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

WELMEC Guide 7.2

Software Guide

(EU Measuring Instruments Directive 2014/32/EU)

Version 2022

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 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

(Measuring Instruments Directive 2014/32/EU)

Contents

Foreword

The Guide in hand is based on the “Software Requirements and Validation Guide”, Version 1.00, 29 October 2004, developed and delivered by the European Growth Network “*MID-Software”* [1]. The Network was supported from January 2002 to December 2004 by the EU commission under the contract number G7RT-CT-2001-05064.

The Guide is purely advisory and does not itself impose any restrictions or additional technical requirements beyond those contained in the Measuring Instruments Directive (MID) [2]. Alternative approaches may be acceptable, but the guidance provided in this document represents the considered view of WELMEC as to a good practice to be followed.

Although the Guide is oriented on instruments included in the regulations of the MID, the results are of a general nature and may be applied beyond.

The issue 6 considers the latest experience gained from the applications of the Guide.

[1]**Please note**: This issue of the guide remains also valid for Directive 2004/22/EC [3].

Introduction

This document provides technical guidance for the application of the Measuring Instruments Directive (MID) [2], for software-equipped measuring instruments. It addresses all those who are interested in the technical understanding of software-related requirements of the MID, in particular of the essential requirements in annex 1 of the MID. The level of detailedness is oriented on the needs of manufacturers of measuring instruments and of notified bodies (NB) which perform conformity assessments of measuring instruments according to module B.

By following the Guide, a compliance with the software-related requirements of the MID can be assumed. It can be further assumed that all notified bodies accept this Guide as a compliant interpretation of the MID with respect to software. To show how the requirements set up in this Guide are related to the respective requirements in the MID, a cross reference has been included in this guide as an annex (Chapter 13).

Latest information relating to the Guides and the work of WELMEC Working Group 7 is available on the web site www.welmec.org.

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.

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.

Authentication: Verification of the declared or alleged identity of a user, process, or device.

Authenticity: Property of being genuine and able to be verified and be trusted [4].

Basic configuration: Design of the *measuring instrument* with respect to the basic architecture. There are two different basic configurations*: built-for-purpose measuring instruments* and *measuring instruments using a universal device.* The terms are accordingly applicable to *sub-assemblies*.

Built-for-purpose measuring instrument (type P): A *measuring instrument* designed and built specially for the task in hand. Accordingly, the entire application software is constructed for the measuring purpose. For a more detailed definition refer to sub-chapter 4.1.

Category 1 component: components that are part of the measuring process i.e. that handle measurement data to construct the measurement result including the primary indicator device

Category 2 component: components that further process the measurement result without modification to finalize the transaction

Closed network: A network of a fixed number of participants with a known identity, functionality, and location (see also *Open network*).

Communication interface: An electronic, optical, radio or other technical interface that enables information to be automatically passed between parts of *measuring instruments, sub-assemblies*, or external devices.

Component: identifiable part of an instrument that performs a specific function or functions, and that can be separately evaluated according to specific metrological and technical performance requirements

Device-specific parameter: *Legally relevant parameter* with a value that depends on the individual instrument. Device-specific parameters comprise calibration parameters (e.g. span adjustment or other adjustments or corrections) and configuration parameters (e.g. maximum value, minimum value, units of measurement, etc). They are adjustable or selectable only in a special operational mode of the instrument. Device-specific parameters may be classified as those that should be secured (unalterable) and those that may be accessed (settable parameters) when the instrument is in use.

Event counter: An event counter registers each change of a parameter value. It serves as a means to supervise changes.

Event logger: An event logger registers each change of software or parameters. It serves as a means to supervise changes. It registers at least the identifier of the changed item.

Integrated storage: non-removable storage that is part of the measuring instrument, e.g. RAM, EEPROM, hard disk.

Integrity of data and software: Assurance that the data and software have not been subjected to any changes while in use, transfer or storage.

IT configuration: Design of the *measuring instrument* with respect to IT functions and features. There are four IT configurations considered in this guide: *long-term storage of measurement data*, *transmission of measurement data*, *software download* and *software separation* (see also *Basic configuration*). The terms are accordingly applicable to *sub-assemblies*.

Legally relevant parameter: Parameter of a *measuring instrument* or *a sub-assembly* subject to legal control. The following types of legally relevant parameters can be distinguished: *type-specific parameters and device-specific parameters.*

Legally relevant software: Part of software including type-specific *parameters* that fulfils functions, which are subject to legal control. All other software is called legally non-relevant. Measurement data generated by the instrument or processed by legally relevant software is separately treated and not considered a part of legally relevant software.

Legally relevant software identifier: Identifiers of the legally relevant software are called the *legally relevant software identifiers*

Long-term storage of measurement data: Storage used for keeping measurement data available after completion of the measurement for later legally relevant purposes

Measurement data: Legally relevant measurement values generated or processed by measuring instruments and accompanied by physical units and other information, e.g. time stamps, that is connected to them on a regular basis that characterise them metrologically.

Measuring instrument: Any device or system with a measurement function. The adjective “measuring” is omitted if confusions can be excluded. [2]

Measuring instruments using a universal device (type U): *Measuring instrument* that comprises a general-purpose computer, usually a PC-based system, for performing legally relevant functions. A type U system is assumed if the conditions of a *built-for-purpose measuring instrument (type P)* are not fulfilled.

Open network: A network of arbitrary participants (devices with arbitrary functions). The number, identity and location of a participant can be dynamic and unknown to the other participants (see also *Closed network*).

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, and file management in a computer system [5].

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: For category 1 components or complete measuring instruments the legally relevant parts of the operating system, usually, at least consist of the boot loader, the kernel, the interfaces (hardware and inter-process communication), the (background) services, administration of user privileges, cryptographic libraries as well as the configuration files of those parts.
Note 3: For category 2 components the legally relevant parts of the operating system, usually, at least consist of the interfaces (hardware and inter-process communication),

administration of user privileges, cryptographic libraries as well as the configuration files of those parts.

Protective Software Interface: Interface between the legally relevant and legally non-relevant software, for protection conditions see requirement S3.

Risk class: Class of *measuring instrument* types with almost identical risk assessments.

Sealing: Means intended to protect the measuring instrument against any modification, readjustment, removal of parts or software, etc.

Securing: Means preventing unauthorized access to hardware or software.

Software download: The process of automatically transferring software to a target *measuring instrument* or hardware-unit 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).

Software identifier: A sequence of characters, that identifies the software. The identifier is logically considered a part of the software.

Software protection: Protection of measuring instrument software or data domain by a hardware or software implemented seal with the intention of making an intervention impossible or evident.

Software separation: The unambiguous separation of software into *legally relevant software* and legally non-relevant software. If no software separation exists, the whole software is to be considered as legally relevant.

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 [MID, Article 4].

Transmission of measurement data: Transmission of measurement data via communication networks or other means to a distant device where they are further processed and/or used for legally regulated purposes.

TEC: Type examination certificate.

Type-specific parameter: *Legally relevant parameter* with a value that is equal for all instruments of the type. A type-specific parameter is considered a part of the legally relevant software.

User interface: An interface forming the part of the instrument or measuring system that enables information to be passed between a human user and the measuring instrument or its hardware or software parts, as, e.g., switch, keyboard, mouse, display, monitor, printer, touchscreen.

Validation: Confirmation by examination and provision of objective evidence (i.e., information that can be proved true, based on facts obtained from observations, measurement, test, etc.) that the particular requirements for the intended use are fulfilled. In the present case the related requirements are those of the MID [2].

The following definitions are rather specific. They are only used in some extensions and for risk class D or above.

Hash algorithm: Algorithm that compresses the contents of a data block to a hexadecimal number of defined length (hash code), so that the change of any bit of the data block leads in practice to another hash code. Hash algorithms are selected such that there is theoretically a very low probability of two different data blocks having the same hash code.

Signature algorithm: A cryptographic algorithm that encrypts (encodes) a hash code using an encoding *key* and that allows decoding of the encrypted hash code if the corresponding *decoding key* is available.

Key: An appropriate number or sequence of characters used to encode and / or decode information.

Public Key System (PKS): A pair of two different *keys*, one called the secret key and the other the public key. To verify *integrity* and *authenticit*y of information, the hash value of the information generated by a *hash algorithm* is encrypted with the secret key of the sender to create the signature, which is decrypted later by the receiver using the sender's public key.

Public Key Infrastructure (PKI): Organisation to guarantee the trustworthiness of a *public key system*. This includes granting and distributing digital certificates to all members that take part in the information exchange.

Certification of keys: The process of binding a public key value to an individual, organisation or other entity.

Electronic signature: A short code (the signature) that is unambiguously assigned to a text, data block or binary software file to prove the *integrity* and *authenticity* of data stored or transmitted. The signature is created using a *signature algorithm* and a secret *key.* Usually, the generation of an electronic signature is composed of two steps: (1) first a *hash algorithm* compresses the contents of the information to be signed to a short value, and (2) then a signature algorithm combines this number with the secret key to generate the signature.

Trust Centre: An association that trustworthily generates, keeps, and issues information about the authenticity of public keys of persons or other entities, e.g., measuring instruments.

2 How to use this guide

This chapter describes the organisation of the guide and explains how to use it.

2.1 Overall structure of the guide

The guide is organised as a structured set of requirement blocks. The overall structure of the guide follows the classification of measuring instruments into basic configurations and the classification of so-called IT configurations. The set of requirements is complemented by instrument-specific requirements.

Consequently, there are three types of requirement sets:

1. requirements for two basic configurations of measuring instruments (called type P and U),
2. requirements for four IT configurations (called extensions L, T, S and D)
3. instrument-specific requirements (called extensions I.1, I.2, …).

The first type of requirements is applicable to all instruments. The second type of requirements concerns the following IT functions: long-term storage of measurement data (L), transmission of measurement data (T), software download (D) and software separation (S). Each set of these requirements is only applicable if the corresponding function exists. The last type is a collection of further, instrument-specific requirements. The numbering follows the numbering of instrument-specific annexes in the MID [2]. The set of requirements blocks that may be applied to a given measuring instrument is schematically shown in **Figure 2-1**.

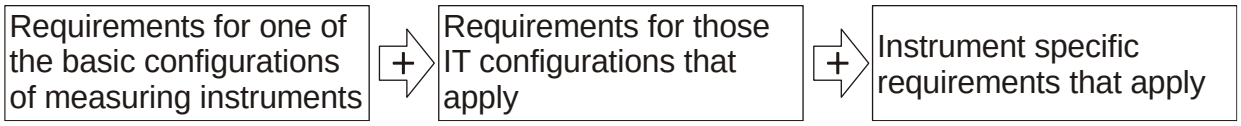

Figure 2-1: Type of requirement sets that should be applied to an instrument

The schemes in the following **Figure 2-2** show what sets of requirements exist.

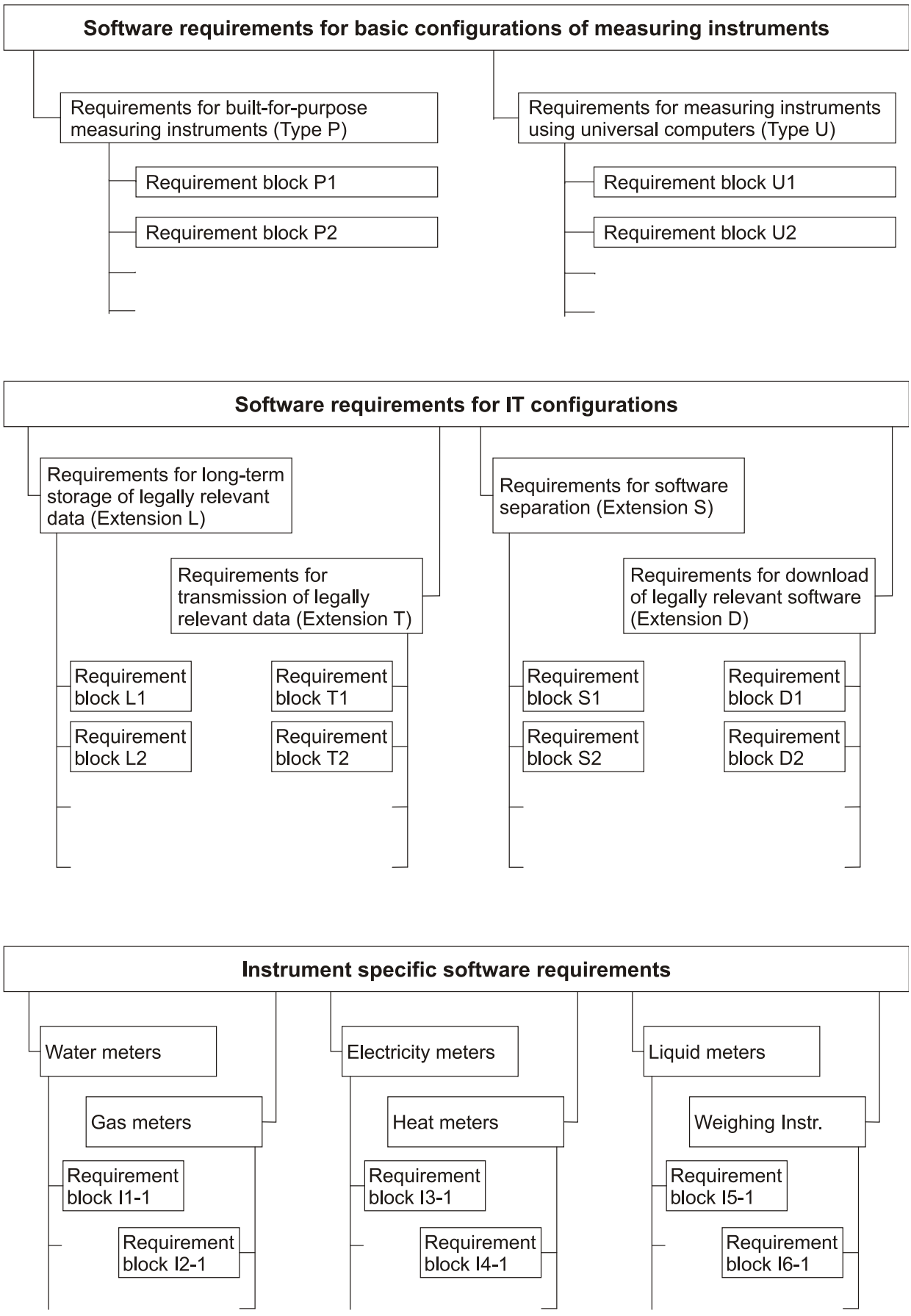

Figure 2-2: Overview of requirement sets

In addition to the structure described, the requirements of this guide are differentiated according to risk classes. Six risk classes, numbered from A to F with increasing risk assumptions, are introduced. The lowest risk class A and the highest risk classes E and F are not used for instruments under MID regulation, for the present. They are place-holders for the eventual case, that they will become necessary in future. The remaining risk classes B to D cover all of the instrument classes falling under the regulation of MID. Moreover, the risk classes from A to F provide a sufficient window of opportunity for the case of changing risk evaluations. The classes are defined in Chapter 3 of this guide.

Each measuring instrument shall be assigned to a risk class because the particular software requirements to be applied are governed by the risk class the instrument belongs to.

2.2 How to select the appropriate parts of the guide

This comprehensive software guide is applicable to a large variety of instruments. The guide is modular in form. The appropriate requirement sets can be easily selected by observing the following procedure.

Step 1: *Selection of the basic configuration (P or U)*

Only one of the two sets of requirements for basic configurations needs to be applied. Decide which basic configuration the instrument conforms to: a built-for-purpose instrument with embedded software (type P, see sub-chapter 4.1) or an instrument using a universal device (type U, see sub-chapter 5.1). If type U is selected and the instrument is equipped with a legally relevant operating system, i.e. the operating system is used to fulfil the essential requirements of the MID or can be used to affect compliance with requirements, the extension for operating systems (O) shall be applied simultaneously. If extension O is not applicable because the prerequisites laid down in the extension do not apply the entire software of the instrument shall be treated as type P. If only a sub-assembly or component of the instrument is the matter of concern, then decide accordingly for the sub-assembly or component. Always apply the complete set of requirements that belongs to the respective basic configuration and extension O respectively.

Step 2: *Selection of applicable IT configurations (extensions L, T, S and D)*

The IT configurations comprise: long term storage of measurement data (L), transmission of measurement data (T), software separation (S) and download of legally relevant software (D). The corresponding requirement sets, called modular extensions, are independent of each other. The sets selected depend only on the IT configuration. If an extension set is selected, then it shall be applied in full. Decide which, if any, of the modular extensions are applicable and apply them accordingly (Figure 2-2).

Step 3: *Selection of instrument-specific requirements (extension I)*

If applicable, select a respective instrument-specific extension Ix, and apply the instrument-specific requirements accordingly (see Figure 2-2).

Step 4: *Selection of the applicable risk class (extension I)*

Select the risk class as defined in the respective instrument-specific extension Ix, sub-chapter I.x.6. There, the risk class is defined uniformly for a class of measuring instruments or possibly further differentiated for categories, fields of application, etc. Once the applicable risk class has been identified, only the respective requirements and validation guidance need to be considered.

2.3 How to work with a requirement block

Each requirement block contains a well-defined requirement. It consists of a defining text, explanatory specifying notes, the documentation to be provided, the validation guidance and examples of acceptable solutions (if available). The content within a requirement block may be subdivided according to risk classes. This leads to the schematic presentation of a requirement block shown in **Figure 2-3**.

<table>
<tr><td colspan="3">Title of the requirement</td></tr>
<tr><td colspan="3">Main statement of the requirement</td></tr>
<tr><td colspan="3">Specifying notes (scope of application, additional explanations, exceptional cases, etc.)</td></tr>
<tr><td colspan="3">Documentation to be provided (eventually differentiated between risk classes)</td></tr>
<tr><td>Validation guidance for one risk class</td><td>Validation guidance for another risk class</td><td>...</td></tr>
<tr><td>Example of an acceptable solution for one risk class</td><td>Example of an acceptable solution for another risk class</td><td>...</td></tr>
</table>

Figure 2-3: Structure of a requirement block

The requirement block represents the technical content of the requirement including the validation guidance. It addresses both the manufacturer and the notified body in two directions: (1) to consider the requirement as a minimal condition, and (2) not to put demands beyond this requirement.

Notes for the manufacturer:

- Observe the main statement and the additional specifying notes.
- Provide documentation as required.
- Acceptable solutions are examples that comply with the requirement. There is no obligation to follow them.
- The validation guidance has an informative character.

Notes for notified bodies:

- Observe the main statement and the additional specifying notes.
- Follow the validation guidance.
- Confirm the completeness of the documentation provided.

2.4 How to work with the checklists

Checklists are means of ensuring that all the requirements within a chapter have been covered by the manufacturer or examiner. They are part of the test report. Be aware, the checklists are only of a summarising nature, and they do not distinguish between risk classes. Checklists do not replace the requirement definitions. Refer to the requirement blocks for complete descriptions.

Procedure:

- Gather the checklists, which are necessary according to the selection described in steps 1, 2 and 3 in sub-chapter 2.2.
- Go through the checklists and prove whether all requirements have been met.
- Fill in the checklists as required.

3 Definition of Risk Classes

3.1 General principle

The specific requirements of this guide are differentiated according to (software) risk classes. In this guide, risks are related to software of the measuring instrument and not to any other component. For convenience reasons, the shorter term “risk class” is used. Each measuring instrument shall be assigned to a risk class because the specific software requirements to be applied are tailored to the risk class the instrument belongs to.

Software risks in measuring instruments addressed by this guide are mainly caused by three risk factors: inadequate protection of software, inadequate examination of software, and non-conformity to type. A risk class is a combination of levels of these three risk factors where the definition of levels of the risk factors is indirectly made by definition of levels for the correspondingly necessary counteractions. Three levels of counteractions, low, middle and high, are introduced for each of the risk factors. The higher the risk is assumed, the higher the level of counteraction is taken.

3.2 Description of levels of counteractions for the risk factors

The following definitions are used for the corresponding levels.

Software protection levels

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

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

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

Software examination levels

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

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

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

Software conformity levels

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

Middle: In addition to the conformity level “low”, the binary code of legally relevant software of individual instruments is identical to the software of the type under examination (or re-examination). Software separation is allowed if the restrictions in part S of this guide (chapter 8) are fulfilled.

High: The binary code of the complete software implemented in the individual instruments is identical to the software of the type under examination. Software separation is not anymore relevant.

3.3 Derivation of risk classes

Out of the 27 theoretically possible level combinations, only 3 or at the utmost 6 are of practical interest (risk classes B, C, D and eventually A, E and F). They cover all of the instrument classes falling under the regulation of MID. Moreover, they provide a sufficient window of opportunity for the case of changing risk evaluations. The classes are defined in the table below. The table shall be interpreted in a way that a certain risk class is defined by the corresponding combination of levels of necessary counteractions.

Risk Class	Software Protection	Software Examination	Software Conformity
A	*low*	*Low*	*low*
B	*middle*	*Middle*	*low*
C	*middle*	*Middle*	*middle*
D	*high*	*Middle*	*middle*
E	*high*	*High*	*middle*
F	*high*	*High*	*high*

Table 3-1: *Definition of risk classes*

3.4 Interpretation of risk classes

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

Risk class B: In comparison to risk class A, the protection of software is required on the middle level. Correspondingly, the examination level is raised to the

middle level. The conformity remains unchanged in comparison to risk class A.

The software examination is carried out on the basis of the documentation. In the consequence, the TEC allows different implementations with respect to the same documentation when putting the instruments into market[1].

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

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

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

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

[1] After having put the instrument into market, the allowance for changing software depends on national regulations.

4 Basic Requirements for Embedded Software in a Built-for-purpose Measuring Instrument (Type P)

The set of specific requirements of this chapter are valid for built-for-purpose instruments as well as for sub-assemblies and for parts according to WELMEC Guide 8.8 (Modular Evaluation of Measuring instruments) that are of the built-for-purpose type. The validity for sub-assemblies and parts is included even if it is not repeatedly mentioned in the following text. The conditions, however, under which sub-assemblies and parts may be separately examined and the corresponding certificates may be accepted, are not part of this guide.
If the measuring instrument uses a universal device (general-purpose PC), the set of specific requirements in chapter 5 shall be referred to (type U instrument). The specific requirements of type U instruments shall always be used if at least one of the subsequent technical characteristics of built-for-purpose instruments is not matched.

4.1 Technical Description

A type P instrument is a measuring instrument with an embedded IT system (e.g., a microprocessor or microcontroller-based system). *All components of the IT system used are open for evaluation.*

The embedded IT system is characterised in particular 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 programs, parameters or data or running programs,
  - if 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 the specific requirements of extension D (chapter 9) are observed.

