and subject to future decisions of the responsible WELMEC Working Group, the following risk class should be applied if software examinations based on this guide are carried out for (software-controlled) exhaust gas analyzers:

- Risk class B for embedded systems
- Risk class C for all other systems and totalizers

The embedded IT system is characterized as follows:

- The software is exclusively constructed for the measuring purpose. Additional functions for securing software and data, for transmitting data and for downloading software are considered constructed for the measuring purpose.
- The user interface is dedicated to the measuring purpose, i.e., it is normally in an operating mode subject to legal control. Switching to an operating mode not subject to legal control is possible.
- An operating system (OS) or subsystems of it may be included
    - if all communication is under control of legally relevant software,
    - it does not allow loading or changing modules, parameters or data or running programs,
    - it does not allow to change the environment of the legally relevant application, etc.
- This includes that the access prevention shall be preset and not the result of a respective subsequent configuration of these components.
- The software environment is invariable and there are no internal or external means for programming or changing the software in its embedded status.
- Software download is allowed if implemented according to this guide, see also generic attack vector IID1.

Annex IV. Software Examination Template

The software examination template, also applicable to risk assessments in accordance with Guide 7.6, is available as a separate Excel file on the WELMEC website here[9]. This template may be used by manufacturers and examiners alike.

[9] https://www.welmec.org/welmec/documents/guides/7.2/2026/WELMEC_Guide_7.2_2026_Annex_IV_Software_Examination_Template.xlsm

Annex V. Test Report Template

A unified test report template for software examination, also applicable to risk assessments in accordance with Guide 7.6, is available as a separate Excel file on the WELMEC website here[10]. This template may be used by manufacturers and examiners alike.

[10] https://www.welmec.org/welmec/documents/guides/7.2/2026/WELMEC_Guide_7.2_2026_Annex_V_Test_Report_Template.docx

Annex VI. Revision History

No.	Date	Significant Changes
1	June 2026	Guide first issued.