4.2 Specific Requirements for Type P

Risk Classes B to E
P1: Documentation *In addition to the specific documentation required in each of the following requirements, the documentation shall basically include:* *a. A description of the legally relevant software.* *b. A description of the accuracy of the measuring algorithms (e.g. price calculation and rounding algorithms).* *c. A description of the user interface, menus and dialogues.* *d. The software identifier(s) of the legally relevant software.* *e. An overview of the system hardware, e.g., topology block diagram, type of computer(s), type of network.* *f. The operating manual.*

Risk Class B	Risk Class C	Risk Class D
P2: Software identification *The legally relevant software shall be clearly identified. The identifier(s) shall be permanently presented by the instrument or presented on command or during operation.*		
Specifying Notes: 1. Legally relevant software identifiers may be independent or part of well-structured identifiers. In the second case, the legally relevant software identifier(s) shall be clearly distinguishable. 2. If different software versions are valid implementations of the same type (e.g., for instruments in risk class B), then the legally relevant software identifier(s) shall be unique for each version 3. The legally relevant software identifiers are type-specific parameters. 4. The legally relevant software identifiers shall be easily presented without requiring an additional tool. 5. The identifier(s) shall be displayed permanently on a secured plate, on command or on start-up.		
Required Documentation: 1. The documentation shall list the software identifier(s) and describe how they are created, how they are secured, how they are presented and how they are structured in order to differentiate between legally relevant software identifiers and others as well as to assess the uniqueness. 2. The documentation shall list which legally relevant software part is covered by which legally relevant software identifier.		
Validation Guidance: *Checks based on documentation:* • Check whether legally relevant software identifiers are given in the documentation. • Check whether the software performing legally relevant functions is clearly described so that it is reproducible which legally relevant software part is covered by which legally relevant software identifier. • Examine the description of the visualisation of the legally relevant software identifiers. • Check whether all legally relevant software identifiers are unique (in particular in cases of re-examinations). *Functional Checks:* • Check that the legally relevant software identifiers can be visualised as described in the documentation. • Check that the legally relevant software identifier(s) presented are identical to the identifiers given in the documentation. • The legally relevant software identifier(s) are distinguishable from other identifiers.		
Example of an Acceptable Solution: a) a checksum over code. b) any string, possibly added by a version number, c) any string of numbers, letters, other characters, • If the manufacturer chooses a mixed identifier for legally relevant and legally non-relevant software, a simple solution that allows distinguishing the identifiers is using placeholders in the TEC, e.g. “abc1.xx” with “abc1” for the legally relevant software and “xx” as placeholder for legally non-relevant software. .		

Additions for Risk Class E
Required Documentation Identical to risk classes B to D.
Validation Guidance Identical to risk classes B to D.

Risk Class B	Risk Class C	Risk Class D
P3: Influence via user interfaces *Commands entered via the user interfaces shall not inadmissibly influence the legally relevant software*, device-specific parameters *and measurement data.*		
Specifying Notes: 1. There shall be an unambiguous assignment of each command to an initiated function or data change. 2. Commands that are not documented shall have no effect on legally relevant functions, device-specific parameters and measurement data. 3. The respective parts of the software that interpret commands are considered to be legally relevant software.		
Required Documentation: If the instrument has the ability to receive commands, the documentation shall include: • Description of commands and their effect on legally relevant software, device-specific parameters and measurement data. • Description of how the legally relevant software, device-specific parameters and measurement data are protected from being influenced by other inputs.		
Validation Guidance: *Checks based on documentation:* • Check that documented commands are admissible, i.e., that they have an allowed influence on the legally relevant software, device-specific parameters and measurement data). • Check the protection measures against influences from other inputs. *Functional Checks:* • Carry out practical tests (spot checks) with documented commands. • Check whether there are undocumented commands.		
Example of an Acceptable Solution: There is a software module that receives and interprets commands from the user interface. This module belongs to the legally relevant software. It forwards only allowed commands to the other legally relevant software modules. All unknown or not allowed sequences of switch or key actuations are rejected and have no impact on the legally relevant software, device-specific parameters and measurement data.		

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes B to D)**:** Source code of the legally relevant software.
Validation Guidance (in addition to the guidance for risk classes B to D)**:** *Checks based on the source code:* • Check the software design whether data flow concerning commands is unambiguously defined and realised only in the legally relevant software. • Search inadmissible data flow from the user interface to domains to be protected. • Check with tools or manually that commands are decoded correctly. • Check the code for undocumented commands.

Risk Class B	Risk Class C	Risk Class D

P4: Influence via communication interfaces

Commands input via communication interfaces of the instrument shall not inadmissibly influence the legally relevant software, device-specific parameters *and measurement data.*

Specifying Notes:

1. There shall be an unambiguous assignment of each command to an initiated function or data change.
2. Commands that are not documented shall have no effect on legally relevant functions, device-specific parameters and measurement data.
3. The respective parts of the software that interpret commands are considered to be legally relevant software.
4. Interfaces that allow commands with inadmissible effects on the legally relevant software, device-specific parameters and measurement data shall be sealed or protected in another appropriate way. This also applies for interfaces that cannot be completely assessed.
5. This special requirement does not apply to software download according to Extension D.

Required Documentation:

If the instrument has an interface, the documentation shall include:

- Description of commands and their effect on the legally relevant software, device-specific parameters and measurement data.
- Description of how the legally relevant software, device-specific parameters and measurement data are protected from being influenced by other inputs.

Validation Guidance:

Checks based on documentation:

- Check that documented commands are admissible, i.e., that they have an allowed influence on the legally relevant software, device-specific parameters and measurement data).
- Check the protection measures against influences from other inputs.

Functional checks:

- Carry out practical tests (spot checks) using peripheral equipment.

Example of an Acceptable Solution:

There is a software module that receives and interprets data from the interface. This module is part of the legally relevant software. It forwards only allowed commands to the other legally relevant software modules. All unknown or not allowed signal or code sequences are rejected and have no impact on the legally relevant software, device-specific parameters and measurement data.

Additions for Risk Classes E

Required Documentation (in addition to the documentation required for risk classes B to D)**:**

Source code of the legally relevant software.

Validation Guidance (in addition to the guidance for risk classes B to D)**:**

Checks based on the source code:

- Check the software design whether data flow concerning commands is unambiguously defined in the legally relevant software and can be verified.
- Search inadmissible data flow from the interface to domains to be protected.
- Check with tools or manually that commands are decoded correctly.
- Check the code for undocumented commands.

Risk Class B	Risk Class C	Risk Class D

P5: Protection against accidental or unintentional changes

Legally relevant software and device-specific parameters shall be protected against accidental or unintentional changes.

Specifying Notes:

1. The software shall be capable to detect changes caused by physical effects (electromagnetic interference, temperature, vibration, etc).
2. Means shall be implemented to protect from unintentional misuse of the user interfaces.

Required Documentation:

1. The documentation should show the measures that have been taken to detect and protect the legally relevant software and device-specific parameters from unintentional changes.

Validation Guidance:

Checks based on documentation:

- Check that measures against unintentional changes are described and appropriate.

Functional checks:

- Practical spot checks to show that a warning is given before deleting measurement data, if deleting is possible at all.

Example of an Acceptable Solution:

- The accidental modification of legally relevant software and device-specific parameters is checked by periodically calculating checksum(s) and automatically comparing them with deposited nominal value(s). If the comparison does not match, reactions are necessary that are adequate for the instrument (e.g., stop of measurement, corresponding indication of measurement data, see chapter 10 for eventual recommendations).
- Alternative methods are possible if the change status of software can be identified by them.
- For fault detection see Extension I (chapter 10).

Additions for Risk Class E

Required Documentation (in addition to the documentation required for risk classes C and D):
Source code of the legally relevant software.

Validation Guidance (in addition to the guidance for risk classes C and D)**:**

Checks based on the source code:

- Check whether measures taken for detection of changes are appropriate.
- Check whether all parts of the legally relevant software and all device-specific parameters are covered by the checksum.

<table>
<tr><th>Risk Class B</th><th>Risk Class C</th><th>Risk Class D</th></tr>
<tr><td colspan="3">P6: Protection against inadmissible intentional changes
Legally relevant software and measurement data shall be secured against inadmissible intentional modification, loading or swapping of hardware memory.</td></tr>
<tr><td colspan="3">Specifying Notes:
1. For protection against manipulation using the user interface, see P3.
2. For protection against manipulation using communication interfaces, see P4.
3. Measurement data are already considered to be sufficiently protected, if only legally relevant software processes them (e.g. in memory or registers).</td></tr>
<tr><td colspan="2"></td><td>Specifying Notes:
4. A checksum or an alternative method with the same level of protection shall be provided in order to support the detection of software modifications.
5. The calculated checksum or an alternative indication of software modification shall be made visible on command for control purposes.
6. The checksum or the alternative indication is calculated over the legally relevant software. The software that organizes the generation of checksums or alternative indications is part of the legally relevant software.
7. If a checksum is used, the algorithm shall have a key length of at least 4 bytes; (See also Extensions L and T).</td></tr>
<tr><td colspan="3">Required Documentation:
The documentation shall describe the protection methods.</td></tr>
<tr><td colspan="3">• Description of measures that have been taken to protect the software and device-specific parameters, in particular the method of checksum calculation and nominal checksums or alternative methods with the corresponding nominal indication.
• Description of methods to prevent exchange of the memory that contains the software
• Description of programming mode and its disabling, if applicable</td></tr>
<tr><td colspan="3">Validation Guidance:
Checks based on documentation:
• Examine whether the documented means of securing against unauthorised exchange of the memory that contains the software are sufficient.
• Check that the checksum(s) or alternative indication(s) cover the legally relevant software.

Functional checks:
• Test practically the programming mode and check whether disabling works.
• Compare calculated checksums or alternative indications with the nominal values.</td></tr>
<tr><td colspan="2">Example of an acceptable Solution:
a) To prevent from removing and replacing physical memory, the housing of the instrument or the physical memory itself is secured against unauthorised removal.
b) The instrument is sealed, and the interfaces comply with the requirements P3 and P4.</td><td>Example of an acceptable Solution: (in addition to a) and b))
c) Program code is protected by means of checksums. The program calculates its own checksum and compares it with a desired value that is hidden in the executable code. If the self-check fails, the program is blocked. A CRC-32 checksum with a secret initial vector (hidden in the executable code) is used.</td></tr>
</table>

Additions for Risk Classes E
Required Documentation (in addition to the documentation required for risk classes B to D)**:** Source code of the legally relevant software

Validation Guidance (in addition to the guidance for risk classes B to D)**:**

Checks based on the source code:

- Check whether measures taken for the detection of intentional changes are appropriate.

Risk Class B	Risk Class C	Risk Class D
P7: Parameters protection *Device-specific parameters shall be secured against inadmissible modification.*		
Specifying Notes: 1. In normal secured operating mode, device-specific parameters shall not be alterable anymore. They shall only be adjustable in a special operating mode of the instrument. 2. There may be device-specific parameters that are allowed to remain unsecured. See extension I for instrument-specific parameters.		
Required Documentation: The documentation shall describe the device-specific parameters, whether they may be set and how they are set and how they are secured.		
Validation Guidance: *Checks based on documentation:* • Check that changing or adjusting of device-specific parameters is impossible after securing. • Check that all relevant device-specific parameters (given in Extension I, if any) are secured. *Functional checks:* • Test the adjusting (configuration) mode and check whether disabling after securing works. • Examine the classification and state of parameters (secured/settable) at the display of the instrument, if a suitable menu item is provided.		
Example of an Acceptable Solution: a) Device-specific Parameters are secured by sealing the instrument or memory housing and disabling the write enable/disable input of the memory circuit by an associated jumper or switch, which is sealed.		
b) *Event counter / event logger:* • An **event counter** registers each change of a device-specific parameter value. The current count can be displayed and can be compared with the initial value of the counter that was registered before putting the measuring instrument into use or at the last official verification respectively and is indelibly labelled on the instrument. • Changes of device-specific parameters are registered in an **event logger**. It is an information record stored in a non-volatile memory. Each entry is generated automatically by the legally relevant software and contains: o the identifier of the parameter (e.g. the name) o the parameter value (the current or the value before) o the time stamp of the change • The event logger cannot be deleted or be changed without destroying a seal. The content of the event logger is shown on the display or printed upon command.		÷

Additions for Risk Classes E
Required Documentation (in addition to the documentation required for risk classes B to D)**:** Source code of the legally relevant software showing the way of securing and viewing legally relevant parameters.
Validation Guidance (in addition to the guidance for risk classes B to D)**:** *Checks based on the source code:* • Check code whether measures taken for protecting device-specific parameters are appropriate (e.g., adjusting mode disabled after securing).

Risk Class C	Risk Class D

P8: Authentication presented of measurement data
The authenticity of the measurement data that are presented shall be guaranteed.

Specifying Notes:

1. Presented measurement data are considered authentic if the presentation is issued from within the legally relevant software.
2. It shall not be possible to fraudulently simulate (spoof) legally relevant software for presenting measurement data.
3. Presented measurement data shall be comprehensible and clearly distinguishable from other, legally non-relevant information. If necessary, additional explanation shall be given.
4. If the source of the presented measurement data (e.g., a sensor) is not implicitly identifiable or verifiable (e.g. if there is more than one sensor or if the sensor is remotely connected), the instrument shall supply the identification of the respective source. The unique identifier of the approved data source is a legally relevant parameter covered by P6/U6 or P7/U7. Depending on the type of the data link, Extension T may need to be applied.

Required Documentation:

- The documentation should describe how authenticity of the measurement data is guaranteed.

Validation Guidance:

Checks based on documentation:

- Check that presented measurement data is generated by legally relevant software.
- Check that the presentation of measurement data can only be performed by legally relevant software.
- If the source of the presented measurement data is not implicitly identifiable or verifiable, check that the source of these data is identified and indicated by the legally relevant software.

Functional checks:

- Check that the meaning of all presented legally relevant measurement data is clear and that they are distinguishable from each other.
- Check through visual control if the presentation of measurement data is easily distinguishable from other information that may also be presented.
- If applicable, check through visual control that the presented measurement data are accompanied by all necessary information.

Example of an Acceptable Solution:

1. A measurement application is generated by the legally relevant software. The technical measures required of the application are:
   - No access to measurement data is given to legally non-relevant programs until the measurement data have been indicated.
   - The application is refreshed periodically. The associated program checks that the application is visible as long as the measurement is not concluded. Processing of measurement values stops whenever this application is closed or not completely visible.

2a The sensor unit encrypts the measuring values with a key known to the authentic software running on the built-for-purpose device (its version number). Only the authentic software can decrypt and use the measurement values, non-authentic programs on the measuring instrument cannot as they do not know the key. For key treatment see Extension T.

2b Before sending measurement values the sensor initiates a handshake sequence with the legally relevant software on the built-for-purpose device based on secret keys. Only if the program on the built-for-purpose device communicates correctly, the sensor unit sends its measurement values. For key treatment see Extension T.

3. The key used in 2a / 2b is chosen and entered to the sensor unit and software on the built-for-purpose device without destroying a seal.	3. The key is chosen and entered in the sensor unit and in the software on the built-for-purpose device only when a seal is destroyed.

4. If the presented measurement data are not explicitly linked to a sensor, the originating sensor transmits its data together with a unique identification of the sensor itself. All presented measurement data are labelled with the identification of the individual sensor. The identification of each sensor is a legally relevant parameter shown on the sensor housing.

Additions for Risk Class E

Required Documentation (in addition to the documentation required for risk classes C to D)**:**
Source code of the legally relevant software.

Validation Guidance (in addition to the guidance for risk classes C to D)**:**

Checks based on the source code:

- Check that legally relevant software generates the presented measurement data.
- Check whether all measures taken are correct to guarantee the presentation of measurement results by legally relevant software.

5 Basic Requirements for Software of Measuring Instruments using a Universal Device (Type U)

The set of specific requirements of this chapter is valid for measuring instruments based on a general-purpose computer as well as for sub-assemblies and for parts according to WELMEC guide 8.8 that uses universal device. The validity for sub-assemblies and parts is included even if it is not repeatedly mentioned in the following text. The conditions, however, under which sub-assemblies and parts may be separately examined and the corresponding certificates may be accepted, are not part of this guide.

5.1 Technical Description

A type U measuring system is typically characterised by the following configurations.

Hardware Configuration

a) A modular general-purpose computer-based system. The computer system may be stand-alone, part of a closed network, e.g. Ethernet, token-ring LAN, or part of an open network, e.g. Internet.

b) Because the system is general purpose, the sensor is normally external to the computer unit and linked to it by a communication connection.

c) The user interface offers further functions, which are not under legal control, besides the operating mode for the measurement task.

d) Storage may be fixed, e.g., hard disk, or removable, e.g., USB, or remote.

Software Configuration

e) Usually, an operating system is used.

f) In addition to the measuring instrument application, other software applications may also reside on the system at the same time.

In addition to configurations described above, a type U system shall also be assumed if the characteristics of a type P instrument (see sub-chapter 4.1) are not completely fulfilled.

Consequences for risk classification

The software of type U instruments is much more openly accessible than the software of type P instruments. The protection of software integrity shall be enhanced in comparison to type P instruments. In particular, a checksum or an equivalent means shall be required to support integrity checks of the software code. The consequence is that the conformity level “low” (only functional correspondence of the software to the technical documentation of the type under examination) is not an adequate means for ensuring software integrity. This means risk class C is the lowest possible risk class instruments of the U type may be allocated to.

5.2 Specific Software Requirements for Type U

Risk Classes C to E

U1: Documentation

In addition to the specific documentation required in each requirement below, the documentation shall basically include:

a. *A description of the legally relevant software functions, meaning of the data, etc.*
b. *A description of the accuracy of the measuring algorithms (e.g. price calculation and rounding algorithms).*
c. *A description of the user interface, menus and dialogues.*
d. *The software identifier(s) of the legally relevant software .*
e. *An overview of the system hardware, e.g., topology block diagram, type of computer(s), type of network*
f. *Regarding the documentation of the configuration of the operating system, see Extension O.*
g. *The operating manual.*

Risk Class C and D

U2: Software identification

The legally relevant software shall be clearly identified. The identifier(s) *shall be permanently presented by the instrument, presented on command or during operation.*

Specifying Notes:

1. Legally relevant software identifier(s) may be independent or part of well-structured identifiers.
2. In the case that a legally relevant software identifier is embedded in an overall identifier, it shall be clearly distinguishable.
3. The legally relevant identifier(s) shall be unique for each legally relevant software an instrument is equipped with.
4. The legally relevant identifiers shall be easily presented without requiring an additional tool.
5. For the identification of operating system parts, see O6. These specifying notes apply in conjunction with O6 to the identification of the operating system.
6. The legally relevant software identifier(s) are type-specific parameters and shall be protected as such (see U5 and U6). If the identifiers are not inextricably linked to the software itself, other securing means are required.
7. The identifier(s) shall be displayed permanently, on command or on start-up.

Required Documentation:

The documentation shall list the software identifiers and describe how they are created, how they are secured, how they are presented and, if applicable, how they are structured in order to differentiate between legally relevant identifiers and others.

Validation Guidance:

Checks based on documentation:

- Check whether legally relevant software identifiers are given in the documentation.
- Check whether the software performing the legally relevant tasks is clearly described so that it is reproducible which software part is covered by which software identifier.
- Examine the description of generation and visualisation of identifiers.
- Check whether all legally relevant software identifiers are unique.

Functional checks:

- The software identifiers can be visualised as described in the documentation.
- The presented identifiers are identical to the identifiers given in the documentation.
- The legally relevant identifiers are distinguishable from other identifiers.

Example of an Acceptable Solution:

a) a checksum over code
b) a string added by a version number,
c) any string of numbers, letters, other characters,
d) .

- If the manufacturer chooses a mixed identifier for legally relevant and legally non-relevant software, a simple solution that allows distinguishing the identifiers is using placeholders in the TEC, e.g. “abc1.xx” with “abc1” for the legally relevant software and “xx” as placeholder for legally non-relevant software.

Additions for Risk Class E
Required Documentation Identical to risk classes C and D.
Validation Guidance Identical to risk classes C and D.

Risk Class C	**Risk Class D**
U3: Influence via user interfaces *Commands entered via the user interfaces shall not inadmissibly influence legally relevant software, device-specific parameters and measurement data.*	
Specifying Notes: 1. There shall be an unambiguous assignment of each command to an initiated function or data change. 2. Commands that are not documented shall have no effect on legally relevant functions, device-specific parameters and measurement data. 3. The respective parts of the software that interpret commands are considered to be legally relevant software.	
Required Documentation: If the instrument has the ability to receive commands, the documentation shall include: • Description of commands and their effect on legally relevant software, device-specific parameters and measurement data. • Description of how the legally relevant software, device-specific parameters and measurement data are protected from being influenced by other inputs.	
Validation Guidance: *Checks based on documentation:* • Check that documented commands are admissible, i.e., that they have an allowed influence on the legally relevant software, device-specific parameters and measurement data). • Check the protection measures against influences from other commands. *Functional checks:* • Carry out practical tests (spot checks) with documented commands. • Check whether there are undocumented commands.	**Validation Guidance** (in addition to the guidance for risk class C)**:** *Checks based on documentation:* • Check whether the measures taken and test protocols are appropriate for the high protection level.
Example of acceptable Solution: • A module in the legally relevant software filters out inadmissible commands. Only this module receives commands, and there is no circumvention of it. Any false input is blocked.	**Example of acceptable Solution:** • For using the measuring system, only an account with restricted permissions is set up. Access to the administrator account is blocked according to U6. • The user shell is closed, i.e. the user cannot load programs, write programs or perform commands to the operating system.

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk class D)**:** Source code of the legally relevant software.
Validation Guidance (in addition to the guidance for risk class D)**:** *Checks based on the source code:* • Check the software design whether data flow concerning commands is unambiguously defined in the legally relevant software and can be verified. • Search inadmissible data flow from the user interface to domains to be protected. • Check with tools or manually that commands are decoded correctly. • Check the code for undocumented commands.

Risk Class C	Risk Class D

U4: Influence via communication interfaces

Commands input via communication interfaces of the device shall not inadmissibly influence the legally relevant software, device-specific parameters *and measurement data.*

Specifying Notes:

1. There shall be an unambiguous assignment of each command to an initiated function or data change.
2. Commands that are not documented shall not have any effect on legally relevant functions, device-specific parameters and measurement data.
3. The respective parts of the software that interpret commands are considered to be legally relevant software.
4. Interfaces that allow commands with inadmissible effects on the legally relevant software, device-specific parameters and measurement data shall be sealed or protected in another appropriate way. This also applies for interfaces that cannot be completely assessed.
5. This special requirement does not apply to software download according to Extension D.

Please note: If the operating system allows remote control or remote access, the requirements U3 apply to the communication interface and the connected remote terminal, respectively.

Required Documentation:

If the instrument has an interface, the documentation shall include:

- Description of commands and their effect on legally relevant software, device-specific parameters and measurement data.
- Description of how the legally relevant software, device-specific parameters and measurement data are protected from being influenced by other inputs.

Validation Guidance:

Checks based on documentation:

- Check that documented commands are admissible, i.e., that they have an allowed influence on the legally relevant software, device-specific parameters and measurement data).
- Check the protection measures against influences from other commands.

Functional checks:

- Carry out practical tests (spot checks) using peripheral equipment.

Examples of Acceptable Solutions:

- There is a software module that receives and interprets commands from the interface. This module belongs to the legally relevant software. It forwards only allowed commands to the other legally relevant software modules. All unknown or not allowed commands are rejected and have no impact on the legally relevant software, device-specific parameters and measurement data.
- The operating system policy for serial connections and the firewall settings for network connection preventing an inadmissibly command execution to affect the legally relevant application.

Additions for Risk Class E

Required Documentation (in addition to the documentation required for risk classes C to D)**:**
Source code of the legally relevant software.

Validation Guidance (in addition to the guidance for risk classes C to D)**:**

Checks based on the source code:

- Check the software design whether data flow concerning commands is unambiguously defined in the legally relevant software and can be verified.
- Search inadmissible data flow from the interface to domains to be protected.
- Check with tools or manually that commands are decoded correctly.
- Check the code for undocumented commands.

Risk Class C	Risk Class D

U5: Protection against accidental or unintentional changes

Legally relevant software and device-specific parameters shall be protected against accidental or unintentional changes.

Specifying Notes:

1. The software shall be capable to detect changes caused by physical effects (electromagnetic interference, temperature, vibration, etc).
2. Means shall be implemented to protect from unintentional misuse of the user interfaces.
3. The accidental modification of legally relevant software and device-specific parameters shall be periodically checked by calculating checksum(s) and automatically comparing them with deposited nominal value(s). If the comparison does not match, reactions are necessary that are adequate for the instrument (stop of measurement, indication of measurement data, see chapter 10 for eventual recommendations)
   Alternative methods are possible if the change status of software can be identified by them.
4. For additional protection measures to be implemented in the operating system, see O4.

Required Documentation:

- Description of measures that have been taken to detect and protect the legally relevant software and device-specific parameters from unintentional changes.
- Description of the checksum method and of reactions in case of non-matching.
- Description of how and where the nominal checksum(s), or the alternative indications of change status, are deposited.

Validation Guidance:

Checks based on documentation:

- Check that measures against unintentional changes are described and appropriate.
- Check that the checksum(s) comprise the legally relevant software.
- Check that methods of checksum calculation, comparison and of reactions in the case of non-matching are correct.

Example of an Acceptable Solution:

- Misuse of the operating system, overwriting or deletion of stored data and programs: It is made full use of the protection or privacy rights provided by the operating system or programming language.
- All user rights for the deletion, moving or amendment of legally relevant software are removed, and access is controlled via utility programs.
- The accidental modification of legally relevant software is checked by calculating a checksum over the relevant code, comparing it with the nominal value and initiating appropriate actions if the code has been modified.

Additions for Risk Class E

Required Documentation (in addition to the documentation required for risk classes C to D)**:**
Source code of the legally relevant software.

Validation Guidance (in addition to the guidance for risk classes C to D)**:**

Checks based on the source code:

- Check whether measures taken for detection of changes (faults) are appropriate.
- Check whether all parts of the legally relevant software and all device-specific parameters are covered by the checksum.

<table>
<tr><th>Risk Class C</th><th>Risk Class D</th></tr>
<tr><td colspan="2">U6: Protection against inadmissible intentional changes
Legally relevant software and measurement data shall be secured against inadmissible intentional modification or replacement.</td></tr>
<tr><td colspan="2">Specifying Notes:
1. Mass storage device where legally relevant software, configuration files and device-specific parameters are stored shall be protected against physical exchange.
2. A checksum or an alternative method with the same level of protection shall be provided in order to support the detection of software modifications. The calculated checksum or an alternative indication of software modification shall be made visible on command for control purposes.
3. The checksum or the alternative indication is calculated over the legally relevant software. The software that organizes the generation of checksums or alternative indications is part of the legally relevant software.
4. For additional protection measures to be implemented in the operating system, see O4 and O7.
5. If a checksum is used, the algorithm shall have a key length of at least 4 bytes;</td></tr>
<tr><td></td><td>6. In general, a universal device is only usable if additional hardware can be used to support securing.
7. Concerning algorithms and minimum key lengths, the requirements or recommendations of the national and international institutions responsible for data security shall be taken into consideration.</td></tr>
<tr><td colspan="2">Required Documentation:
• Description of measures that have been taken to protect the software, in particular the method of checksum calculation and nominal checksums or alternative methods with the corresponding nominal indication.
• Description of methods protecting the mass storages from exchange, if applicable.
• Description of how the checksum or an alternative indication are presented.</td></tr>
<tr><td colspan="2">Validation Guidance:
Checks based on documentation
• Check that the checksum(s) or alternative indication(s) comprise the legally relevant software.
• Check that measures taken to prevent from modifying or replacing legally relevant software by using the operation system are adequate.
• Check that mass storage devices are protected from being physically exchanged, if applicable.

Functional checks
• Arrange to calculate checksums or alternative indications and compare them with the nominal values.</td></tr>
<tr><td></td><td>Checks based on documentation:
• Check whether the measures taken are appropriate with respect to the required state of the art for a high protection level.</td></tr>
<tr><td>Examples of an Acceptable Solution:
1. Program code is protected by means of checksums. The program is calculating its own checksum and compares it with a desired value that is hidden in the executable code. If the self-check fails, the program is blocked. A CRC-32 checksum with a secret initial vector (hidden in the executable code) is used. The access to the administrator account is blocked by means</td><td>Example of an Acceptable Solution:
• Program code is secured by storing the legally relevant software in a dedicated plug-in-unit, which is sealed. The plug-in unit includes a read-only memory and a microcontroller.</td></tr>
</table>

of a random password generated automatically, known to nobody. Change of the legally relevant configuration is only possible by performing a new operating system set up. Circumvention of the protection means of the operating system by direct writing to mass storages or physical replacement is prohibited by sealing. 2. The unauthorised manipulation of legally relevant software is inhibited by the access control or privacy protection attributes of the operating system. The administration level of these systems is secured by sealing or equivalent means.	

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes C to D)**:** Source code of the legally relevant software.
Validation Guidance (in addition to the guidance required for risk class D)**:** *Checks based on the source code:* • Check communication with the additional securing hardware. • Check that changes of legally relevant software are detected.

Risk Class C	**Risk Class D**
U7: Parameters protection *Device-specific parameters shall be secured against inadmissible modification.*	
Specifying Notes: 1. Because settable device-specific parameters could be manipulated using simple tools on universal devices, they shall be stored in secured hardware, e.g., in the respective sensor.	
Required Documentation: The documentation shall describe the device-specific parameters, whether they may be set and how they are set and how they are secured.	
Validation Guidance: *Checks based on documentation:* • Check that changing or adjusting of device specific parameters is impossible after setting. • Check that all relevant device-specific parameters (given in Extension I, if any) are secured.	
Example of an Acceptable Solution: • Device-specific parameters to be protected are stored on a plugged-in storage which is sealed against removing or directly on the sensor unit. Writing of device-specific parameters is inhibited by sealing a write-enable switch in the disabled state. • Unprotected settable device-specific parameters are stored on a standard storage of the universal device.	

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes C to D)**:** Source code of the legally relevant software.
Validation Guidance (in addition to the guidance for risk classes C to D)**:** *Checks based on the source code:* • Check whether measures taken for protecting device-specific parameters are appropriate.

Risk Class C	Risk Class D
U8: Authentication of presented measurement data *The authenticity of the measurement data that are presented shall be guaranteed.*	

Specifying Notes:

1. Presented measurement data are considered authentic if the presentation is issued from within the legally relevant software.
2. It shall not be possible to fraudulently simulate (spoof) legally relevant software for presenting measurement data.

3a. For each presented legally relevant measurement data the meaning shall be clear. All presented legally relevant measurement data shall be distinguishable from each other.

3b. Presented legally relevant measurement data shall be clearly distinguishable from legally non-relevant data.

4. On the universal device only the legally relevant software shall be able to perform the legally relevant functions (e.g., a sensor shall only work together with the legally relevant indicating program on the universal device).
5. Presented measurement data shall be accompanied by all information, which is necessary to interpret them (e.g., quantity, unit, sensor number, scale factor). Regarding necessary information to accompany the data, see L1, T1.

Required Documentation:

The documentation should describe how authenticity of the measurement data is guaranteed.

Validation Guidance:

Checks based on documentation:

- Check that presented measurement data is generated by legally relevant software.
- Check that the presentation of measurement data can only be performed by legally relevant software.
- If the source of the presented measurement data is not implicitly identifiable or verifiable, check that the source of these data is identified and indicated by the legally relevant software.

Functional checks:

- Check that the meaning of all presented legally relevant measurement data is clear and that they are distinguishable from each other.
- Check through visual control if the presentation of measurement data is easily distinguishable from other information that may also be presented.
- If applicable, check through visual control that the presented measurement data are accompanied by all necessary information.

Examples of an Acceptable Solution:

1. The legally relevant software shows the measurement data in a window, which is always on top. The legally non-relevant software has no access to the measurement data until they are indicated

2a The sensor unit encrypts the measuring values with a key known to the authentic software running on the universal device (e.g. a secret number). Only the authentic software can decrypt and use the measurement values, non-authentic programs on the universal device cannot as they do not know the key. For key treatment see Extension T.

2b Before sending measurement values the sensor initiates a handshake sequence with the legally relevant software on the universal device based on secret keys. Only if the program on the universal device communicates correctly, the sensor unit sends its measurement values. For key treatment see Extension T.

3. The key used in 2a / 2b is chosen and entered to the sensor unit and software on the universal device without destroying a seal.	3. The key used in 2a / 2b is the hash code of the program on the universal device. Each time the software on the universal device is changed; the new key is entered into the sensor unit and is secured in a way that the seal must be broken to change it.

4. If the presented measurement data are not explicitly linked to a sensor, the originating sensor transmits its data together with a unique identification of the sensor itself. All presented measurement data are labelled with the identification of the individual sensor. The identification of each sensor is a legally relevant parameter shown on the sensor housing.

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes C to D)**:** Source code of the legally relevant software.
Validation Guidance (in addition to the guidance for risk classes C to D)**:** *Checks based on the source code:* • Check that legally relevant software generates the presented measurement data. • Check whether all measures taken are correct to guarantee the presentation of measurement results by legally relevant software.

Risk Classes C to E
U9: Influence of other software *The legally relevant software shall be designed in such a way that other software does not inadmissibly influence it.*
Specifying Notes: 1. This requirement implies software separation between the legally relevant and legally non-relevant software under consideration of the state-of-the-art of software engineering for modularisation or object-oriented concepts. Extension S shall be observed. This is the standard case for universal devices.
Required Documentation: See Extension S.
Validation Guidance: See Extension S.
Example of an Acceptable Solution: See Extension S.

6 Extension O: General-Purpose Operating Systems

The specific requirements of this chapter only apply if an operating system on a component of a measuring instrument is legally relevant, i.e. the operating system is used to fulfil the essential requirements of the MID or can be used to affect compliance with requirements. They are an addition to the specific requirements of software for measuring instruments using a universal device (type U requirements). These requirements do not have to be applied for measuring instruments type P.

6.1 Technical description

Software is described as a *general-purpose operating system* if system resources of a measuring instrument (CPU, memory, interfaces) are administrated by that software and are made available to the legally relevant application. In addition, the operating system has a multi-user capacity and an administration mode (multi-user operating system).

Any general-purpose operating system evaluated according to this extension shall fulfil the following prerequisites:

- shall be proven in use,
- shall be suitable for the general purpose,
- shall be state-of-the-art[2] and
- must not have been developed by the manufacturer of the measuring instrument, sub-assembly or producer of the component. However, a manufacturer or producer can contribute to the OS with respect to drivers or modules that are specifically programmed for a legally relevant task provided that the requirements of O6 and O7 are met, i.e. drivers or modules that are specifically programmed for a legally relevant task shall have their own identification and protection.

In this case, the software examination of the general-purpose operating system can be reduced to an examination of the legally relevant configuration based on the requirements in Extension O.

Each of the implemented protective measures can be combined with measures on hardware level or on the level of the legally relevant application.

6.2 Applicability of requirements for components

With respect to off-the-shelf operating systems, this extension distinguishes two categories of measuring instrument components, see definitions for components of categories 1 and 2 in Chapter 1.
This chapter only applies to components of a measuring instrument that can be evaluated separately under the conditions specified in WELMEC guide 8.8. In the case of a complete instrument the requirements of a category 1 component shall be applied.

For components from category 2:

- O2 does not apply.
- O3, O4 and O5 apply in full.
- O1, O6 and O7 apply to the configuration/settings of the OS.

If this is the case, regular updates to the operating system are possible, as long as they do not affect the configuration. Technical working groups may decide which components from category 2 (if any) may be subject to this exception.

[2] i.e. patches for all known bugs and vulnerabilities have been applied

For some operating system types, an update might result in fundamental changes that also affect the configuration (i.e. a major version upgrade in Windows or in a common Debian-based Linux distribution). In this case, the aforementioned exception would not apply.

6.3 Specific requirements for configuration of general-purpose operating systems

<table>
<tr><th>Risk Class C</th><th>Risk Class D</th><th>Risk Class E</th></tr>
<tr><td colspan="3">O1 Hardware
The hardware part on which the legally relevant operating system runs, shall be protected against inadmissible access.</td></tr>
<tr><td colspan="3">Specifying Notes:
1. For category 1 components and complete instruments, the legally relevant operating system shall be protected against removal or exchange.
2. Hardware interfaces that might influence the operating system shall either be disconnected from power supply, disabled by the OS, protected by a hardware seal or bound to a protective software interface (see O5).
3. Interfaces with direct memory access shall be protected by a hardware seal.
4. The operating system shall use memory protection to prevent retrieval of sensitive cryptographic material.</td></tr>
<tr><td colspan="2">Required Documentation:
• A list of all components with an operating system.
• Description of the securing measures for mass storages.
• Description of the protective measures of hardware interfaces.</td><td>Required Documentation (in addition to the documentation for risk class C):
• If cryptographic material is used: Description of protective measures for volatile memory and storage devices.</td></tr>
<tr><td colspan="3">Validation Guidance:
Checks based on documentation:
• Check that all components with a legally relevant operating system are documented.
• Check that all hardware interfaces are protected or necessary for the legally relevant data exchange in which case they shall be equipped with a protective software interface, see U4.
• Check that all measures for the protection of memory, mass storages and hardware interfaces are effective and adequate.</td></tr>
<tr><td colspan="2"></td><td>Checks based on the configuration files:
• Check that the configuration of the operating system for memory protection correspond to the documented measures
Functional checks:
• Check that the additional protection measures for legally relevant operating system and cryptographic material are effective.</td></tr>
<tr><td colspan="3">Example of an Acceptable Solution:
• The housing of the measuring instrument is physically protected by seals to prevent exchange of mass storages or mass storages are fitted with sealed connections during use.
• A hardware seal is applied to ensure the mass storage device, on which the legally relevant OS resides, cannot be exchanged or removed.</td></tr>
<tr><td colspan="2"></td><td>• Cryptographic material, such as passwords, is stored in a separate hardware component which is protected against access by the operating system.</td></tr>
</table>

<table>
<tr><th>Risk Class C</th><th>Risk Class D</th><th>Risk Class E</th></tr>
<tr><td colspan="3">O2 Boot process
For category 1 components and complete instruments the configuration of the boot process shall provide the same configured environment for the execution of legally relevant software.</td></tr>
<tr><td colspan="3">Specifying Notes:
1. The boot process of the operating system shall be unambiguous and reproducible
2. The legally relevant software application shall be included in the start-up procedure of the universal device.
3. The boot configuration shall be protected against modifications.
4. At the end of the boot process, a chain of trust shall be established over the individual components of the boot process.
5. The processing of the chain of trust may be interrupted if the integrity of the chain of trust is preserved.
6. Booting via open interfaces shall be prohibited.</td></tr>
<tr><td colspan="2"></td><td>7. The boot process shall be secured by adequate means, depending on the level of protection.</td></tr>
<tr><td colspan="3">Required Documentation:
• Information regarding the boot configuration of the operating system (e.g. mass storage, partitions, kernel parameters).
• Description of protective measures for the boot process.
• Description of the structure of the chain of trust.
• Description of the booted operating system environment for the legally relevant software.</td></tr>
<tr><td colspan="3">Validation Guidance:
Checks based on documentation:
• Check that the configuration of the boot process is protected against inadmissible modifications.
• Check that the operating system boots into the same secured environment for the legally relevant software at each start up.
• Check that there are no undocumented interruptions of the boot process.
• Check the booting via open interfaces is prohibited.</td></tr>
<tr><td colspan="2"></td><td>Checks based on the documentation:
• Check if the used cryptographic measures are effective and correspond to the requirements or recommendations of the national and international institutions responsible for data security.
Checks based on the configuration files:
• Check if the configuration of the boot loader is unambiguous.
• Check if it is possible to boot the operating system via open interfaces.</td></tr>
<tr><td colspan="3">Example of an Acceptable Solution:
• The boot configuration (BIOS) has been secured by a strong password.
The integrity of the boot loader and of the legally relevant parts of the operating system is checked by means of a checksum
• A TPM (trusted platform module) verifies the signature of the boot loader, the boot loader then verifies the operating system, which in turn verifies and starts the legally relevant application.</td></tr>
<tr><td colspan="2"></td><td>• Secure boot: Only a signed kernel can be loaded by the boot loader. Prior to booting of the operating system, the signature of the kernel is verified.</td></tr>
</table>

Risk Class C	Risk Class D	Risk Class E
O3 System resources *The configuration of the operating system shall ensure that there are enough resources for the operation of the legally relevant application.*		
Specifying Notes: 1. The operating system should be configured as restrictively as possible. 2. The resources of the legally relevant software application are not reduced below the necessary minimum by other software (legally relevant and legally non-relevant).		
Required Documentation: • Information regarding the configuration of the installed operating system parts.		
	• Information regarding the running processes during use of the measuring instrument.	
Validation Guidance: *Checks based on documentation:* • Check that the installed operating system parts are appropriate and sufficiently configured to ensure the operation of the measuring instrument.		
Functional checks: • Check that the export of running processes corresponds to the documentation. • The manufacturer checks via the system utilization indication whether there are sufficient system resources for the legally relevant application during use.		
Examples of Acceptable Solution: • By means of the package administration of the operating system, the manufacturer removes all unnecessary programs. • The manufacturer limits the runtime for legally non-relevant tasks. • Interrupt hierarchy is designed in a way that avoids adverse influences.		

Risk Class C	Risk Class D	Risk Class E
O4 Protection during use *The operating system shall be configured in such a way that the legally relevant software application cannot be inadmissibly influenced by functions of the operating system or by other software.*		
Specifying Notes: 1. The administration tasks of the legally relevant software (application and operating system) shall be protected. 2. The access control shall be configured in such way that the intended use cannot be inadmissibly influenced. a. The access permissions shall be routinely checked by the legally relevant operating system. 3. The operating system shall be configured to prevent removal of the legally relevant software application. The connection of auxiliary devices shall not have an inadmissible influence on the OS, or the configuration settings.		
Required Documentation: • A list of mounted or mountable storage media with their attributes and policies for limiting their usage. • Description of the administration of the user access control and protection of the administrator account. • Description of the operation mode of the GUI. • Description of the connection of auxiliary devices.		

<table>
<tr><td colspan="2">Validation Guidance:
Checks based on documentation:
• Check that the usage of the legally relevant application has been separated from administration of the system, i.e. the legally relevant application cannot change any legally relevant administration/configuration of the operating system.
• Check that the protection measures of the administrator account are sufficient and that there is no second account with inadmissible administrator privileges.
• Check that no inadmissible software can be executed from mounted storage media.
• Check that no inadmissible operating system functions can be called through input devices (e.g. keyboard shortcuts) or by the user shell.
• Check that the application control only allows the execution of legally relevant software, unless software separation has been implemented.
• Check that the connection of auxiliary devices does not inadmissibly affect the legally relevant operating system or the configuration settings.
• Check that legally relevant settings of the operating system cannot be reset or modified.
Functional checks:
• Check that the administrator account is locked during use.
• Check that all inadmissible keyboard shortcuts have been deactivated.
• Check that exiting or changing the operation mode of the GUI is impossible.
• Check that application control and policies for storage media as well as auxiliary devices are effective.
• Check that the legally relevant settings are retained after a reboot.</td></tr>
<tr><td></td><td>Checks based on the configuration files:
Check that
• user and group privileges, administrator account,
• configuration of the application control,
• mounted storage media as well as partitions or media with access attributes,
• policies for storage media and auxiliary devices
correspond to the information contained in the documentation and are correctly configured.</td></tr>
<tr><td>Example of an Acceptable Solution:
• All legally relevant tasks are bundled into one dynamically linkable library on a PC.
• Cryptographic means ensure that only the legally relevant dynamically linkable library can communicate with the sensor connected to the PC.
• The window displaying the legally relevant data is generated and controlled by procedures in the legally relevant dynamically linkable library.
• During measurement, these procedures check cyclically that the relevant window is still on top of all the other open windows; if not, the procedures place it on top while process prioritization ensures that other I/O devices do not permanently block the CPU.</td><td>Example of an Acceptable Solution:
• The operating system possesses a secured administrator account for the administrative tasks, as well as a user account with limited privileges for usage during a measurement operation.
• The operating system boots at each start up into a kiosk mode with only the legally relevant application accessible. Keyboard shortcuts have been limited to legally relevant usage.
• Access to exchangeable media and auxiliary devices has been restricted by means of group policies
• There are no directories with write and execute permissions for files on the system.
• The administrator account has been permanently deactivated</td></tr>
</table>

<table>
<tr><th>Risk Class C</th><th>Risk Class D</th><th>Risk Class E</th></tr>
<tr><td colspan="3">O5 Protective interfaces
Operating system functions accessible via open interfaces shall not inadmissibly influence the legally relevant software.</td></tr>
<tr><td colspan="3">Specifying Notes:
1. Communication with the legally relevant operating system shall be made via protective interfaces.
2. In case of software separation on an operating system, Extension S and Extension T for open networks apply for transmission of legally relevant data via software interfaces of the operating system.
3. If the operating system configuration ensures that the communication partner connected to an open interface can only be a certified component and the connection is protected, no further checking of the interface is needed.</td></tr>
<tr><td colspan="3">Required Documentation:
• Description of the operating system configuration for open hardware and software interfaces.
• A list of open hardware and software interfaces not configured by the operating system.
• A list of all accepted commands and their influence for all open interfaces managed by the operating system.</td></tr>
<tr><td colspan="3">Validation Guidance:
Checks based on documentation:
• Check that the operating system configuration for open interfaces is such that inadmissible influence is not possible.
• Check that there are no unsupervised open interfaces.
• Check that open interfaces have no inadmissible influence on the legally relevant operating system, its configuration, the legally relevant software application, legally relevant parameters or data.</td></tr>
<tr><td colspan="2"></td><td>Checks based on the configuration files:
It shall be checked that inadmissible influence is prevented for the following open interfaces:
• network interfaces (open and closed ports, used protocols and commands, policies)
• serial interfaces (command interpreter of the application, policies for user account control
• software interfaces of the operating system (access control used commands
In addition, it shall be checked
• whether the used cryptographic measures are effective and correspond to the requirements or recommendations of the national and international institutions responsible for data security.
Functional checks:
• Check the effectiveness of the configuration of open serial interfaces.
• Check the effectiveness of the configuration of open network interfaces.</td></tr>
<tr><td colspan="3">Example of an Acceptable Solution:
• All hardware interfaces with legally relevant data exchange are configured via the operating system (network firewall, USB policies).</td></tr>
<tr><td colspan="2"></td><td>• Usage of IT-security protocols (VPN, PISEC) for open networks.</td></tr>
</table>

Risk Class C	Risk Class D	Risk Class E

O6 Identification of the operating system and its configuration

The operating system and configuration of the operating system shall be identifiable. The identification of the operating system and identification of the configuration of the operating system shall be presented on command or during operation.

Specifying Notes:

1. If the legally relevant functions and the account of the measuring task are protected by a specific configuration of the operating system, the relevant configuration files shall have an own identifier.
2. Identification shall include drivers and modules of the operating system that have been modified or specifically programmed for a legally relevant task.

Required Documentation:

- General information regarding the operating system (manufacturer, distribution, product name, kernel version).
- Information regarding the identification of those parts of the operating system configured for the legally relevant task.
- Information regarding the identification of modified or added self-developed parts of the operating system for the legally relevant task (kernel modules, drivers, libraries)
- A list of all used identifiers as well as a description of how they are created, of their indication and how to distinguish them from legally non-relevant identifiers.

Validation Guidance:

Checks based on documentation:

- Check that all identifiers of the legally relevant operating system configuration have been documented.
- Check that all identifiers of modified or added programmed parts have been documented.
- Check that all identifiers of the operating system are unambiguous and that coverage of the legally relevant part of the operating system is complete and comprehensible.
- Check that creation, indication and securing of the identifiers as well as their distinguishability from other legally non-relevant identifiers is fully documented and free of contradictions.

Functional checks

- Check the indication of the identifiers of the operating system and compare them with the documentation.

Example of an Acceptable Solution:

- The identifier consists of the name of the OS producer, the product name, and the version of the operating system. Alternatively, the name and version of the distribution as well as the version of the kernel are used.
- In addition, those operating system parts configured for the legally relevant task are identified by means of a checksum.

<table>
<tr><th>Risk Class C</th><th>Risk Class D</th><th>Risk Class E</th></tr>
<tr><td colspan="3">O7 Protection of the operating system
The operating system shall be protected in such a way that evidence of an intervention is available.</td></tr>
<tr><td colspan="3">Specifying Notes:
1. Drivers or modules that are specifically programmed for a legally relevant task shall have their own protection.
2. The protective measures for the operating system shall cover all legally relevant parts completely. An exception may be made to include the boot loader configuration in the protective measure instead of the boot loader itself, if it is not part of the file system of the operating system.
3. If a checksum or an equivalent integrity measure are used, they should be calculated by means of the operating system. The calculated checksum or equivalent integrity measure shall be indicated by the operating system or by a legally relevant application.
4. The integrity of the legally relevant operating system shall be periodically checked. If the integrity check fails, reactions are necessary that are adequate for the instrument.
5. Updates to legally relevant operating system parts are not addressed by this requirement. Such updates would fall under Extension D.</td></tr>
<tr><td></td><td colspan="2">6. The checksum shall be obtained with cryptographically strong methods.</td></tr>
<tr><td colspan="3">Required Documentation:
• Documentation of the protective measures of the operating system.
• Description of methods for creation and indication of the integrity measure.
• Exhaustive list of legally relevant parts of the operating system
• A list of all operating system parts covered by the integrity measure.</td></tr>
<tr><td colspan="3">Validation Guidance:
Checks based on documentation:
• Check that all legally relevant operating system parts are adequately covered by the protective measures.
• Check that creation and indication of the protective measures are fully documented and free of contradictions.
Functional checks:
• If a checksum has been used: Check the indication of the checksum for the legally relevant operating system parts (see definition for categories 1 and 2) and compare it with the reference values given in the documentation.
• If alternative measures have been used: Check the prototype and compare it with the documentation.</td></tr>
<tr><td></td><td colspan="2">• Check whether the used cryptographic measures are effective and correspond to the requirements or recommendations of the national and international institutions responsible for data security.</td></tr>
<tr><td colspan="3">Example of an Acceptable Solution:
• Linux: Checksum covering boot loader, kernel and the directory /etc.
• Windows: Checksum covering parts of the system directory, parts of the exported registry and parts of the policy settings regarding user privileges, firewall, USB etc.</td></tr>
<tr><td>• The checksum is a CRC32.</td><td colspan="2">• The checksum is a SHA-value (secure hashing algorithm) of a length recommended by ENISA.</td></tr>
</table>

7 Extension L: Long-term Storage of Measurement Data

The specific requirements of this chapter only apply if long-term storage of measurement data is designed. They are an addition to the specific requirements of embedded software for built-for-purpose measuring instrument (type P requirements) and of software for measuring instruments using a universal device (type U requirements).

Long-term storage includes the time from when a measurement is physically completed to the point in time when all processes to be done by the *legally relevant software* are finished. It may also be applied to long-term storage of the data thereafter.

7.1 Technical description

Three different technical configurations for long-term storage are listed in the following table. For a built-for-purpose device, the variant of an integrated storage is typical: here the storage is part of the metrologically necessary hardware and software. For instruments using a universal device, another variant is typical: the use of resources already existing, e.g., hard disks. The third variant is the removable storage: here the storage can be removed from the device, which could be either a built-for-purpose device or a universal device, to be taken elsewhere. When data is retrieved from removable storage for legal purposes, e.g. visualisation, ticket printing, etc, the retrieving device shall be subject to legal control.

A) Integrated storage Simple instrument, built-for-purpose, no externally usable tools or means available for editing or changing data, integrated storage for measurement data or parameters, e.g. RAM, flash memory, hard disk.
B) Storage for universal device Universal device, graphical user interface, multitasking operating system, tasks subject to legal control and not subject to legal control exist in parallel, storage can be removed from the device or contents can be copied anywhere inside or outside the device.
C) Removable or remote (external) storage Arbitrary basic instrument (built-for-purpose instrument or instrument using universal device), storage can be taken from the instrument. These can be, for example, USB stick, flash cards, or remote databases connected via network.

Table 7-1: Technical description of long-term storages

The classification may be reduced for selected kinds of measuring instruments on conclusion of the responsible WELMEC Working Groups, see chapter 10.

7.2 Specific software requirements for Long-term Storage

Risk Class B	Risk Class C	Risk Class D

L1 Completeness of stored measurement data

The measurement data stored shall be accompanied by all relevant information needed for legally relevant purposes.

Specifying Notes:

5. The measurement data stored shall be capable of being traced back to the measurement that has generated the data.
6. The measurement data stored shall be sufficient for checking invoices.
7. The kind of necessary information may depend on the type of instrument.
8. A presupposition to comply with this special requirement is an identification of each measurement data set stored.

Required Documentation:

Description of all fields of the measurement data sets.

Validation Guidance:

Checks based on documentation:

- Check whether all information needed for legally relevant purposes are contained in the measurement data set.

Example of an Acceptable Solution:

- A legally and metrologically complete measurement data set comprises the following fields:
  - Measurement value(s) with correct resolution
  - the unit of measure
  - the unit price or the price to pay (if applicable)
  - the date and time of the measurement (if applicable)
  - identifier of the instrument
  - the place of the measurement (if applicable)
- Measurement Data is stored with the same resolution, values, units etc as indicated or printed on a delivery note.

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes B to D)**:** Source code of the legally relevant software that generates the measurement data sets for storing.
Validation Guidance (in addition to the guidance for risk classes B to D)**:** *Checks based on the source code:* • Check whether the measurement data sets are correctly built.

Risk Class B	Risk Class C	Risk Class D

L2: Protection against accidental or unintentional changes

Stored measurement data shall be protected against accidental and unintentional changes.

Specifying Notes:

1. Measurement data stored shall be capable to detect accidental data changes caused by physical effects (electromagnetic interference, temperature, vibration, etc).
2. Means shall be implemented to protect from unintentional change or deletion of measurement data.

Required Documentation:

Description of protection measures.

Validation Guidance:

Checks based on documentation:

- Check that a method is implemented to detect accidental measurement data changes.
- Check that the method captures all measurement data.
- Check that overwriting of measurement data cannot occur before the end of the data storage period that is foreseen.
- Check that a warning is issued to the user if he is about to change or delete measurement data files.

Functional checks:

- Check by practical spot checks that before changing/deleting measurement data a warning is given, if changing/deleting is possible at all.

Example of an Acceptable Solution:

- Stored measurement data is accompanied by additional redundant information to enable the software retrieving, evaluating, and indicating of the measurement data (see L6)
- To detect measurement data changes due to physical effects, a checksum with the CRC-16 algorithm is calculated over the entire measurement data set and inserted into the measurement data set to be stored.

  Note: The algorithm is not secret and, in contrast to requirement L3, neither is the initial vector of the CRC-register nor the generator polynomial i.e. the divisor in the algorithm. The initial vector and generator polynomial are known to both of the programs that create and verify the checksums.
- Measurement data/invoice files are protected by attaching an automatic date stamp on creation and a flag or label stating whether invoices were paid/unpaid. A utility program would only move/delete files if invoices had been paid or were out-of-date.
- Measurement data is not deleted without prior authorisation, e.g. a dialogue statement or window asking for confirmation of deletion.
- Automatic overwriting of measurement data is allowed if there is adequate protection of the records to be retained. A parameter determining the number of days before measurement data can be deleted is set and secured when putting into use according to the user's needs and data storage size. The instrument stops if the memory is full and all the records are not old enough to be overwritten. Manual deletion (with prior authorisation) is performed in that case.

Additions for Risk Class E

Required Documentation (in addition to the documentation required for risk classes B to D)**:**
Source code of the legally relevant software that realises the protection of stored data.

Validation Guidance (in addition to the guidance for risk classes B to D)**:**

Checks based on the source code:

- Check whether measures taken for protecting stored measurement data are appropriate and correctly implemented.

<table>
<tr><th>Risk Class B</th><th>Risk Class C</th><th>Risk Class D</th></tr>
<tr><td colspan="3">L3: Protection against inadmissible intentional changes
The measurement data stored shall be protected against intentional changes.</td></tr>
<tr><td colspan="3">Specifying Notes:
1. Stored measurement data in integrated storages in general are protected by hardware means. No extra software protection is necessary.
2. The protection shall apply against intentional changes carried out by easily available and manageable software tools.
3. Stored measurement data shall be accompanied by additional redundant information to enable the software retrieving, evaluating, and indicating or otherwise processing the data to verify integrity of the measurement data.</td></tr>
<tr><td colspan="2"></td><td>4. The protection shall also apply against intentional changes carried out by special sophisticated software tools.
5. Concerning algorithms and minimum key lengths, the requirements or recommendations of the national and international institutions responsible for data security have to be taken into consideration.
6. Even if the algorithm and key meet the level high, a technical solution with a standard personal computer would not realise this protection level provided that there are no appropriate protection means for the programs that sign or verify a data set (see basic guide U for universal devices, comment on requirement U6-Risk Class D).</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="3">Required Documentation:
The method of how the protection is realised and how corrupted data is marked shall be documented.</td></tr>
<tr><td colspan="2">Validation Guidance:
Checks based on documentation:
• If a checksum or signature is used:
Check that the checksum or signature is generated over the entire measurement data set.
Check that legally relevant software, which reads the measurement data and calculate a checksum or decrypts a signature really compares calculated and the nominal values.
• Check that secret data (e.g. key initial value if used) are kept secret against spying out with simple tools.</td><td>Validation Guidance (in addition to the guidance for risk classes B and C):
Checks based on documentation:
• Check whether the measures taken are appropriate with respect to the required state of the art for a high protection level.</td></tr>
<tr><td colspan="2">Example of an Acceptable Solution:
Stored measurement data are secured by CRC-16.</td><td>Example of an Acceptable Solution:
Stored measurement data are secured by a cryptographic signature.</td></tr>
<tr><td colspan="3">Additions for Risk Class E</td></tr>
<tr><td colspan="3">Required Documentation (in addition to the documentation required for risk classes B to D):
Source code of the legally relevant software that realises the integrity of stored data.</td></tr>
</table>

Validation Guidance (in addition to the guidance for risk class D)**:**

Checks based on the source code:

- Check whether measures taken for ensuring integrity are appropriate and correctly implemented.

Risk Class B	Risk Class C	Risk Class D
L4 Traceability of stored measurement data *Stored measurement data shall be capable of being traced back to the measurement and the measuring instrument that generated them.*		
Specifying Notes: 1. Traceability requires the correct assignment (linking) of measurement data to the measurement that has generated the data. 2. Traceability requires the correct assignment (linking) of measurement data to the measuring instrument that has generated them. 3. Traceability to measurements presupposes an identification of measurements. 4. Traceability to a measuring instrument presupposes an identification of the measuring instrument.		
Required Documentation: Description of the method used for ensuring the authenticity.		
Validation Guidance: *Checks based on documentation:* • Check that there is a correct linking between each measurement value and the corresponding measurement. • If a checksum or signature is used, check that the checksum or signature is generated over the entire measurement data set. • Check that secret data (e.g. key initial value if used) are kept secret against spying out with simple tools. *Functional checks:* • Check whether corresponding stored data and data printed on the ticket or invoice are identical. • Check whether the ticket shows a hint that the measurement values can be compared with the reference data on a means of storage subject to legal control.		**Validation Guidance** (in addition to the guidance for risk classes B and C)**:** *Checks based on documentation:* • Check whether the measures taken are appropriate with respect to the required state of the art for a high protection level.
Example of an Acceptable Solution: Stored measurement data contain the following data fields: • A unique (sequential) identification number and an identification of the measuring instrument that has generated the value. A signature that is used for ensuring the integrity of data can simultaneously be used for ensuring the traceability. • Time when the measurement has been performed (time stamp) and an identification of the measuring instrument that has generated the value. *Note:* The ticket may state that the measurement values can be compared with the reference data on a means of storage subject to legal control. Assignment is demonstrated by comparing the identification number or time stamp printed on the delivery note with that in the stored measurement data set.		**Example of an acceptable solution:** In addition to the acceptable solution to risk classes B and C, the origin of certificates used for signing the measurement data is verified by means of a PKI.

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes B to D)**:** Source code that generates the data sets for storing and realises the authentication..
Validation Guidance (in addition to the guidance for risk class D)**:** *Checks based on the source code:* • Check whether the measurement data sets are correctly built and reliably authenticated.

Risk Class B	Risk Class C	Risk Class D

L5: Confidentiality of keys

Keys and associated information shall be treated as measurement data and shall be kept secret and be protected against compromise.

Specifying Notes:

1. This requirement only applies if secret information is used at all.
2. This requirement only applies to measurement data storages, which are external from the measuring instrument or realised on universal devices.
3. If the access to the secret keys is prevented by hardware means, no additional software protection means are necessary.
4. The protection shall apply against intentional changes carried out by easily available and manageable software tools.
5. Depending on the protection means the secret information may consist of keys, generator polynoms, initial vectors / start values, seeds, etc.

	6. The protection shall also apply against intentional changes carried out by special sophisticated software tools. 7. A technical solution with a standard personal computer would not be sufficient to ensure high protection level if there were no appropriate hardware protection means for the key and other secret data (see basic guide for universal devices U6).

Required Documentation:

Description of the management of secret information and means for keeping keys and other information secret.

Validation Guidance: *Checks based on documentation:* • Check that the secret information cannot be disclosed.	**Validation Guidance** (in addition to the guidance for risk classes B and C)**:** *Checks based on documentation:* • Check whether the measures taken are appropriate with respect to the required state of the art for a high protection level.
Examples of Acceptable Solutions: • The secret key and associated information are stored in binary and encrypted format in the executable code of the legally relevant software. The system software does not offer any features to view or edit these data.	**Example of an Acceptable Solution:** The secret key is stored in a hardware part that can be physically sealed. The software does not offer any features to view or edit these data.

Additions for Risk Class E

Required Documentation (in addition to the documentation required for risk classes B to D)**:**
Source code that realises key management.

Validation Guidance (in addition to the guidance for risk class D)**:**

Checks based on the source code:

• Check whether measures taken for management of secret information are appropriate.

Risk Class B	Risk Class C	Risk Class D

L6: Retrieval, verification, and indication of stored measurement data
There shall be legally relevant software for reading, verifying and indicating stored measurement data.

Specifying Notes:
1. The software shall have the capability to indicate the measurement data stored along with the relevant information (see L1).
2. Retrieved measurement data should be verified.
3. Displayed or printed measurement data shall indicate an eventual violation of traceability and integrity. origin (

Required Documentation:
- Description of the functions of the retrieval software.
- Description how corrupted measurement data is indicated.

Validation Guidance:

Checks based on documentation:

- Check that the retrieval software has the required capabilities

Functional checks:

- Perform spot checks verifying that retrieval provides all necessary information.

Example of an Acceptable Solution:
The integrity and traceability of the stored measurement data is ensured by a signature over all data fields. If the verification of the signature fails, the measurement data are indicated as invalid otherwise they are printed out.

Additions for Risk Class E

Required Documentation (in addition to the documentation required for risk classes B to D)**:**
Source code of the retrieval software.

Validation Guidance (in addition to the guidance for risk classes B to D)**:**

Checks based on the source code:
- Check whether measures taken for retrieval, verification of signatures etc. are appropriate and correctly implemented.

Risk Class B	Risk Class C	Risk Class D
L7: Automatic storing *The measurement data shall be stored automatically when the measurement is concluded.*		
Specifying Notes: 1. The storing function shall not depend on the decision of the operator. 2. In cases where a decision is required from the operator whether or not to accept a measurement result, the measurement data shall be stored automatically after making the decision.		
Required Documentation: Description of automatic storing. Description of the Graphical User Interface in case of operator-dependent storing decisions.		
Validation Guidance: *Checks based on documentation:* • Check that storing process is automatic. *Functional checks:* • Examine by spot checks that the measurement values are stored automatically after measurement or acceptance of measurement is concluded. Check that there are no buttons or menu items to interrupt or disable the automatic storing.		
Example of an Acceptable Solution: There is no menu item or button in the Graphical User Interface (GUI) that supports manual initiation of storing measurement results. The measurement values are wrapped in a measurement data set along with additional information such as time stamp and signature and are stored immediately after the measurement, or the acceptance of measurement, respectively.		

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes B to D)**:** Source code of the legally relevant software.
Validation Guidance (in addition to the guidance for risk classes B to D)**:** *Checks based on the source code:* • Check whether measures taken for automatic storing are appropriate and correctly implemented.

Risk Class B	Risk Class C	Risk Class D
L8: Storage capacity and continuity *The long-term storage shall have a capacity which is sufficient for the intended purpose.*		
Specifying Notes: 1. When storage is full or removed or disconnected from the instrument, a warning shall be given to the operator. 2. It shall be ensured that only outdated measurement data can be overwritten. 3. The regulations concerning the minimum period for storing measurement data and the required inscriptions are left to national regulations and therefore beyond the scope of this guide. 4. The information on the capacity of the storage shall be made available.		
Required Documentation: • Capacity of storage, Description of the management of storing measurement data. • Description of the behaviour of the device if storage is full or removed.		
Validation Guidance: *Checks based on documentation:* • Check that the capacity of storage or a formula for calculating it, is given. • Check that overwriting of measurement data cannot occur before the end of the data storage period that is foreseen and documented by the manufacturer. *Functional checks:* • Check that a warning is given if the storage is full or removed, if applicable.		
Example of an Acceptable Solution: • Interruptible measurements: When the storage becomes unavailable before the measurement is completed: The measuring instrument has a buffer that is large enough to store the current measurement. No new measurement is started, and the buffered values are kept for later transmission to a fresh storage. • Uninterruptible measurements: The cumulative register is read out and transmitted to the storage at a later time, when the storage is available again. • Measurement data is automatically overwritten by a tool that checks if the measurement data is out-of-date (refer to national regulations for the relevant time period). The tool prompts the user for permission to delete and measurement data is deleted in the order oldest first.		

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes B to D)**:** Source code of the legally relevant software that realises storing of measurement data.
Validation Guidance (in addition to the guidance for risk classes B to D)**:** *Checks based on the source code:* • Check whether measures taken for storing are appropriate and correctly implemented.

8 Extension T: Transmission of Measurement Data via Communication Networks

The specific requirements of this chapter only apply if measurement data is transmitted via communication networks to be used for legally relevant purposes. If that is the case, measurement data shall be transmitted and received by a legally relevant component or module.

They are an addition to the specific requirements of software for built-for-purpose measuring instruments (type P requirements) and of software for measuring instruments using a universal device (type U requirements).

If software is downloaded to a device subject to legal control, then the requirements of Extension D apply.

8.1 Technical description

In the following table two network configurations are identified.

Description of configurations
A) Closed network Only a fixed number of participants with clear identity, functionality and location are connected. All devices in the network are subject to legal control.
B) Open network Arbitrary participants (devices with arbitrary functions) can be connected to the network. The identity and functionality of a participating device and its location may be unknown to other participants. Any network that contains legally controlled devices with infrared or wireless network communications interfaces shall be considered to be an open network.

Table 8-1: Technical description of communication networks.

8.2 Specific software Requirements for Transmission of Measurement Data

Risk Class B	Risk Class C	Risk Class D
T1: Completeness of transmitted measurement data *The transmitted measurement data shall contain all relevant information necessary to present or further process the measurement result in the receiving unit.*		
Specifying Notes: 1. The completeness depends individually from the type of measurement.		
Required Documentation: Document all fields of the measurement data set.		
Validation Guidance: *Checks based on documentation:* • Check whether all information for further processing the measurement values at the receiving unit are contained in the measurement data set.		
Example of an Acceptable Solution: The measurement data set comprises the following fields: • Measurement value(s) with correct resolution • the unit of measure • the unit price or the price to pay (if applicable) • the time and date of the measurement (if applicable) • identifier of the instrument if applicable (data transmission) • the place of the measurement (if applicable)		

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes B to D)**:** Source code that generates the measurement data sets for transmission.
Validation Guidance (in addition to the guidance for risk classes B to D)**:** *Checks based on the source code:* • Check whether measurement data sets are built correctly.

Risk Class B	Risk Class C	Risk Class D

T2: Protection against accidental or unintentional changes

Transmitted measurement data shall be protected against accidental and unintentional changes.

Specifying Notes:

1. Means shall be implemented to protect from unintentional change or deletion of measurement data.

Required Documentation:

Description of the methods used to detect transmission errors.

Validation Guidance:

Checks based on documentation:

- Check that a method is implemented to detect transmission errors.

Example of an Acceptable Solution:

- Transmitted measurement data is accompanied by additional redundant information to enable the software of the receiver to detect accidental data transmission errors.
- To detect data changes, a checksum with the CRC-16 algorithm is calculated over all bytes of a data set and inserted into the data set to be transmitted. Just before the data is reused, the value of the checksum is recalculated by the receiver and compared with the attached nominal value. If the values match, the measurement data set is valid and may be used, otherwise it shall be deleted or marked invalid.

  Note: The algorithm is not secret and, in contrast to requirement T3, neither is the initial vector of the CRC-register nor the generator polynomial i.e. the divisor in the algorithm. The initial vector and generator polynomial are known to both of the programs that create and verify the checksums.
- Use of means provided by transmission protocols e.g. TCP/IP, IFSF.

Additions for Risk Class E

Required Documentation (in addition to the documentation required for risk classes B to D)**:**

Source code of the legally relevant software that realises the protection of transmitted data.

Validation Guidance (in addition to the guidance for risk classes B to D)**:**

Checks based on the source code:

- Check whether measures taken for protecting transmitted measurement data are appropriate and correctly implemented.

<table>
<tr><th>Risk Class B</th><th>Risk Class C</th><th>Risk Class D</th></tr>
<tr><td colspan="3">T3: Protection against inadmissible intentional changes
The transmitted measurement data shall be protected against intentional changes.</td></tr>
<tr><td colspan="3">Specifying Notes:
1. This requirement only applies to open networks, not to closed networks.
2. The protection shall apply against intentional changes carried out by easily available and manageable software tools.</td></tr>
<tr><td colspan="2"></td><td>3. The protection shall also apply against intentional changes carried out by special sophisticated software tools.
4. Concerning algorithms and minimum key lengths, the requirements or recommendations of the national and international institutions responsible for data security have to be taken into consideration.
5. To meet the high level of protection, appropriate protection means for the software (e.g., hardware support) that signs or verifies a data set are necessary (see also chapter 5 for software on universal devices, special requirement U6, specifying note 6 for risk class D).</td></tr>
<tr><td colspan="3">Required Documentation:
Description of the protection method.</td></tr>
<tr><td colspan="3">Validation Guidance:
Checks based on documentation:
Check that an appropriate method has been selected.</td></tr>
<tr><td colspan="2">Example of an Acceptable Solution:
• Transmitted measurement data is accompanied by additional redundant information to enable the software of the receiver to detect intentional data transmission errors.
• A checksum is generated of the measurement data set to be transmitted. Just before the measurement data is reused, the value of the checksum is recalculated and compared with the nominal value that is contained in the received data set. If the values match, the data set is valid and may be used, otherwise it shall be deleted or marked invalid.
• An acceptable solution is the CRC-16 algorithm.

<u>Note:</u> The algorithm is not secret but in contrast to requirement T2, the initial vector of the CRC-register or the generator polynomial (i.e. the divisor in the algorithm) is secret. The initial vector and generator polynomial are known only to the programs generating and verifying the checksums. They shall be treated as keys (see T5).</td><td>Example of an Acceptable Solution:
• Transmitted measurement data is accompanied by additional redundant information to enable the software of the receiver to detect intentional data transmission errors.
• Instead of the CRC, a signature is calculated.
• Protection is provided by some transmission protocols, e.g. HTTPS.</td></tr>
<tr><td colspan="3">Additions for Risk Class E</td></tr>
<tr><td colspan="3">Required Documentation (in addition to the documentation required for risk classes B to D):
Source code of the legally relevant software that realises the integrity protection of transmitted data.</td></tr>
<tr><td colspan="3">Validation Guidance (in addition to the guidance for risk classes B to D):
Checks based on the source code:
• Check whether measures taken for guaranteeing integrity of transmitted measurement data are appropriate.</td></tr>
</table>

<table>
<tr><th>Risk Class B</th><th>Risk Class C</th><th>Risk Class D</th></tr>
<tr><td colspan="3">T4: Traceability of transmitted measurement data
Transmitted measurement data to be used for legally relevant purposes shall be capable of being traced back to the measurement and the legally relevant component or module or measuring instrument that generated them.</td></tr>
<tr><td colspan="3">Specifying Notes:
1. This requirement only applies to open networks, not to closed networks.
2. Traceability requires the correct assignment (linking) of measurement data to the measurement that has generated the data.
3. Traceability requires the correct assignment (linking) of measurement data to the measuring instrument that has generated them.
4. Traceability to measurements presupposes an identification of measurements.
5. Traceability to a measuring instrument presupposes an identification of the measuring instrument.
6. The protection shall apply against intentional changes carried out by easily available and manageable software tools.</td></tr>
<tr><td colspan="2"></td><td>7. The protection shall also apply against intentional changes carried out by special sophisticated software tools.
8. Concerning algorithms and minimum key lengths, the requirements or recommendations of the national and international institutions responsible for data security have to be taken into consideration.</td></tr>
<tr><td colspan="3">Required Documentation:
• Description of the authentication means.</td></tr>
<tr><td colspan="3">Validation Guidance:
Checks based on documentation:
Check that authentication means are adequate.</td></tr>
<tr><td colspan="3">Example of an Acceptable Solution:
• Each measurement data set has a unique (sequential) identification number, containing the date when the measurement has been performed (time stamp).
• Each measurement data set contains information about the origin of the measurement data, i.e. serial number or identity of the measuring instrument that generated the value.
• In open networks, authenticity is guaranteed if the measurement data set carries an unambiguous signature. The signature covers all of these fields of the measurement data set.
• The receiver of the data set checks all data for plausibility.</td></tr>
<tr><td colspan="2"></td><td></td></tr>
</table>

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes B to D)**:** Source code of legally relevant software for sending and receiving device.
Validation Guidance (in addition to the guidance for risk classes B to D)**:** *Checks based on the source code:* • Check whether measures taken for guaranteeing the authenticity of transmitted measurement data are appropriate.

<table>
<tr><th>Risk Class B</th><th>Risk Class C</th><th>Risk Class D</th></tr>
<tr><td colspan="3">T5: Confidentiality of keys
Keys and associated information shall be treated as measurement data and shall be kept secret and be protected against .</td></tr>
<tr><td colspan="3">Specifying Notes:
1. This requirement only applies if secret information is used at all.
2. The protection shall apply against read access or changes carried out by easily available and manageable software tools.
3. If the access to the secret keys is prevented by hardware means, no additional software protection means are necessary.
4. Depending on the protection means the secret information may consist of keys, generator polynoms, initial vectors / start values, seeds, etc.</td></tr>
<tr><td colspan="2"></td><td>5. The protection shall apply against read access or changes carried out by special sophisticated software tools.
6. A technical solution with a standard personal computer would not be sufficient to ensure high protection level if there were no appropriate hardware protection means for the key and other secret data (see basic guide for universal devices U6).</td></tr>
<tr><td colspan="3">Required Documentation:
Description of the management of secret information and means for keeping keys and other information secret and preventing their modification.</td></tr>
<tr><td colspan="2">Validation Guidance:
Checks based on documentation:
• Check that the secret information cannot be disclosed or modified.</td><td>Validation Guidance (in addition to the guidance for risk classes B and C):
Checks based on documentation:
• Check whether the measures taken are appropriate with respect to the required state of the art for a high protection level.</td></tr>
<tr><td colspan="2">Example of an Acceptable Solution:
• The secret key and associated information are stored in binary and encrypted format in the executable code of the legally relevant software. The system software does not offer any features to view or edit these data. If the CRC algorithm is used instead of a signature algorithm, the initial vector or generator polynomial play the role of a key.
•</td><td>Example of an Acceptable Solution:
The secret key is stored in a hardware part that can be physically sealed. The software does not offer any features to view or edit these data.</td></tr>
</table>

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes B to D)**:** Source code of legally relevant software that realises key management.
Validation Guidance (in addition to the guidance for risk class D)**:** *Checks based on the source code:* • Check whether measures taken for key management are appropriate.

Risk Class B	Risk Class C	Risk Class D
T6: Receiving, verification and handling of transmitted measurement data *In case measurement data is used for legally relevant purposes, there shall be legally relevant component or module for receiving, verifying and handling transmitted measurement data.*		
Specifying Notes: 1. Though communication protocols normally repeat a data transmission until it succeeds, nevertheless it is possible that a corrupted data set is received. 2. Received measurement data shall indicate an eventual violation of traceability and integrity.		
Required Documentation: • Description of the functions of the receiving software • Description how corrupted data is handled.		
Validation Guidance: *Checks based on documentation and functional checks:* • Check that corrupted data is detected and marked.		
Example of an Acceptable Solution: When the program that is receiving, verifying and handling transmitted data fails to validate the signature, it first tries to reconstruct the original value if redundant information is available. If reconstruction fails, it generates a warning to the user, does not output the measurement value and sets a flag in a special field of the data set (status field) with the meaning “not valid”		

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes B to D)**:** Source code of legally relevant software in the receiving device.
Validation Guidance (in addition to the guidance for risk classes B to D)**:** *Checks based on the source code:* • Check whether measures taken for handling corrupted data are appropriate.

Risk Class B	Risk Class C	Risk Class D
T7: Transmission delay *The measurement shall not be inadmissibly influenced by a transmission delay.*		
Specifying Notes: 1. The timing of the data transmission shall be organised so that under worst case conditions the measurement is not inadmissibly influenced.		
Required Documentation: Description of the concept, how measurement is protected against transmission delay.		
Validation Guidance: • Check the concept that the measurement is not influenced by transmission delay.		
Example of an Acceptable Solution: Implementation of transmission protocols for field buses.		

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes B, C and D)**:** Source code of legally relevant software that realises the data transmission.
Validation Guidance (in addition to the guidance for risk classes B, C and D)**:** *Checks based on the source code:* • Check whether measures taken for handling transmission delay are appropriate.

Risk Class B	Risk Class C	Risk Class D
T8: availability of transmission services *If network services become unavailable, no measurement data shall get lost.*		
Specifying Notes: 1. It shall not be possible to corrupt measurement data by delaying or suppressing transmission. 2. The sending device shall be able to handle transmission disturbances accidentally happening. 3. The reaction of the measuring instrument if transmission services become unavailable depends on the measuring principle (see Extension I).		
Required Documentation: Description of protection measures against transmission interruption or other failures.		
Validation Guidance: *Checks based on documentation:* • Check the measures taken to protect measurement data from transmission disturbances and interruption. *Functional checks:* • Spot checks shall show that no relevant data get lost due to a transmission interruption.		
Example of an Acceptable Solution: 1) Interruptible measurements: The measurement is completed even though the transmission is down. However, the measuring instrument or the device that is sending the measurement data has a buffer that is large enough to store the current measurement. After this no new measurement is started and the buffered values are kept for later transmission. For other examples see part I. 2) Uninterruptible measurements: The cumulative register is read out and transmitted at a later time when the connection is up again.		

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes B to D)**:** Source code of the legally relevant software that realises data transmission.
Validation Guidance (in addition to the guidance for risk classes B to D)**:** *Checks based on the source code:* • Check whether measures taken for reacting on interrupted transmission services are appropriate.

9 Extension S: Software Separation

Software separation is an optional design method that allows to separate legally relevant software from legally non-relevant software. The communication between these parts of software is carried out via controlled interfaces. If following the conditions for software separation, the manufacturer need not to pass conformity assessment procedures when changing legally non-relevant software.

The specific requirements of this extension, if applicable, shall be considered in addition to the basic requirements of types P or type U instruments, respectively, described in Chapters 0 and 5 of this guide.

9.1 Technical description

Software-controlled measuring instruments or systems in general have complex functionality and contain modules that are legally relevant and modules that are not. It is advantageous – though it is not prescribed – to separate these types of software modules.

9.2 Specific software requirements for software separation

Risk Class B	Risk Class C	Risk Class D

S1: Realisation of software separation

There shall be a part of the software that contains all legally relevant software and parameters that is clearly separated from other parts of software.

Specifying Notes:

1. All *software parts* (program units, subroutines, procedures, functions, classes, *programs, libraries etc.).*
   - that contribute to the calculation of measurement values or have an impact on it,
   - that contribute to auxiliary functions such as displaying data, data security, data storage, software identification, performing software download, data transmission or storing, verifying received or stored data etc.

   belong to the legally relevant software.

   All *variables, temporary files and parameters* that have an impact on measurement data or on legally relevant software also belong to the legally relevant software.
2. The protective software interface itself (see S3) is part of the legally relevant software.
3. Legally non-relevant software comprises the remaining program units, data or parameters not covered above.

Required Documentation:

Naming of all components that belong to the legally relevant software.

Validation Guidance:

Checks based on documentation:

- Check that the naming is correct and the list of named components is complete.

Example of an Acceptable Solution:

Additions for Risk Class E

Required Documentation (in addition to the documentation required for risk classes B to D)**:**
Source code of the legally relevant software.

Validation Guidance (in addition to the guidance for risk classes B to D)**:**

Checks based on the source code:

- Check (e.g. by data flow analysis with tools or manually) that all program units, programs or libraries that are involved in processing the measurement values are registered as legally relevant software.

Risk Class B	Risk Class C	Risk Class D
S2: Mixed indication *Information generated by the legally non-relevant software shall be shown on a display or printout in a way that confusions with the information generated by the legally relevant software are avoided.*		
Specifying Notes: ---		
Required Documentation: Description of the legally relevant software that realises the indication. Description of how the indication of legally relevant information is protected against misleading indication generated by legally non-relevant software.		
Validation Guidance: *Functional checks:* • Judge through visual checks that additional information generated by legally non-relevant software and presented on display or printout cannot be confused with the information originating from legally relevant software.		
Example of an Acceptable Solution: • If additional information, part of which is legally not relevant, should be indicated besides the legally relevant information e.g. product identifier, an indication pattern shall be defined which is controlled by the legally relevant software. To ensure that all legally relevant information is extracted from an input string, it should pass through a filter which is part of the legally relevant software that detects inadmissible information, e.g. measurement units. The admissible information is then inserted into the indication pattern controlled by the legally relevant software.		

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes B to D)**:** Source code of the legally relevant software.
Validation Guidance (in addition to the guidance for risk classes B to D)**:** *Checks based on the source code:* • Check that legally relevant software generates the indication of measurement values. • Check whether the realised implementation of mixed indication is correct. • Check that this indication cannot be changed or suppressed by legally non-relevant programs.

Risk Class B	Risk Class C	Risk Class D

S3: Protective software interface

The data exchange between the legally relevant and legally non-relevant software shall be exclusively carried out via a protective software interface.

Specifying Notes:

1. This requirement applies to all kinds of interactions and data exchanges between the legally relevant and legally non-relevant software.
2. All communication shall exclusively be carried out via the defined protective interface.
3. There shall be only those interactions and data flows allowed that do not inadmissibly influence the measuring process, in particular the legally relevant software, device-specific parameters and measurement data.
4. Scheduling and runtime of the measuring process shall not be influenced by legally non-relevant software
5. In case of software separation on a legally relevant operating system, see also O4.

Required Documentation: Description of the software interface

- Description of the interface including description of allowed interactions and data flows.

Validation Guidance:

Checks based on documentation:

- Check that functions of the legally relevant software and actions of the measuring process, that may be triggered via the protective software interface are defined and described.
- Check that data that may be exchanged via the interface are defined and described.
- Undertake plausibility checks that the description of interactions and data exchanges is complete.

Example of an Acceptable Solution:

- The data domains of the legally relevant software part are encapsulated by declaring only local variables in the legally relevant part.
- The interface is realised as a subroutine belonging to the legally relevant software that is called from the legally non-relevant software. The data to be transferred to the legally relevant software are passed as parameters of the subroutine.
- The legally relevant software filters out inadmissible interface commands.

Additions for Risk Class E

Required Documentation (in addition to the documentation required for risk classes B to D)**:**
Source code of the legally relevant software.

Validation Guidance (in addition to the guidance for risk classes B to D)**:**

Checks based on the source code:

- Check the software design whether data flow is unambiguously defined in the legally relevant software and can be verified.
- Check the data flow via the software interface by using appropriate tools or manually. Check whether the complete data flow between the software parts has been documented. Search for inadmissible data flow.
- Check that interactions triggered by the legally non-relevant software are documented. Search for inadmissible interactions.

10 Extension D: Download of Legally Relevant Software

This extension shall be used if instruments are equipped with facilities for a software download without breaking a seal. The specific requirements of this extension, if applicable, are to be considered in addition to the basic requirements of types P or type U instruments, respectively, described in Chapters 0 and 5 of this guide.

This guide does not impose any prescriptions whether a software download to instruments in use without breaking a seal is allowed or not. However, if a download without breaking a seal is allowed, then the specific requirements laid down below shall be considered.

10.1 Technical Description

The scope of configurations, which are in principle suitable for a software download is large. It is described in the following table.

Hardware Configuration The instrument with facilities for a software download may be a built-for-purpose type (type P) or an instrument with a universal device (type U). Communications links for the software transmission may be direct, e.g. RS 232, USB, over closed networks, e.g. Ethernet, token-ring LAN, or over open networks, e.g. Internet.
Software Configuration The entire software to be downloaded may be legally relevant or there may be a separation between legally relevant and legally non-relevant software. In the latter case, only the download of legally relevant software is subject to the requirements laid down below. Download of legally non-relevant software is allowed without any restrictions, provided the software separation has been certified.

Table 10-1: Technical description of configurations for automatic software download.

The software download consists of two (logical) phases: (1) The transmission process to the measuring instrument and (2) the installation of the software transmitted.

10.2 Specific Software Requirements

Risk Class B	Risk Class C	Risk Class D

D1: Download mechanism

Both phases of the software download, the transmission and the subsequent installation of software, shall run automatically and not affect the protection of legally relevant software.

Specifying Notes:

1. The instrument shall be equipped with legally relevant software that carries out the checking functions required in D2 to D4.
2. The instrument shall be capable of detecting if the transmission of software or the subsequent installation fails. A warning shall be given. If the transmission or the installation is unsuccessful or has been interrupted, then the original status of the measuring instrument shall be unaffected. Alternatively, the instrument shall display a permanent error message and its metrological functioning shall be inhibited until the fault has been cleared.
3. On successful completion of the installation, all protective means shall be activated.
4. During transmission and subsequent installation of software, the measurement process shall be inhibited, or correct measurement shall be appropriately guaranteed.
5. The number of retries of transmissions and installation attempts shall be reasonably limited.

Required Documentation:

The documentation shall describe how the conditions given in the specifying notes are implemented.

Validation Guidance:

Check that the conditions given in the specifying notes are fulfilled.

Functional checks:

- Perform at least one software download to check its correct process.

Example of an Acceptable Solution:

The whole legally relevant software part is fixed, i.e. it cannot be downloaded or changed without breaking a seal.

An auxiliary program resident in the legally relevant part of the software that:

a. Handshakes with the sender and checks for consent
b. Automatically inhibits measurement during transmission and installation
c. Automatically transmits the legally relevant software to a secure holding area
d. Automatically carries out the checks required by D2 to D4
e. Automatically installs the software into the correct location
f. Takes care of housekeeping, e.g. deletes redundant files, etc.
g. Ensures that any protection removed to facilitate transmission and installation is automatically replaced to the required level on completion.
h. Initiates the appropriate fault handling procedures if a fault occurs.

For member states where software download for instruments in use is not allowed, it shall be possible to disable the software download mechanism by means of a sealable setting (switch, secured parameter). In this case it must not be possible to download legally relevant software without breaking the seal.

Additions for Risk Class E

Required Documentation (in addition to the documentation required for risk classes B to D)**:**

Part of source code of legally relevant software that is responsible for the management of the download process.

Validation Guidance (in addition to the guidance for risk classes B to D)**:**

Checks based on the source code:

- Check whether measures taken for managing the download process are appropriate.

Risk Class B	Risk Class C	Risk Class D
D2: Authentication of transmitted software *Means shall be employed to guarantee that the transmitted software is authentic.* **Specifying Notes:** 1. Before the transmitted software is installed, it shall be checked that: a. The software is authentic. b. The software belongs to the measuring instrument on which it shall be installed. 2. A negative check result shall be considered as failure of transmission and treated as laid down in D1.		
	3. Concerning algorithms and minimum key lengths, the requirements or recommendations of the national and international institutions responsible for data security have to be taken into consideration.	
Required Documentation: The documentation shall describe how the checks mentioned in the specifying notes are carried out.		
Validation Guidance: *Checks based on documentation:* • Check that the described checks are appropriate *Functional checks:* • Check that installation of not authentic or not to the instrument belonging software is inhibited.		
Example of an Acceptable Solution: 1. **Authenticity:** For integrity reasons (see D3) an electronic signature is generated over the software part to be downloaded. Authenticity is guaranteed if a key stored in the legally relevant software of the instrument confirms that the signature originates from the authorised body. Signature matching is done automatically. The key can only be exchanged by breaking a seal. 2. **Correct type of measuring instrument** Checking the instrument type requires automatically matching an identification of instrument type that is stored in the legally relevant software part of the instrument with a compatibility list attached to the software.		

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes B to D)**:** Source code of the legally relevant software part that is responsible for checking the authenticity.
Validation Guidance (in addition to the guidance for risk classes B to D)**:** *Checks based on the source code:* • Check whether measures are taken for checking the conditions laid down in the specifying notes.

<table>
<tr><th>Risk Class B</th><th>Risk Class C</th><th>Risk Class D</th></tr>
<tr><td colspan="3">D3: Integrity of downloaded software
Means shall be employed to guarantee that the software has not been changed during transmission.</td></tr>
<tr><td colspan="3">Specifying Notes:
1. Before the transmitted software is installed, it shall be checked that the software has not been changed during transmission.
2. A negative check result shall be considered as failure of transmission and treated as laid down in D1.</td></tr>
<tr><td colspan="2"></td><td>3. Concerning algorithms and minimum key lengths, the requirements or recommendations of the national and international institutions responsible for data security have to be taken into consideration.</td></tr>
<tr><td colspan="3">Required Documentation:
The documentation shall describe how the checks are carried out.</td></tr>
<tr><td colspan="3">Validation Guidance:
Checks based on documentation:
• Check that the described check is appropriate.
Functional checks:
• Check that installation of changed software is inhibited.</td></tr>
<tr><td colspan="2">Example of an Acceptable Solution:
• Integrity is demonstrated by calculating a checksum over the legally relevant software and comparing it against the checksum attached to the software.
• Acceptable algorithm: CRC, secret initial vector, length 32 bit. The initial vector is stored in the legally relevant software part.</td><td>Example of an Acceptable Solution:
• SHA with RSA is used as a signature algorithm. The key for decrypting is stored in the legally relevant software part and cannot be exchanged or read out without breaking a seal.</td></tr>
</table>

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes B to D)**:** Source code of that part of legally relevant software that is responsible for checking the integrity of the software.
Validation Guidance (in addition to the guidance for risk classes B to D)**:** *Checks based on the source code:* • Check whether measures taken for checking the integrity are appropriate.

Risk Class B	Risk Class C	Risk Class D
D4: Traceability of legally relevant software download *It shall be guaranteed by appropriate technical means that downloads of legally relevant software are adequately traceable within the instrument for subsequent controls.*		
Specifying Notes: 1. All relevant data making a download or a download attempt traceable shall be recorded and secured. Relevant data includes date and time of download, identifier(s) of software, origin of transmission, success note. 2. The data recorded shall be available for an adequate period of time (the period depends on regulations outside MID). 3. The recorded data shall be presented on demand. 4. The traceability means and records are part of the legally relevant software and shall be protected as such.		
Required Documentation: The documentation shall describe: • how the traceability means are implemented and protected, • the structure of records, • how the recorded data may be presented		
Validation Guidance: *Checks based on documentation:* • Check that implemented traceability means fulfil the conditions laid down in the specifying notes. *Functional checks:* • Check the functionality of the means while carrying out a software download.		**Validation Guidance** (in addition to the guidance for risk classes B and C)**:** *Checks based on documentation:* • Check whether the measures taken are appropriate with respect to the required state of the art for a high protection level.
Example of an Acceptable Solution: • Event logger. The measuring instrument is equipped with an event logger that automatically records at least the date and time of the download, identifier of the downloaded legally relevant software, the identifier of the sending party, and an entry of the success. An entry is generated for each download attempt regardless of the success. • After having reached the limit of the event logger, it is ensured by technical means that further downloads are impossible. Event logger may only be erased by breaking a seal and may be resealed only by the inspection authorities.		

Additions for Risk Class E
Required Documentation (in addition to the documentation required for risk classes B to D)**:** Source code of the legally relevant software part that is responsible for tracing download processes.
Validation Guidance (in addition to the guidance for risk class D)**:** *Checks based on the source code:* • Check whether measures taken for tracing the download process are appropriate. • Check whether measures taken for protecting the recorded data are appropriate.

11 Extension I: Instrument-Specific Software Requirements

This extension is intended to complement the general software requirements of the previous chapters and cannot be considered isolated from parts P or U and the other extensions (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 harmonised interpretation of the MID requirements.

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

For the present, Extension I 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. The numbering x of the sub-chapters 10.x follows the numbering of the specific MID Annex MI-x. Non-MID instruments could be added starting from 10.11.

There are different instrument-specific software aspects that might need consideration for a certain type x of measuring instrument. These aspects should be treated in a systematic manner as follows: Each sub-chapter 10.x should be subdivided into sub-chapters 10.x.y where y covers the following aspects.

10.x.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 guidelines 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 the specific annexes MI-x.

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) of the general software requirements, or whether one (or more) general software requirements is (are) not applicable, and the reason why.

10.x.2 Technical description

Here

- examples of most common specific technical configurations,
- the application of parts P, U and extensions 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), and
- the fault detection and reaction; two cases are possible:
  a) the presence of a defect is obvious or can simply be checked or there are hardware means for fault detection,
  b) the presence of a defect is not obvious and cannot be easily checked and there are no hardware means for fault detection.

  In the latter case (b) fault detection and reaction requires appropriate software means and hence appropriate software requirements.
- the hardware configuration; at least the following issues should be addressed:
  a) Is there a modular, general-purpose computer-based system or a dedicated instrument with an embedded system subject to legal control?
  b) 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?
  c) Is the sensor separated (separate housing and separate power supply) from the type U system or is it partly or completely integrated into it?
  d) Is the user interface always under legal control (both for type P and type U instruments) or can it be switched to an operating mode which is not under legal control?
  e) Is long-term data storage foreseen? If yes, then is the storage local (e.g. hard disk) or remote (e.g. file server)?
  f) 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:
  a) Which operating system is used or can be used?
  b) Do other software applications reside on the system besides the legally relevant software?
  c) Is there software not subject to legal control that is intended to be freely modified after approval?

10.x.3 Specific software requirements

Here, the specific software requirements should be listed and commented using a similar form as in the previous chapters.

10.x.4 Examples of legally relevant parameters, functions, and data

Here, examples of

- 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

may be given.

10.x.5 Other aspects

Here, other 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.

10.x.6 Assignment of risk class

Here, the appropriate risk class for instruments of type x should be defined. This can be done

- either generally (for all categories within the respective type), or
- depending on the field of application, or category, or other aspects if these exist.

11.1 Water Meters

11.1.1 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.

11.1.2 Technical description

11.1.2.1 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.

11.1.2.2 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.

11.1.2.3 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.

11.1.2.4 Fault Detection and Reaction

The requirement Annex III (MI-001), 7.1.2 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 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 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 49:2013-1 A3, A5)

11.1.3 Specific software requirements

Risk Class B	Risk Class C	Risk Class D
I1-1: Fault Recovery *The software shall recover from a disturbance to normal processing.*		
Specifying Notes: Date stamped flags should be raised to help logging of periods of faulty operation.		
Required Documentation: • A brief description of the fault recovery mechanisms and an explanation of how and when it is invoked. • A brief description of the related tests carried out by the manufacturer. • A brief description of SW recovery mechanism steps after an error (from the manufacturer of the meter), if this is required for SW validation.		
Validation Guidance: *Checks based on documentation:* • Check whether the realisation of fault recovery is appropriate. *Functional checks:* • Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		
Example of an Acceptable Solution: A hardware watchdog is reset by a cyclically processed microprocessor subroutine in order to inhibit the firing of the watchdog. If any function has not been processed or – in the worst case – the microprocessor hangs in an arbitrary endless loop, the reset of the watchdog does not happen, and it fires after a certain time span.		

Risk Class B	Risk Class C	Risk Class D
I1-2: Non-legally Relevant Software and Dynamic Behaviour *The legally non-relevant software shall not adversely influence the dynamic behaviour of a measuring process.*		
Specifying Notes: This requirement ensures that for real time applications of meters the dynamic behaviour of the legally relevant software is not inadmissibly influenced by legally non-relevant software, i.e. the resources of the legally relevant software are not inadmissibly reduced by the non-legal part.		
Required Documentation: • Description of the interrupt hierarchy. • Timing diagram of the software tasks. Limits of proportionate runtime for legally non-relevant tasks.		
Validation Guidance: *Checks based on documentation:* • Documentation covering limits of the proportionate runtime for legally non-relevant tasks is available for the programmer of the legally non-relevant software part. *Functional checks:* • Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		
Example of an Acceptable Solution: The interrupt hierarchy is designed in a way that avoids adverse influences.		

Risk Class B	Risk Class C	Risk Class D
I1-3: Additional Functionality[3] *Additional functionality, for example prepayment or interval metering[4], should not influence the legally relevant measurement functions as specified by MID Annex III Water meters (MI-001).*		
Specifying Notes: Additional functionality is allowed provided it does not influence the legally relevant measurement functions as specified by MID, Annex III Water meters (MI-001).		
Required Documentation: See S1 to S3.		
Validation Guidance: See S1 to S3.		
Example of an Acceptable Solution: See S1 to S3.		

Risk Class B	Risk Class C	Risk Class D
I1-4: Back-up Facilities *There may be a facility that provides for periodic back-up of measurement data, such as measurement values and the current status of the process. This data shall be stored in a non-volatile storage.*		
Specifying Notes: 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: • A brief description of which data is backed up and when this occurs. • Calculation of the minimum interval for the back-up to ensure that the critical change value is not exceeded.		
Validation Guidance: *Checks based on documentation:* • Check whether measurement data is saved to non-volatile storage and can be recovered. *Functional checks:* • Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		
Example of an Acceptable Solution: Measurement data is backed up as required.		

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

Risk Class B	Risk Class C	Risk Class D
I1-5: Software Download *During installation of the software, the measurement process should be inhibited for no longer than one minute in total.* *In case that the installation of the software takes more than one minute, extra measures needs to be taken (e.g. installation takes place at low water consumption).*		
Specifying Notes: • This requirement applies in addition to D1, D2, D3 and D4 if software download has been realized. • The additional requirement ensures that for real time applications of the meter measurements are not interrupted for too long.		
Required Documentation: See D1, D2, D3 and D4.		
Validation Guidance: See D1, D2, D3 and D4.		
Example of an Acceptable Solution: See D1, D2, D3 and D4.		

Risk Class B	Risk Class C	Risk Class D
I1-6: MID-Annex I, 8.5 Inhibit Resetting of Cumulative Measurement Values *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: • 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 water meters shall be fitted with all securing provisions as specified by the TEC after which resetting of the cumulative measurement values shall not be possible without evidence of an intervention. • 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 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 measured values. Cumulative registers are not allowed to be reset during use in distribution network. NB: specified in ISO 4064 under 6.8.2. - Electronic sealing devices		
Required Documentation: Documentation of protection means against resetting the volume registers.		
Validation Guidance: *Checks based on documentation:* • Check that the reset operation of the cumulative legally relevant measurement values is secured and that the securing measures foreseen shall provide for evidence of an intervention. *Functional checks:* • Confirm correct functioning of the securing measures foreseen, see also P3/U3 and P4/U4.		
Example of an Acceptable Solution: The register for the total measured quantity has to be protected by a hardware seal. Other registers, for example day or night tariff register, may be protected by the same means as parameters (see P7/U7) provided that a total (overall cumulative) register is available which is protected by a hardware seal. For further information see WELMEC Guide 11.1/13 and ISO 4064 article 6.8.2. – electronic sealing		

Risk Class B	Risk Class C	Risk Class D

I1-7: MID Annex I, article 10.5 Reading of Measurement Results

The measurement results that serve as the basis for the price to pay may be the values 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:

- Cumulative registers or totalised registers of the water meter 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 securing provisions as specified by the TEC by the manufacturer after which resetting of the cumulative measurement values shall not be possible without evidence of an intervention, see I1-6.
- When the maximum indicating range of the volume totalization is reached, the indicating range will continue measuring starting from zero cubic meter, see also I1-9 (Number of Digits).

Required Documentation:

Documentation of how the measurement results are obtained that serves as the basis for the price to pay.

Validation Guidance:

Checks based on documentation:

- Check the correct handling of the measurement results.

Functional checks:

- Confirm correct functioning of the handling of the measurement results.

Example of an Acceptable Solution:

If a meter is designed to count the quantities defined in MID (MI-001) in different registers a meter shall be able to display the total quantities of each register on the display by means of the user interface (see P3/U3, e.g.: buttons on instruments) as well as the currently active rate register. It is allowed to show the results on different displays, periodically or on request via the user interface. However, when displaying different measurement results it shall be clear which display belongs to which register, there shall be no ambiguity in that respect.

If needed, additional inscriptions can be provided on the water meter, clarifying the different registers or indication of test mode (see I1-9).

Risk Class B	Risk Class C	Risk Class D
I1-8: Protection against Intentional Changes for water meters type P (with mechanical register) *The calculated checksum or an alternative indication to support detection of software modification shall be made visible on command for control purposes, see P6. As an exception for water meters of type P with a mechanical counter, an imprint of the checksum or an alternative indication of software modification on the name plate of an instrument shall be an acceptable solution if the following conditions A, B and C are fulfilled:* *A. The user interface does not have any control capability to activate the indication of the value of the checksum or an alternative indication of software modification on the display or the display does not allow technically showing these values (mechanical counter).* *B. The instrument does not have any interface to communicate the software identifier.* *C. After production of a meter a change of the software is not possible or only possible if also the hardware or a hardware part that contains the software is changed.*		
Specifying Notes: • The manufacturer of hardware or relevant part of hardware is responsible that the checksum or an alternative indication of software modification is correctly marked on the concerned hardware. • All other Specifying Notes of P6 apply.		
Required Documentation: According to P6.		
Validation Guidance: *Checks based on documentation:* • According to P6. *Functional checks:* • According to P6.		
Example of an Acceptable Solution: Imprint of the checksum or an alternative indication of software modification on the name plate of the instrument.		

Risk Class B	Risk Class C	Risk Class D

1-9: Number of Digits

The display of total quantity shall have sufficient numbers of digits. According to ISO 4064, part 1 the number of digits displayed are based on permanent flow Q3:

Permanent flow Q3 [m3/h]	*Minimum range of indication [m3]*
Q3 ≤ 6,3	*9 999*
6,3 < Q3 ≤ 63	*99 999*
63 < Q3 ≤ 630	*999 999*
630 < Q3 ≤ 6300	*9 999 999*

Also, according to ISO 4064 part 1 the resolution of the indicating device shall fulfil the following requirement:

- *The subdivisions of the verification scale shall be small enough to ensure that the resolution error of the indicating device does not exceed 0,25 % for accuracy class 1 meters, and 0,5 % for accuracy class 2 meters, of the volume passed during 90 min at the minimum flow rate Q1.*
- *Additional verification elements may be used provided that the uncertainty of reading is not greater than 0,25 % of the test volume for accuracy class 1 meters and 0,5 % of the test volume for accuracy class 2 meters and that the correct functioning of the register is checked.*

Suitability according to clause 7.6 and 10.5 of Annex I of Directive 2014/32/EU (MID):
A measuring instrument shall be designed so as to allow the control of the measuring tasks after the instrument has been placed on the market and put into use. If necessary, special equipment or software for this control shall be part of the instrument.
Also, for a measuring instrument with remotely read it shall in any case be fitted with a metrologically controlled display accessible without tools to the consumer.
When the maximum indicating range of the volume totalization is reached, the indicating range will continue measuring starting from zero cubic meter.

Specifying Notes:

According to ISO 4064 part 1:

- The indicating device of a water 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.
- Every indicating device shall provide means for visual, non-ambiguous verification testing and calibration.
- The visual verification display may have either a continuous or a discontinuous movement.

Required Documentation:

- A description of the display and display menu.
- A description of the visual verification display and an explanation on how to initiate visual verification display.

Validation Guidance:

Functional checks:

- Check if the display of total quantity have a sufficient numbers of digits.
- Initiate the visual verification display and
  - check if the resolution of the visual verification display fulfils the requirements
  - check if special equipment or software for this control is part of the instrument (if relevant).

Example of an Acceptable Solution:

There are on the water meter sufficient number of digits on the display which fulfil both the requirements of the total quantity with the required resolution.

Switching display modes on the indicating device for showing the values for the total quantity with the correct resolution and the "test mode" with additional verification elements. These display modes shall be possible to be displayed by means of:

- the user interface (See P3/U3, e.g.: buttons on instruments) or
- by cycling through the different display modes.

However, it should by clear what the primary display is when using different display modes, it shall be clear how to read these values and there shall be no ambiguity in that respect to the other display modes (See I1-7).

Note: It is not in line with the essential requirements of the Directive 2014/32/EU (MID) according to article 7.6, Annex I, that a verification organisation, inspection body or Notified Body has to ask the manufacturer for the special equipment or the software.

Risk Class B	Risk Class C	Risk Class D
I1-10: Display Test *For verifying the correct function of all segments of the display, a display test shall be possible to be executed.*		
Specifying Notes: The display test is according to ISO 4064: • The meter shall provide visual checking of the entire display which shall have the following sequence: 1) for seven segment type displaying all the elements (e.g. an “eights” test); 2) for seven segment type blanking all the elements (a “blanks” test); **3)** for graphical displays an equivalent test to demonstrate that display faults cannot result in any digit being misinterpreted. • Each step of the sequence shall last at least 1 s.		
Required Documentation: A description of the display test and an explanation on how to initiate such a test.		
Validation Guidance: Initiate the display test and check if visual checking of the entire display is possible.		
Example of an Acceptable Solution: A display test is initiated after a special command by the user interface (See P3/U3, e.g.: buttons on instruments) or is part of the cycling procedure that shows the different display modes.		

11.1.4 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[5].

Parameter	Protected	Settable	Comment
Calibration factor	x		
Linearisation 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 part of the software	x		

11.1.5 Assignment of risk class

The following risk class is considered appropriate and should be applied if software examinations based on this guide are carried out for (software-controlled) active electrical energy meter:

– **Risk class C for instruments of type P**

[5]. With respect to securing a water meter additional guidance is given in WELMEC guide 13.3.

11.2 Gas Meters and Volume Conversion Devices

11.2.1 Specific regulations, standards, normative documents and other WELMEC guides.

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 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.

11.2.2 Technical description

11.2.2.1 Hardware Configuration

Gas meter and conversion devices are usually separate hardware units.
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.

11.2.2.2 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.

11.2.2.3 Measuring Principle

Gas meters continually cumulate the volume or mass flowed 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.

11.2.2.4 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 totalise 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).

11.2.3 Specific software requirements

11.2.3.1 Gas meters and volume converters

Risk Class B	Risk Class C	Risk Class D
I2-1: MID, Annex IV Gas meters and Volume Conversion Devices (MI-002) article 3.1, Fault Recovery *The software shall recover from a disturbance to normal processing.*		
Specifying Notes: Date stamped flags should be raised to help logging of periods of faulty operation.		
Required Documentation: A brief description of the fault recovery mechanisms and an explanation of how and when it is invoked.		
Validation Guidance: *Checks based on documentation:* • Check whether the realisation of fault recovery is appropriate. *Functional checks:* • Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		
Example of an Acceptable Solution: The hardware watchdog is reset by a cyclically processed microprocessor subroutine in order to inhibit the firing of the watchdog.		

Risk Class B	Risk Class C	Risk Class D
I2-2: Legally Non-Relevant Software and Dynamic Behaviour *The legally non-relevant software shall not adversely influence the dynamic behaviour of a measuring process.*		
Specifying Notes: This requirement ensures that for real time applications of meters the dynamic behaviour of the legally relevant software is not inadmissibly influenced by legally non-relevant software, i.e., the resources of the legally relevant software are not inadmissibly reduced by the non-legal part.		
Required Documentation: • Description of the interrupt hierarchy. • Timing diagram of the software tasks. Limits of proportionate runtime for legally non-relevant tasks.		
Validation Guidance: *Checks based on documentation:* • Documentation covering limits of the proportionate runtime for legally non-relevant tasks is available for the programmer of the legally non-relevant software part. *Functional checks:* • Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		
Example of an Acceptable Solution: The interrupt hierarchy is designed in a way that avoids adverse influences.		

Risk Class B	Risk Class C	Risk Class D
I2-3: MID, Annex IV Gas meters and Volume Conversion Devices (MI-002), article 3.1.2 Back-up Facilities *There may be a facility that provides for periodic back-up of measurement data, such as measurement values and the current status of the process. This data shall be stored in a non-volatile storage.*		
Specifying Notes: 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: A brief description of what data is backed up and when this occurs. Calculation of the minimum interval for the back-up to ensure that the critical change value is not exceeded.		
Validation Guidance: *Checks based on documentation:* • Check whether measurement data is saved to non-volatile storage and can be recovered. *Functional checks:* • Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		
Example of an Acceptable Solution: Measurement data is backed up as required.		

Risk Class B	Risk Class C	Risk Class D
I2-4: Additional Functionality[6] *Additional functionality, for example prepayment or interval metering[7], should not influence the legally relevant measurement functions as specified by MID, Annex IV Gas and Volume Conversion Devices Meters (MI-002).*		
Specifying Notes: • Additional functionality is allowed provided it does not influence the legally relevant measurement functions as specified by MID, Annex IV Gas Meters and Volume Conversion Devices (MI-002).		
Required Documentation: See S1 to S3.		
Validation Guidance: See S1 to S3.		
Example of an Acceptable Solution: See S1 to S3.		

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

Risk Class B	Risk Class C	Risk Class D
I2-5: Software Download *During installation of the software, the measurement process should not be suspended longer than one minute in total.* *In case that the installation of the software takes more than one minute, extra measures needs to be taken (e.g. installation takes place at low flow rate).*		
Specifying Notes: • This requirement applies in addition to D1, D2, D3 and D4 if software download has been realised. • The additional requirement ensures that for real time applications of the meter measurements are not interrupted for too long.		
Required Documentation: See D1.		
Validation Guidance: See D1.		
Example of an Acceptable Solution: See D1.		

Risk Class B	Risk Class C	Risk Class D

I2-6: MID-Annex I, article 8.5 (Inhibit Resetting of Cumulative Measurement Values)
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:

. During a conformity assessment procedure according to annex D, F or H1 the utility meters shall be fitted with all securing provisions as specified by the TEC by the manufacturer after which resetting of the cumulative measurement values shall not be possible without evidence of an intervention.

For gas meters the register for the total measured volume has to be protected by hardware metrological seals.

For conversion devices the volume at base conditions has to be protected by hardware metrological seals.

Required Documentation:
Documentation of protection means against resetting the volume registers.

Validation Guidance:

Checks based on documentation:

- Check that the reset operation of the cumulative legally relevant measurement values is secured and that the securing means foreseen shall provide evidence of an intervention.

Functional checks:

- Confirm correct functioning of the securing measures foreseen.

Example of an Acceptable Solution:
For gas meters the register for the total measured volume has to be protected by hardware metrological seals. Other registers, for example day or night tariff register, may be protected by the same means as parameters (see P7/U7) provided that a total (overall cumulative) register is available which is protected by a hardware seal. See WELMEC guide 11.1 and 11.3 for additional guidance.
For conversion devices the volume at base conditions has to be protected by hardware metrological seals. The register showing the volume at measurement conditions can also be protected by the same means as parameters (see P7/U7).
Note: The volume at measurement conditions may be synchronized with the indication of the connected gas meter. Depending on national legislation additional actions have to be taken e.g. re-verifications.

Risk Class B	Risk Class C	Risk Class D

I2-7: MID-Annex I, article 10.5 (Reading of Measurement Results)

A. The measurement results that serve as the basis for the price to pay may be the values 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. The meter should show the values of each register periodically or on request via the user interface

Specifying Notes:

Cumulative registers of a 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 securing provisions as specified by the TEC by the manufacturer after which resetting of the cumulative measurement values shall not be possible without evidence of an intervention.

Required Documentation:

Documentation of how the measurement results are obtained that serves as the basis for the price to pay.

Validation Guidance:

Checks based on documentation:

- Check the correct handling of the measurement results.

Functional checks:

- Confirm correct functioning of the handling of the measurement results.

Example of an Acceptable Solution:

If a meter is designed to count the quantities defined in MID, Annex IV Gas meters and Volume Conversion Devices (MI-002) in different registers the meter shall be able to display the total quantities of each register on the display by means of the user interface (see this guide, for instance buttons on the instrument) as well as the currently active rate register.
An acceptable solution is also to show the results of the different register in different displays, periodically or on request via the user interface. However, when displaying different measurement results it shall be clear which display belong to which register, there shall be no ambiguity in that respect.

Risk Class B	Risk Class C	Risk Class D
I2-8: Protection against Intentional Changes for Gas Meters of Type P with a Mechanical Counter *The calculated checksum or an alternative indication to support the detection of software modification shall be made visible on command for control purposes, see P6, Risk Class C.* *As an exception for gas meters and volume converters type P with a mechanical counter, an imprint of the checksum or an alternative indication of software modification on the name plate of an instrument shall be an acceptable solution if the following conditions A, B and C are fulfilled:* *A. The user interface does not have any control capability to activate the indication of the value of the checksum or an alternative indication of software modification on the display or the display does not allow technically showing the identifier of the software (mechanical counter).* *B. The instrument does not have any interface to communicate the software identifier.* *C. After production of a meter a change of the software is not possible or only possible if also the hardware or a hardware part that contains the software is changed.*		
Specifying Notes: • The manufacturer is responsible that the checksum or an alternative indication of software modification is correctly marked on the concerned hardware. • All other Specifying Notes of P6 apply.		
Required Documentation: According to P6.		
Validation Guidance: *Checks based on documentation:* • According to P6. *Functional checks:* • According to P6.		
Example of an Acceptable Solution: Imprint of the checksum or an alternative indication of software modification on the name plate of the instrument.		

Risk Class B	Risk Class C	Risk Class D
I2-9: MID, Annex IV Gas meters and Volume Conversion Devices (MI-002), article 5.3 Number of Digits (Gas meter and Electronic conversion device) *The display of the total quantity shall have a sufficient number 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: Documentation of the internal representation of the register.		
Validation Guidance: *Checks based on documentation:* • Check that there is sufficient number of numerals that after the volume passed during 8.000 h of flow at Q_{max}, the index has not pass to its initial value.		
Example of an Acceptable Solution: Typical values for domestic gas meters are: Q_{max} = 6 m³/h. The required range is then 48000 m³ requiring 5 digits to fit (currently mechanical and electronic gas meters display up to 99999 m³ which is more than adequate for this size of meter).		

Risk Class B	Risk Class C	Risk Class D
I2-10: MID, Annex IV Gas meters and Volume Conversion Devices (MI-002), article 5.2 Power Source Lifetime *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: Lifetime is used here in the sense of available energy capacity. If the power source can be changed in the field, parameters and measurement data shall not be corrupted during the changeover. Additional warnings before the 90% threshold is reached, is allowed provided that these warnings are not confusing.		
Required Documentation: 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.		
Validation Guidance: *Checks based on documentation:* Check whether the measures taken are appropriate for the surveillance of the energy available.		
Example of an Acceptable Solution: The operating hours or the wake-up events of the device are counted, stored in a non-volatile memory and compared with the nominal value of the battery lifetime. If 90% of the lifetime has elapsed an appropriate warning is shown. The software detects the exchange of the power source and resets the counter. Another solution would be to monitor the health of the power supply continuously. A warning is considered as appropriate in case of a visible warning like a message on the display or a warning indication. In addition, an electronic interface may provide the warning to the network / meter operator. A hidden, “silent” warning (via the electronic interface) to the network / meter operator only is not a sufficient solution.		

10.2.3.2 Gas meters

Risk Class B	Risk Class C	Risk Class D

I2-11: MID, Annex IV Gas meters and Volume Conversion Devices (MI-002), article 5.5 Test Element of the Gas Meter *The gas meter shall have a test element, which shall enable tests to be carried out in a reasonable time.*
Specifying Notes: The test element for accelerating time consuming test procedures is normally used for testing before installation and normal operation. During the test mode the same registers and software parts shall be used as during standard operating mode.
Required Documentation: Documentation of the test element and instructions for activating the test mode.
Validation Guidance: *Checks based on documentation:* Check whether all time consuming test procedures of the gas meter can be completed by means of the test element.
Example of an Acceptable Solution: For test purposes the increment of the test element or pulse shall occur at least every 60 seconds at Q_{min}, see WELMEC Guide 11.1, paragraph 2.4.4. The time base of the internal clock can be accelerated. Processes that last e.g. a week, a month or even a year and overrun of registers may be tested in the test mode within a time span of minutes or hours.

10.2.3.3 Electronic conversion device

Risk Class B	Risk Class C	Risk Class D
I2-12: MID, Annex IV Gas meters and Volume Conversion Devices (MI-002), article 9.1 (Electronic Conversion Device) *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 totalise separately the converted quantity for the time it is operating outside the operating range(s).*		
Specifying Notes: There shall be a display indication of the failure state.		
Required Documentation: Documentation of the different registers for converted quantity and failure quantity.		
Validation Guidance: *Checks based on documentation:* • Check whether the measures taken are appropriate for the management of unusual operating conditions.		
Example of an Acceptable Solution: The software monitors the relevant input values and compares them with predefined limits. If all values are inside the limits the converted quantity is integrated to the normal register (a dedicated variable). Else it totalizes the quantity in another variable. Another solution would be to have only one cumulating register but to record the start and end date, time and register values of the out-of-range period in an event logger (see P7). Both quantities can be indicated. The user can clearly identify and distinguish the regular and the failure indication by means of a status indication.		

Risk Class B	Risk Class C	Risk Class D
I2-13: Recalculation of the Conversion Factor *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 next volume signal is received.*		
Specifying Notes:		
Required Documentation: Documentation of the recalculating sequence.		
Validation Guidance: *Checks based on documentation:* Check whether the measures taken are appropriate.		
Example of an Acceptable Solution:		

11.2.4 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[8].
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***		
Settings 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 part of the 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***		
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 part of the software	***x***		

[8] 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.

11.2.5 Assignment of risk class

The following risk class is considered appropriate and should be applied if software examinations based on this guide are carried out for (software-controlled) gas meters and volume conversion devices:

- **Risk class C for instruments of type P and U.**

11.3 Active Electrical Energy Meters

11.3.1 Specific requirements, 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.

11.3.2 Technical description

11.3.2.1 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.

11.3.2.2 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.

11.3.2.3 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.

11.3.2.4 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.

11.3.3 Specific software requirements

Risk Class B	Risk Class C	Risk Class D
I3-1: MID, Annex V Active Electrical Energy Meters (MI-003), article 4.3.1 Fault Recovery *The software shall recover from a disturbance to normal processing.*		
Specifying Notes: Date stamped flags should be raised to help logging of periods of faulty operation.		
Required Documentation: A brief description of the fault recovery mechanisms and an explanation of how and when it is invoked. And a brief description of the related tests carried out by the manufacturer.		
Validation Guidance: *Checks based on documentation:* • Check whether the realisation of fault recovery is appropriate. *Functional checks:* • Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		
Example of an Acceptable Solution: The hardware watchdog is reset by a cyclically processed microprocessor subroutine in order to inhibit the firing of the watchdog. If any function has not been processed or - in the worst case - the microprocessor hangs in an arbitrary endless loop, the reset of the watchdog does not happen in which case the watchdog fires after a certain time span and resets the microprocessor.		

Risk Class B	Risk Class C	Risk Class D
I3-2: Non-legally Relevant Software and Dynamic Behaviour *The legally non-relevant software shall not adversely influence the dynamic behaviour of a measuring process.*		
Specifying Notes: This requirement ensures that for real time applications of meters the dynamic behaviour of the legally relevant software is not inadmissibly influenced by legally non-relevant software, i.e., the resources of the legally relevant software are not inadmissibly reduced by the non-legal part.		
Required Documentation: • Description of the interrupt hierarchy. • Timing diagram of the software tasks. Limits of proportionate runtime for legally non-relevant tasks.		
Validation Guidance: *Checks based on documentation:* • Documentation covering limits of the proportionate runtime for legally non-relevant tasks is available for the programmer of the legally non-relevant software part. *Functional checks:* • Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		
Example of an Acceptable Solution: The interrupt hierarchy is designed in a way that avoids adverse influences.		

Risk Class B	Risk Class C	Risk Class D
I3-3: Additional Functionality[9] *Additional functionality, for example prepayment or interval metering*[10]*, should not influence the legally relevant measurement functions as specified by MID, Annex V Annex Active Electrical Energy Meters (MI-003), .*		
Specifying Notes: • Additional functionality is allowed provided it does not influence the legally relevant measurement functions as specified by MID, Annex V Active Electrical Energy Meters (MI-003).		
Required Documentation: See S1 to S3.		
Validation Guidance: See S1 to S3.		
Example of an Acceptable Solution: See S1 to S3.		

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

Risk Class B	Risk Class C	Risk Class D
I3-4: MID, Annex V Active Electrical Energy Meters (MI-003), article 4.3.1 Back-up Facilities *There may be a facility that provides for periodic back-up of measurement data, such as measurement values and the current status of the process. This data shall be stored in a non-volatile storage.*		
Specifying Notes: 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: A brief description of what data is backed up and when this occurs. Calculation of the minimum interval for the back-up to ensure that the critical change value is not exceeded.		
Validation Guidance: *Checks based on documentation:* • Check whether measurement data is saved to non-volatile storage and can be recovered. *Functional checks:* • Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		
Example of an Acceptable Solution: Measurement data is backed up as required.		

Risk Class B	Risk Class C	Risk Class D
I3-5: Software Download *During installation of the software, the measurement process should be inhibited for no longer than one minute in total.* *In case that the installation of the software takes more than one minute, extra measures needs to be taken (e.g. installation takes place at low energy consumption).*		
Specifying Notes: • This requirement applies in addition to D1, D2, D3 and D4 if software download has been realised. • The additional requirement ensures that for real time applications of the meter measurements are not interrupted for too long.		
Required Documentation: See D1.		
Validation Guidance: See D1.		
Example of an Acceptable Solution: See D1.		

Risk Class B	Risk Class C	Risk Class D
I3-6: MID-Annex I, 8.5 Inhibit Resetting of Cumulative Measurement Values *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: 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 utility meters shall be fitted with all securing provisions as specified by the TEC by the manufacturer after which resetting of the cumulative measurement values shall not be possible without evidence of an intervention.		
Required Documentation: Documentation of protection means against resetting the energy registers.		
Validation Guidance: *Checks based on documentation:* • Check that the reset operation of the cumulative legally relevant measurement values is secured and that the securing measures foreseen shall provide for evidence of an intervention. *Functional checks:* • Confirm correct functioning of the securing measures foreseen, see also P3/U3 and P4/U4.		
Example of an Acceptable Solution: The register for the total measured quantity has to be protected by a hardware seal. Other registers, for example day or night tariff register, may be protected by the same means as parameters (see P7/U7) provided that a total (overall cumulative) register is available which is protected by a hardware seal. See WELMEC guide 11.1 for additional guidance.		

Risk Class B	Risk Class C	Risk Class D
I3-7: MID-Annex I, article 10.5 Reading of Measurement Results *The measurement results that serve as the basis for the price to pay may be the values 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: Cumulative registers of a 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 securing provisions as specified by the TEC by the manufacturer after which resetting of the cumulative measurement values shall not be possible without evidence of an intervention.		
Required Documentation: Documentation of how the measurement results are obtained that serves as the basis for the price to pay.		
Validation Guidance: *Checks based on documentation:* • Check the correct handling of the measurement results. *Functional checks:* • Confirm correct functioning of the handling of the measurement results.		
Example of an Acceptable Solution: If a meter is designed to count the quantities defined in MID, Annex V Active Electrical Energy Meters (MI-003) in different registers (a) the meter shall be able to display the total quantities of each register on the display by means of the user interface (see this guide, for instance buttons on the instrument) as well as the currently active rate register. It is allowed to show the results on different displays, periodically or on request via the user interface. However, when displaying different measurement results it shall be clear which display belongs to which register, there shall be no ambiguity in that respect.		

Risk Class B	Risk Class C	Risk Class D

I3-8: Protection against Intentional Changes for Active Electrical Energy Meters of Type P with a Mechanical Counter

The calculated checksum or an alternative indication to support detection of software modification shall be made visible on command for control purposes, see P6. As an exception for active electrical energy meters of type P with a mechanical counter, an imprint of the checksum or an alternative indication of software modification on the name plate of an instrument shall be an acceptable solution if the following conditions A, B and C are fulfilled:

A. The user interface does not have any control capability to activate the indication of the value of the checksum or an alternative indication of software modification on the display or the display does not allow technically showing these values (mechanical counter).

B. The instrument does not have any interface to communicate the software identifier.

C. After production of a meter a change of the software is not possible or only possible if also the hardware or a hardware part that contains the software is changed.

Specifying Notes:

- The manufacturer is responsible that the checksum or an alternative indication of software modification is correctly marked on the concerned hardware.
- All other Specifying Notes of P6 apply.

Required Documentation:

According to P6.

Validation Guidance:

Checks based on documentation:

- According to P6.

Functional checks:

- According to P6.

Example of an Acceptable Solution:

Imprint of the checksum or an alternative indication of software modification on the name plate of the instrument.

Risk Class B	Risk Class C	Risk Class D
I3-9: MID, Annex V Active Electrical Energy Meters (MI-003), article 5.2 Number of Digits *The display of the total quantity shall have a sufficient number 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: Documentation of the internal representation of the electrical energy register and auxiliary quantities.		
Validation Guidance: *Checks based on documentation:* Check whether the number of digits is sufficient (internal and on display)		
Example of an Acceptable Solution: Typical values for three phase electricity meters are: Emax (4000h) = 3*60 A * 230 V * 4.000h / 1.000 = 165600 kWh. This requires a presentation of at least 6 digits.		

11.3.4 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[11].

Parameter	***Protected***	***Settable***	***Comment***
Calibration factor	***x***		
Linearization factor	***x***		
Legally relevant configuration of registers	***x***		
Settings of for example • ***Legally relevant parameters of a correction devices, such as parameters based on curve fitting of an active electrical energy meter*** • ***transformer ratio***	***x***		
Other relevant parameters that can or might influence the measurement result	***x***		
Software download of the legally relevant part of the software	***x***		

11.3.5 Assignment of risk class

The following risk class is considered appropriate and should be applied if software examinations based on this guide are carried out for (software-controlled) active electrical energy meter:

– **Risk class C for instruments of type P and U.**

[11] 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.

11.4 Thermal Energy Meters

11.4.1 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.

11.4.2 Technical description

11.4.2.1 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 both. Separate assemblies of thermal energy meters, which has evaluation unit (contain software) shall be to the subject of the validation process also.

11.4.2.2 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.

11.4.2.3 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.

11.4.2.4 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)

11.4.3 Specific software requirements

Risk Class B	Risk Class C	Risk Class D
I4-1: Fault Recovery *The software shall recover from a disturbance to normal processing.*		
Specifying Notes: Date stamped flags should be raised to help logging of periods of faulty operation.		
Required Documentation: • A brief description of the fault recovery mechanisms and an explanation of how and when it is invoked. • A brief description of the related tests carried out by the manufacturer.		
Validation Guidance: *Checks based on documentation:* • Check whether the realisation of fault recovery is appropriate. *Functional checks:* • Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		
Example of an Acceptable Solution: The hardware watchdog is reset by a cyclically processed microprocessor subroutine in order to inhibit the firing of the watchdog. If any function has not been processed or - in the worst case - the microprocessor hangs in an arbitrary endless loop, the reset of the watchdog does not happen in which case the watchdog fires after a certain time span and resets the microprocessor.		

Risk Class B	Risk Class C	Risk Class D
I4-2: Non-legally Relevant Software and Dynamic Behavior *There shall be a facility that provides for periodic back-up of measurement data, such as measurement values and the current status of the process. This data shall be stored in a non-volatile storage.*		
Specifying Notes: This requirement ensures that for real time applications of meters the dynamic behavior of the legally relevant software is not inadmissibly influenced by legally non-relevant software, i.e. the resources of the legally relevant software are not inadmissibly reduced by the non-legal part.		
Required Documentation: • Description of the interrupt hierarchy. • Timing diagram of the software tasks. Limits of proportionate runtime for legally non-relevant tasks.		
Validation Guidance: *Checks based on documentation:* • Documentation covering limits of the proportionate runtime for legally non-relevant tasks is available for the programmer of the legally non-relevant software part. *Functional checks:* • Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		
Example of an Acceptable Solution: The interrupt hierarchy is designed in a way that avoids adverse influences.		

Risk Class B	Risk Class C	Risk Class D
I4-3: Additional Functionality[12] *Additional functionality, for example prepayment or interval metering[13], should not influence the legally relevant measurement functions as specified by MID, Annex VI Annex Thermal energy meters (MI-004).*		
Specifying Notes: Additional functionality is allowed provided it does not influence the legally relevant measurement functions as specified by MID, Annex VI Annex Thermal energy meters (MI-004).		
Required Documentation: See S1 to S3.		
Validation Guidance: See S1 to S3.		
Example of an Acceptable Solution: See S1 to S3.		

Risk Class B	Risk Class C	Risk Class D
I4-4: Back-up Facilities *There may be a facility that provides for periodic back-up of measurement data, such as measurement values and the current status of the process. This data shall be stored in a non-volatile storage.*		
Specifying Notes: 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: • A brief description of what data is backed up and when this occurs. • Calculation of the minimum interval for the back-up to ensure that the critical change value is not exceeded.		
Validation Guidance: *Checks based on documentation:* • Check whether measurement data is saved to non-volatile storage and can be recovered. *Functional checks:* • Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		
Example of an Acceptable Solution: Measurement data is backed up as required.		

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

Risk Class B	Risk Class C	Risk Class D
I4-5: Software Download *During installation of the software, the measurement process should be inhibited for no longer than one minute in total.* *In case that the installation of the software takes more than one minute, extra measures needs to be taken (e.g. installation takes place at low energy consumption).*		
Specifying Notes: • This requirement applies in addition to D1, D2, D3 and D4 if software download has been realized. • The additional requirement ensures that for real time applications of the meter measurements are not interrupted for too long.		
Required Documentation: See D1, D2, D3 and D4.		
Validation Guidance: See D1, D2, D3 and D4.		
Example of an Acceptable Solution: See D1, D2, D3 and D4.		

Risk Class B	Risk Class C	Risk Class D
I4-6: MID-Annex I, 8.5 Inhibit Resetting of Cumulative Measurement Values *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: • 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 provisions as specified by the TEC by the manufacturer after which resetting of the cumulative measurement values shall not be possible without evidence of an intervention. • 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 measured values. Cumulative registers are not allowed to be reset during use in distribution network. NB: specified in EN 1434-1:2015 under 5.10 - Specific requirements on registration devices		
Required Documentation: Documentation of protection means against resetting the energy registers.		
Validation Guidance: *Checks based on documentation:* • Check that the reset operation of the cumulative legally relevant measurement values is secured and that the securing measures foreseen shall provide for evidence of an intervention. *Functional checks:* • Confirm correct functioning of the securing measures foreseen, see also P3/U3 and P4/U4.		
Example of an Acceptable Solution: The register for the total measured quantity has to be protected by a hardware seal. Other registers, for example day or night tariff register, may be protected by the same means as parameters (see P7/U7) provided that a total (overall cumulative) register is available which is protected by a hardware seal. See WELMEC guide 13.1 for additional guidance.		

Risk Class B	Risk Class C	Risk Class D

I4-7: MID-Annex I, article 10.5 Reading of Measurement Results

The measurement results that serve as the basis for the price to pay may be the values 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:

Cumulative registers of a 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 securing provisions as specified by the TEC by the manufacturer after which resetting of the cumulative measurement values shall not be possible without evidence of an intervention.
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 I1-9 (Number of Digits).

Required Documentation:

Documentation of how the measurement results are obtained that serves as the basis for the price to pay.

Validation Guidance:

Checks based on documentation:

- Check the correct handling of the measurement results.

Functional checks:

- Confirm correct functioning of the handling of the measurement results.

Example of an Acceptable Solution:

If a meter is designed to count the quantities defined in MID, Annex VI Thermal energy meters (MI-004) in different registers a meter shall be able to display the total quantities of each register on the display by means of the user interface (See P3/U3, e.g.: buttons on instruments) as well as the currently active rate register. It is allowed to show the results on different displays, periodically or on request via the user interface. However, when displaying different measurement results it shall be clear which display belongs to which register, there shall be no ambiguity in that respect.

If needed, additional inscriptions can be provided on the thermal energy meter, clarifying the different registers or indication of test mode (see I1-9).

Risk Class B	Risk Class C	Risk Class D

I4-8: MID-Annex I, Protection against Intentional Changes for Thermal Energy Meters of Type P with a Mechanical Counter

The calculated checksum or an alternative indication to support detection of software modification shall be made visible on command for control purposes, see P6. As an exception for thermal energy meters of type P with a mechanical counter, an imprint of the checksum or an alternative indication of software modification on the name plate of an instrument shall be an acceptable solution if the following conditions A, B and C are fulfilled:

A. The user interface does not have any control capability to activate the indication of the value of the checksum or an alternative indication of software modification on the display or the display does not allow technically showing these values (mechanical counter).
B. The instrument does not have any interface to communicate the software identifier.
C. After production of a meter a change of the software is not possible or only possible if also the hardware or a hardware part that contains the software is changed.

Specifying Notes:

- The manufacturer is responsible that the checksum or an alternative indication of software modification is correctly marked on the concerned hardware.
- All other Specifying Notes of P6 apply.

Required Documentation:
According to P6.

Validation Guidance:

Checks based on documentation:

- According to P6.

Functional checks:

- According to P6.

Example of an Acceptable Solution:
Imprint of the checksum or an alternative indication of software modification on the name plate of the instrument.

Risk Class B	Risk Class C	Risk Class D

I4-9: Number of Digits

According to EN1434-1:2015 paragraph 6.3.7:
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 3 000 h 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 h shall correspond to at least one digit of lowest significance of the display.

Suitability according to clause 7.6 and 10.5 of Annex I of Directive 2014/32/EU (MID):
A measuring instrument shall be designed so as to allow the control of the measuring tasks after the instrument has been placed on the market and put into use. If necessary, special equipment or software for this control shall be part of the instrument. Also, for a measuring instrument with remotely read it shall in any case be fitted with a metrologically controlled display accessible without tools to the consumer.

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 I1-9 (Number of Digits).

Note: Heat meter can be read as thermal energy meter.

Specifying Notes:

- For the test signal output shall be according to EN1434-2 paragraph 5.3.
- The indicating device of a water 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.
- Every indicating device shall provide means for visual, non-ambiguous verification testing and calibration.
- The visual verification display may have either a continuous or a discontinuous movement.

Required Documentation:

- Documentation of the internal representation of the calculator of energy, temperature sensor, and flowmeters.
- A description of the display and display menu.
- A description of the visual verification display and an explanation on how to initiate visual verification display.

Validation Guidance:

Checks based on documentation:

- Check whether the number of digits is sufficient (internal and on display).

Functional checks:

- Check if the display of total quantity have a sufficient numbers of digits.
- Initiate the visual verification display and
  - check if the resolution of the visual verification display fulfils the requirements
  - check if special equipment or software for this control is part of the instrument (if relevant).

Example of an Acceptable Solution:

There are on the thermal energy meter sufficient number of digits on the display which fulfil both the requirements of the total quantity with the required resolution.

Switching display modes on the indicating device for showing the values for the total quantity with the correct resolution and the "test mode" with additional verification elements. These display modes shall be possible to be displayed by means of:

- the user interface (See P3/U3, e.g.: buttons on instruments) or
- by cycling through the different display modes.

However, it should by clear what the primary display is when using different display modes, it shall be clear how to read these values and there shall be no ambiguity in that respect to the other display modes (See I1-7).

Note: It is not in line with the essential requirements of the Directive 2014/32/EU (MID) according to article 7.6, Annex I, that a verification organisation, inspection body or Notified Body has to ask the manufacturer for the special equipment or the software.

Risk Class B	Risk Class C	Risk Class D
I4-10: Display Test *For verifying the correct function of all segments of the electronic display, a display test shall be possible to be executed.*		
Specifying Notes: The display test is: • The meter shall provide visual checking of the entire display which shall have the following sequence: 1) for seven segment type displaying all the elements (e.g. an “eights” test); 2) for seven segment type blanking all the elements (a “blanks” test); 3) for graphical displays an equivalent test to demonstrate that display faults cannot result in any digit being misinterpreted. • Each step of the sequence shall last at least 1 s.		
Required Documentation: A description of the electronic display test and an explanation on how to initiate such a test.		
Validation Guidance: Initiate the display test and check if visual checking of the entire display is possible.		
Example of an Acceptable Solution: A display test is initiated after a special command by the user interface (see P3/U3, e.g.: buttons on instruments) or is part of the cycling procedure that shows the different display modes.		

11.4.4 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[14].

Parameter	Protected	Settable	Comment
Calibration factor	x		
Linearisation 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 part of the software	x		

11.4.5 Assignment of risk class

The following risk class is considered appropriate and should be applied if software examinations based on this guide are carried out for (software-controlled) thermal energy meter:

- **Risk class C for instruments of type P**

[14] 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.

11.5 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.

11.5.1 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.

11.5.2 Technical description

11.5.2.1 Hardware configuration

Measuring systems for continuous and dynamic measurement of quantities of liquids other than water are either built-for-purpose device (type P in this document) or could consist of several parts, including universal devices (Type U in this document).

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 extension T must be applied.

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.

11.5.2.2 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.

11.5.2.3 Measurement principles

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.

11.5.2.4 Error detection and troubleshooting

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 and software components. 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.

11.5.3 Specific software requirements

Risk Class B	Risk Class C	Risk Class D

I5-1: Fault Recovery

Non-interruptible measuring systems shall be designed and manufactured in such a way that no significant faults occur when they are exposed to the disturbances. The detection by the checking facilities of incorrectness in the generation, transmission, processing and/or indication of measurement data shall result in appropriate action.

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.*

Specifying Notes:

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.

If the checking facilities of an interruptible electronic measuring systems detect significant faults 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.

Additional requirement is stated in OIML R117-1:2019 section A.1.5 regarding fault generation parameters.

Required Documentation:

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.
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.

Validation Guidance:

Checks based on documentation:

- Check whether the realization of fault recovery is appropriate.

Functional checks:

- Confirm correct functioning in the presence of defined influencing quantities and provoked errors.

Example of an acceptable solution:

The hardware watchdog is reset by a cyclically processed microprocessor subroutine in order to inhibit the firing of the watchdog.
If any function has not been processed or - in the worst case - the microprocessor hangs in an arbitrary endless loop, the reset of the watchdog does not happen in which case the watchdog fires after a certain time span and resets the microprocessor.

Risk Class B	Risk Class C	Risk Class D
I5-2: Legally non-relevant Software and Dynamic Behaviour *The legally non-relevant software shall not inadmissibly influence the dynamic behaviour of a measuring process.*		
Specifying Notes: This requirement ensures that for real time applications of meters the dynamic behaviour of the legally relevant software is not inadmissibly influenced by legally non-relevant software, i.e. the resources of the legally relevant software are not inadmissibly reduced by the legally non-relevant part.		
Required Documentation: • Description of the interrupt hierarchy. • Timing diagram of the software tasks. Limits of proportionate runtime for legally non-relevant tasks.		
Validation Guidance: *Checks based on documentation:* • Documentation covering limits of the proportionate runtime for legally non-relevant tasks is available for the programmer of the legally non-relevant software part. *Functional checks:* • Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		
Example of an acceptable solution: The interrupt hierarchy is designed in a way that avoids adverse influences.		

Risk Class B	Risk Class C	Risk Class D
I5-3: Additional Functionality[15] *Additional functionality should not influence the legally relevant measurement functions as specified by MID Annex VII (MI-005).*		
Specifying Notes: Additional functionality is allowed provided it does not influence the legally relevant measurement functions as specified by MID, Annex VII (MI-005).		
Required Documentation: See P8, U8 and S1 to S3.		
Validation Guidance: See P8, U8 and S1 to S3.		
Example of an acceptable solution: See P8, U8 and S1 to S3.		

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

Risk Class B	Risk Class C	Risk Class D
I5-4: Back-up facilities *In the case of non-interruptible measuring systems there may be a facility that provides for periodic back-up of measurement data, such as measurement values and the current status of the process. This data shall be stored in a non-volatile storage.* *The measuring system must be equipped with a backup source to ensure that all measuring functions are carried out in the event of failure of the main power supply, or it must be equipped with means to preserve and display the data so that the ongoing transaction can be terminated.*		
Specifying Notes: The storage interval must be short enough that the difference between current and stored cumulative values is small.		
Required Documentation: • A brief description of what data is backed up and when this occurs. • Calculation of the maximum error that can occur when you back up the cumulative values.		
Validation Guidance: *Checks based on documentation:* • Check whether measurement data is saved to non-volatile storage and can be recovered. *Functional checks:* • Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		
Example of an acceptable solution: • Measurement data is backed up periodically (frequency depending on application) on a non-volatile storage on a memory device. • A hardware watchdog fires when it is not cyclically reset. This alarm actuates an interrupt in the microprocessor. The assigned interrupt routine at once collects measurement values, state values and other relevant data and stores them in a non-volatile storage e.g. an EEPROM or other appropriate storage. *Note:* It is assumed that the watchdog interrupt has highest interrupt priority and can dominate any normal processing or any arbitrary endless loop, i.e., the program control always jumps to the interrupt routine if the watchdog fires.		

Risk Class B	Risk Class C	Risk Class D
I5-5: Software Download *During installation of the software, the measurement process shall be inhibited, or correct measurement shall be appropriately guaranteed.*		
Specifying Notes: • This requirement applies in addition to D1, D2, D3 and D4 if software download has been realized. • The additional requirement ensures that for real time applications of the meter measurements are not interrupted.		
Required Documentation: See D1, D2, D3 and D4.		
Validation Guidance: See D1, D2, D3 and D4.		
Example of an acceptable solution: See D1, D2, D3 and D4.		

Risk Class B	Risk Class C	Risk Class D

I5-6: Imprinted Software Identifier

The software identifier is usually presented on a display. As an exception for measuring systems for liquids other than water, an imprint of the software identifier on the type plate shall be an acceptable solution if the following conditions A, B and C are fulfilled:

A. The user interface does not have any control capability to activate the indication of the value of the checksum or an alternative indication of software modification on the display or the display does not allow technically showing these values (mechanical counter).

B. The instrument does not have any interface to communicate the software identifier.

C. After production of a meter a change of the software is not possible or only possible if also the hardware or a hardware part that contains the software is changed.

Specifying Notes:

- The tag showing the software identifier shall be non-erasable and non-transferable
- The manufacturer of the hardware or the concerned hardware part is responsible that the software identifier is correctly marked on the concerned hardware.
- All other Specifying Notes of P6 apply.

Required Documentation:

According to P2/U2.

Validation Guidance:

Checks based on documentation:

- According to P2/U2.

Functional checks:

- According to P2/U2.

Example of an acceptable solution:

Imprint of the software identifier on the type plate of the instrument.

Risk Class B	Risk Class C	Risk Class D

I5-7: Parameter Settings

- *For the purpose of verification, it shall be possible to display or print the current parameter settings that fix the legally relevant characteristics of the measuring system.*
- *The parameters shall be secured, see P7 and U7. In the case of an event logger the time stamp shall be read from the clock of the device. The setting of the time and date shall be secured.*

Specifying Notes:

These requirements are stated in OIML R117-1:2019 section A.1.3.3.

Required Documentation:

Information regarding the parameter settings and verification possibilities.

Validation Guidance:

Check the parameter settings and verification possibilities of the measuring instrument.

Example of an acceptable solution:

The above criteria shall be met.

Risk Class B	Risk Class C	Risk Class D
I5-8: Ancillary and additional devices (AAD) *When AAD is part of measuring device that is possible to disconnect (deinstall/remove/unmount) then extension T shall be applied.*		
Specifying Notes: In cases when measuring devices contains AAD without legally relevant software then data from AAD with legally non-relevant software must be clearly distinguishable from data from AAD with legally relevant software. In cases when AAD with the legally relevant software has the possibility of being disconnected without breaking a seal that secures the connection to the measuring device then extension T shall be applied.		
Required Documentation: • The list of ADD which contains legally relevant software with description. • According to extension T. • According to extension S (if applicable).		
Validation Guidance: *Checks based on documentation:* • According to extension T. • According to extension S (if applicable). • Check if documentation contains complete list of ADD with LRSW. *Functional checks:* • According to extension T. • According to extension S (if applicable).		
Example of an acceptable solution:		

11.5.4 Examples of legally relevant parameters, functions and data[16]

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

Parameter	Protected	Settable	Comment
Calibration factor	x		
Linearisation 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, Re-setting 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 temper-ature sensors • Fuel type or density	x		

[16] See also WELMEC guide 10.6: Guide for securing of Fuel Dispensers

• Assignment of temperature sensors to individual nozzles • Configuration of the mass meter • Setting the zero point of the mass meter			
Software download of the legally relevant part of the software	x		
Software setting/configuration in case of pulse signals	x		
Software setting/configuration in case of digital data	x		

11.5.5 Assignment of risk class

The following risk class is considered appropriate and should be applied if software examinations based on this guide are carried out for (software-controlled) measuring systems for liquids other than water:

- **Risk class C for instruments of type P and U**

11.6 Weighing Instruments

Weighing instruments are divided into two main categories:

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

While most AWIs are governed by the MID, NAWIs are not; they are still governed by the European Directive 90/384/EEC. **Therefore, the software guide WELMEC 7.5applies 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.

11.6.1 Specific regulations, standards and other normative documents

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

- Automatic catchweighers (R51)
- Automatic gravimetric filling instruments (R61)
- Discontinuous totalisers (R107)
- Continuous totalisers (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)

AWIs of all categories may be realised as type P or type U, and all extensions could be relevant for each category.

However, of these 6 categories, only **discontinuous totalisers** and **continuous totalisers** (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 fault occurs.

11.6.2 Technical description

11.6.2.1 Hardware Configuration

A discontinuous totaliser is a totalising 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 totaliser 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.

11.6.2.2 Software Configuration

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

11.6.2.3 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.

11.6.2.4 Defects

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

11.6.3 Specific software requirements (Discontinuous and Continuous Totalisers)

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.

Risk Class B	Risk Class C	Risk Class D
I6-1: Fault Detection *The software shall detect that normal processing is disturbed.*		
Specifying Notes: On detection of a fault: a. The cumulative measurement and other relevant legal data shall be automatically saved to non-volatile storage (see Requirement I6-2), and b. the hopper weigher or belt weigher shall be stopped automatically, or a visible or audible alarm signal shall be given (see Required Documentation)		
Required Documentation: 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. 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.		
Validation Guidance: *Checks based on documentation:* • Check whether the realisation of fault detection is appropriate. *Functional checks:* • If possible: simulate certain hardware faults and check whether they are detected and reacted upon by the software as described in the documentation.		
Example of an Acceptable Solution: A hardware watchdog is reset by a cyclically processed microprocessor subroutine in order to inhibit the firing of the watchdog. Before resetting, the subroutine checks the health of the system e.g., whether all legally relevant subroutines have been processed during the last interval. If any function has not been processed or - in the worst case - the microprocessor hangs in an arbitrary endless loop, the reset of the watchdog does not happen, and it fires after a certain time span.		

Risk Class B	Risk Class C	Risk Class D

I6-2: Back-up Facilities

There shall be a facility that provides for the back-up of measurement data, such as measurement values, and the current status of the process in case of a disturbance.

Specifying Notes:

a. The state characteristics and important data shall be stored in a non-volatile storage.

b. 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 values shall be within a defined fraction of the maximum permissible error (see Required Documentation).

c. 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:

A brief description of the back-up mechanism and the data that are backed up, and when this occurs. Specification or calculation of the maximum error that can occur for cumulative values if a cyclical (periodic) back-up is realised.

Validation Guidance:

Checks based on documentation:

- Check back-up facilities.

Functional checks:

- Check by simulating a disturbance whether back-up mechanism works as described in the documentation.

Example of an Acceptable Solution:

A hardware watchdog fires when it is not cyclically reset. This alarm actuates an interrupt in the microprocessor. The assigned interrupt routine at once collects measurement values, state values and other relevant data and stores them in a non-volatile storage e.g., an EEPROM or other appropriate storage.

Note: It is assumed that the watchdog interrupt has highest interrupt priority and can dominate any normal processing or any arbitrary endless loop, i.e., the program control always jumps to the interrupt routine if the watchdog fires.

11.6.4 Examples of legally relevant parameters, functions, and data

Table 11-1: 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). VV indicates variable values.

Functions/data	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)	VV	X		X		X	X	X
Tare, preset tare	VV		X	X	X	X	X	
Unit price, price to pay	VV			X		X		X
Weight value in internal resolution	VV	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			X	X	X	X		
automatic/non-automatic operation,							X	
zero-setting/totalizing		X						X
Record of access to dynamic setting	TF (VV)		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	VV		X	X			X	
Preset weight value	VV		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 fault (if not 1e or 1d)	DD (TD)	X			X			
Limiting value of battery power	DD (TD)	X	X	X	X	X	X	X

Table 11-1: Examples of legally relevant, device-specific and type-specific functions and data

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 realised in each instrument.

11.6.5 Other aspects

None

11.6.6 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 regardless of the type (P or U).

However, as a result of the WG 7 questionnaire (2004), the following differentiation with regard to type P and U instruments, and to discontinuous and continuous totalising instruments (=“totalisers”) seems appropriate:

- **Risk class B for type P instruments (except totalisers)**
- **Risk class C for type U instruments and totalisers type P and U**

11.7 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.

11.7.1 Specific regulations, standards and 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.

11.7.2 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 (type P) in the sense of this guide or an architecture using universal devices (type U).

11.7.3 Specific software requirements

MID Annex IX, 4:

> A taximeter shall be able to supply the following data through an appropriate secured interface(s):
>
> — operation position: ‘For Hire’, ‘Hired’ or ‘Stopped’;
>
> — totaliser data according to paragraph 15.1;
>
> — 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.

Risk Class B	Risk Class C	Risk Class D
I7-1: Back-up Facilities *There shall be a facility that automatically backs-up essential data, e.g., measurement values and the current status of the process if the voltage drops for a longer period.*		
Specifying Notes: 1) This data should normally be stored in non-volatile storage. 2) A voltage level detector to detect when to store measurement values is necessary. 3) 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: A brief description of which data is backed up and when this occurs.		
Validation Guidance: *Checks based on documentation:* • Check whether all legally relevant data are saved in case of a disturbance. *Functional checks:* • Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		
Example of an Acceptable Solution: The voltage level detector fires an interrupt when the voltage level drops for a time of 15 s. The assigned interrupt routine collects measurement values, state values, and other relevant data and stores them in a non-volatile storage e.g., EEPROM. After the voltage level rises again the data is restored and the functioning continues or is stopped (see MI-007, 9.) *Note:* It is assumed that the voltage level interrupt has a high interrupt priority and can dominate any normal processing or any arbitrary endless loop, i.e., the program control always jumps to the interrupt routine if the voltage drops.		

Risk Class B	Risk Class C	Risk Class D
7-2: Long term storage *There shall be a facility that automatically stores the totalised values if disconnected from power.*		
Specifying Notes: 1) The totalised values should normally be stored in non-volatile storage. 2) The facility shall store the totalised values continuously or with an update rate covering the time to detect power down until the (internal) voltage drops below the operating voltage.		
Required Documentation: A brief description of which data is stored and when this occurs.		
Validation Guidance: *Checks based on documentation:* • Check whether all totalised values are saved in case disconnection from power. *Functional checks:* • Confirm correct functioning in the presence of defined influencing quantities and provoked errors.		
Example of an Acceptable Solution: The voltage level detector fires an interrupt when the voltage level drops. The assigned interrupt routine collects totalised values and stores them in a non-volatile storage before the internal voltage drops below the operating level. Or the totalised values are stored continuously in a non-volatile storage. *Note:* It is assumed that the voltage level interrupt has a high interrupt priority and can dominate any normal processing or any arbitrary endless loop, i.e., the program control always jumps to the interrupt routine if the voltage drops.		

Risk Class B	Risk Class C	Risk Class D
I7-3: fraudulent alterations *There shall be a facility that checks the plausibility of the distance measurement signals.*		
Specifying Notes: 1) The facility shall include appropriate routines to check that the pulses or information received are plausible.		
Required Documentation: A brief description of how the routines check the plausibility.		
Validation Guidance: *Checks based on documentation:* • Check if the routines check the plausibility and how. *Functional checks:* • Confirm correct functioning in the presence of provoked errors.		
Example of an Acceptable Solution: The output of the distance signal generator is continuously checked on its defined characteristics regarding voltage level, pulse width and the relation of speed and frequency (stability of the signal). *Note:* the output could be digital information, for example from the CAN bus of the vehicle.		

11.7.4 Examples of legally relevant parameters, functions, and data

In addition to the functions mentioned in 10.7.2 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
annex IX, 4:	
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)

11.7.5 Other aspects

It is recommended that the Automotive Directive is revised, or any other regulation is made to give requirements for the distance signal generators of vehicles used as taxi. A preliminary proposal reads:

For vehicles intended to be used as taxi the following requirements apply:

1. The distance signal generator shall give a signal with a resolution of at least 2 m.
2. The distance signal generator shall give a stable signal at every speed travelled.
3. The distance signal generator shall have defined characteristics regarding voltage level, pulse width and the relation of speed and frequency.
4. Testability…

11.7.6 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 type P instruments**
- **Risk class D for type U instruments**

11.8 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.

11.9 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.

10.9.1 - 10.9.5 will be filled in if considered necessary in the future.

10.9.6 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 type P instruments**
- **Risk class C for type U instruments**

11.10 Exhaust Gas Analysers

Exhaust Gas Analysers 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.

10.10.1 - 10.10.5 will be filled in if considered necessary in the future.

10.10.6 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 analysers:

- **Risk class B for type P instruments**
- **Risk class C for type U instruments**

12 Pattern for Test Report (Including Checklists)

This is a pattern for a test report, which consists of a main part and two annexes. The main part contains general statements on the object under test. It must be correspondingly adapted in practice. The annex 1 consists of two checklists to support the selection of the appropriate parts of the guide to be applied. The annex 2 consists of specific checklists for the respective technical parts of the guide. They are recommended as an aid for manufacturer and examiner to prove that they have considered all applicable requirements.

In addition to the pattern of the test report and the checklists, the information required for the type examination certificate is listed in the last sub-chapter of this chapter.

12.1 Information to be included in the certificate

While the entire test report is a documentation of the object under test, the validation carried out and the results, a certain selection of the information contained in the test report are required for certificate. This concerns the following information, which should be appropriately included in the certificate concerning software:

1. **Software type**
   - Indicate the version of WELMEC Guide 7.2, Type (P or U), the Risk Class (A to E) and the applicable Extensions (L, T, S, D, Ix)

Risk class [A-E]	P	U	L	T	S	D	Ix
_	☐	☐	☐	☐	☐	☐	☐ [1-6] _

Figure 12-1: Indication of the selected Type, the Risk Class as well as applicable Extensions

2. **Software identification**
   - Indicate the validated value(s) of the legally relevant software identifier(s).
   - Describe how to view the legally relevant software identifier(s).

3. **Integrity software verification**
   - For risk classes C and more, indicate the checksum or alternative method with the same level of requirement.
   - For risk class C and more, describe precisely how to view the checksum or alternative method with the same level of requirements.
   - Note: A reference to a document (e.g., user manual) is not suitable.
   - Describe how to view the event counters / event loggers, if applicable.
   - Description of hardware sealing(s) and other types of sealing(s) in relation with software, if applicable.
   - Other means of integrity protection, if applicable.

4. Software environment short description

- Indicate relevant information concerning:
- Software operating environment necessary to operate the software (e.g., Operating System).
- Software modules under legal control (if software separation implemented).
- Hardware and software interfaces (e.g., infrared, Bluetooth, Wireless LAN…).
- Electronic (hardware) parts references and their locations in the measuring instrument including its securing, if needed.

12.2 Pattern for the general part of the test report

Test report no XYZ122344

Flow meter Dynaflow model DF101

Validation of Software

(n annexes)

Commission

The Measuring Instruments Directive (MID) gives the essential requirements for certain measuring instruments used in the European Union. The software of the measuring instrument was validated to show conformance with the essential requirements of the MID.

The validation was based on the report WELMEC MID Software Requirements Guide WELMEC Guide 7.2, where the essential requirements are interpreted and explained for software. This report describes the examination of software needed to state conformance with the MID.

Client

Dynaflow
P.O. Box 1120333
100 Reykjavik
Iceland
Reference: Mr Bjarnur Sigfridson

Test Object

The Dynaflow flow meter DF100 is a measuring instrument intended to measure flow in liquids. The intended range is from 1 l/s up to 2000 l/s. The basic functions of the instrument are:

- measuring of flow in liquids
- indication of measured volume
- interface to transducer

According to the WELMEC Guide 7.2 version yyyy, the flow meter is described as follows:

- a built-for-purpose Measuring instrument (an embedded system)
- long-term storage of measurement data

The flow meter DF100 is an independent instrument with a transducer connected. The transducer is fixed to the instrument and cannot be disconnected. The measured volume is indicated on a display. No communication with other devices is possible.

Page 1 / 4

Software Type

Risk Class [A-E]	P	U	O	L	T	S	D	Ix [1-6]
C	x			x				I1

The embedded software of the measuring instrument was developed by

Dynaflow, P.O. Box 1120333, 100 Reykjavik, Iceland.

Software Identification

The version of the software validated is **V1.2c**. The checksum is 0xA07GT… (CRC32). Software version and checksum can be checked on the LCD display vit button push if the meter is turned on.

The source code comprises following files:

main.c	12301 byte	23 Nov 2003
int.c	6509 byte	23 Nov 2003
filter.c	10897 byte	20 Oct 2003
input.c	2004 byte	20 Oct 2003
display.c	32000 byte	23 Nov 2003
Ethernet.c	23455 byte	15 June 2002
driver.c	11670 byte	15 June 2002
calculate.c	6788 byte	23 Nov 2003

The validation has been supported by following documents from the manufacturer:

- DF 100 User Manual
- DF 100 Maintenance Manual
- Software description DF100 (internal design document, dated 22 Nov 2003)
- Electronic circuit diagram DF100 (drawing no 222-31, date 15 Oct 2003)

The final version of the test object was delivered to National Testing & Measurement Laboratory on 25 November 2003.

Integrity Software Verification

- For risk classes C and more, indicate the checksum or alternative method with the same level of requirement.
- For risk class C and more, describe precisely how to view the checksum or alternative method with the same level of requirements.
- Note: A reference to a document (e.g. user manual) is not suitable.
- Describe how to view the event counters / event loggers, if applicable.
- Description of hardware sealing(s) and other types of sealing(s) in relation with software, if applicable.
- Other means of integrity protection, if applicable.

Software Environment Short Description

- Indicate relevant information concerning:
- Software operating environment necessary to operate the software (e.g. Operating System).
- Software modules under legal control (if software separation implemented).
- Hardware and software interfaces (e.g. infrared, Bluetooth, Wireless LAN…).
- Electronic (hardware) parts references and their locations in the measuring instrument including its securing, if needed.

Examination Procedure

The validation has been performed according to the WELMEC 7.2 Software Guide 2022 (downloaded at www.welmec.org).

The validation was performed between 1 November and 23 December 2021. A design review was held on 3 December by Dr K. Fehler at Dynaflow head office in Reykjavik. Other validation work has been carried out at the National Testing & Measurement Lab by Dr K. Fehler and M. S. Problème.

Following requirements have been validated:

- Specific requirements for embedded software for a built-for-purpose measuring instrument (type P)
- Extension L: Long-term storage for measurement data

Checklist for the selection of the configuration is found in annex 1 to this report.

Risk class C has been applied to this instrument.

Following validation methods have been applied:

- completeness of the documentation
- examination of the operating manual
- functional testing
- software design review
- review of software documentation
- data flow analysis

simulation of input signals

Result

Following requirements of the WELMEC Software Guide 7.2 have been validated without finding faults:

- P1, P2, P3, P5, P6, P7, P8
  (Requirement P4 is considered to be non-applicable.)
- L1, L2, L3, L4, L5, L6, L7, L8

Checklists for the P-requirements are found in annex 2.1 of this report.

Checklists for the L-requirements are found in annex 2.2 of this report.

Two commands which were not initially described in the operator's manual were found. The two commands have been included in the operator's manual dated 10 December 2003.

A software fault which limited the month of February to 28 days also in leap year was found in software package V1.2b. This has been corrected in V1.2c.

The software of the Dynaflow DF100 V1.2c fulfils the essential requirements of the Measuring Instruments Directive.

The result applies to the tested item only.

National Testing & Measurement Lab
Software Department

Dr. K.E.I.N. Fehler
Technical manager

M. S.A.N.S Problème
Technical Officer

Date: 23 December 2003

Page 4 / 4

12.3 Annex 1 of the test report: Checklists to support the selection of the appropriate requirement Sets

The first checklist supports the user to decide which of basic configuration P or U applies for the instrument under test.

Decision on Instrument Type				
		(P)		**Remarks**
1	Is the entire application software constructed for the measuring purpose?			
		(Y)		
2	Are the requirements for the inclusion of an operating system or subsystems of it fulfilled?			
		(Y)		
3	Is the user prevented from accessing the operating system if it is possible to switch to an operating mode not subject to legal control?			
		(Y)		
4	Are the implemented programs and the software environment invariable (apart from updates)?			
		(Y)		
5	Are there any means for programming?			
		(N)		
Tick the empty boxes, as appropriate				

If and only if all answers to the 5 questions can be given as in the (P) column, then the requirements of the part P (Chapter 0) apply. In all other cases the requirements of the part U (Chapter 5) are necessarily to apply.

The second checklist supports to decide which of the IT configuration applies for the instrument under test.

Decision on Required Extensions					
Req. Extension		**YES**	**NO**	**Not Applicable**	**Remarks**
L	Does the device have the ability to store the measurement data either on an integrated storage or on a storage of universal device or on a remote or removable storage?				
T	Is measurement data transmitted via communication networks to a distant device where it is further processed and/or used for legally relevant purposes?				
S	Are there software parts with functions not subject to legal control AND are these software parts desired to be changed after type approval?				
D	Is loading of software possible or desired after putting the measuring instrument into use?				
Consider the required extension for each question answered with YES!					

12.4 Annex 2 of the test report: Specific checklists for the respective technical parts

1) Checklist of basic requirements for type P instrument

Checklist for Type P Requirements						
Requirement	**Testing procedures**		**Passed**	**Failed**	**Not Applicable**	**Remarks***
P1		Does the required manufacturer documentation fulfil the requirement P1 (a-f)?				
P2		Is a software identification realised as required in P2?				
P3		Are commands entered via the user interfaces prevented from inadmissibly influencing the legally relevant software and measurement data?				
P4		Do commands input via communication interfaces of the instrument not inadmissibly influence the legally relevant software, device-specific parameters and measurement data?				
P5		Are legally relevant software and measurement data protected against accidental or unintentional changes?				
P6		Is the legally relevant software secured against the inadmissible, intentional modification, loading or swapping of hardware memory?				
P7		Are legally relevant parameters secured against inadmissible modification?				
P8		Is the authenticity of the measurement data that are presented guaranteed?				
** Explanations are needed if there are deviations from software requirements.*						

2) Checklist for basic requirements for type U instrument

Checklist for Type U Requirements						
Requirement	**Testing procedures**		**Passed**	**Failed**	**Not Applicable**	**Remarks***
U1		Does the required manufacturer's documentation fulfil the requirement U1 (a-g)?				
U2		Is a software identification realised as required in U2?				
U3		Are commands entered via the user interface prevented from inadmissibly influencing the legally relevant software and measurement data?				
U4		Do commands inputted via communication interfaces of the device not inadmissibly influence the legally relevant software, device-specific parameters and measurement data?				
U5		Are legally relevant software and measurement data protected against accidental or unintentional changes?				
U6		Are legally relevant software and measurement data secured against inadmissible, intentional modification or replacement?				
U7		Are legally relevant parameters secured against inadmissible modification?				
U8		Is the authenticity of the measurement data that are presented guaranteed?				
U9		Is the legally relevant software designed in such a way that other software does not inadmissibly influence it?				
** Explanations are needed if there are deviations from software requirements.*						

3) Checklist for specific requirements extension L

Checklist for Requirements of Extension L						
Requirement	**Testing procedures**		**Passed**	**Failed**	**Not Applicable**	**Remarks***
L1		Is the stored measurement data accompanied by all relevant information needed for legally relevant purposes?				
L2		Is stored data protected against accidental and unintentional changes?				
L3		Is the stored measurement data protected against intentional changes?				
L4		Is the stored measurement data capable of being traced back to the measurement and measuring instrument that generated them?				
L5		Are keys and associated information treated as measurement data and are they kept secret and protected against compromise?				
L6		Is there legally relevant software for reading, verifying and indicating stored measurement data?				
L7		Is the measurement data stored automatically when the measurement is concluded?				
L8		Does the long-term storage have a capacity which is sufficient for the intended purpose?				
** Explanations are needed if there are deviations from software requirements.*						

4) Checklist for specific requirements extension T

Checklist for Requirements of Extension T						
Requirement	**Testing procedures**		**Passed**	**Failed**	**Not Applicable**	**Remarks***
T1		Does transmitted data contain all relevant information necessary to present or further process the measurement result in the receiving unit?				
T2		Is transmitted data protected against accidental and unintentional changes?				
T3		Is legally relevant transmitted data protected against intentional changes?				
T4		Is the transmitted measurement data capable of being traced back to the measurement and measuring instrument that generated them?				
T5		Are keys and associated information treated as measurement data and kept secret and protected against compromise?				
T6		Is there legally relevant software for reading, verifying and handling transmitted measurement data?				
T7		Is it ensured that the measurement is not inadmissibly influenced by a transmission delay?				
T8		Is it ensured that no measurement data get lost if network services become unavailable?				
** Explanations are needed if there are deviations from software requirements.*						

5) Checklist for specific requirements extension S

Checklist for Requirements of Extension S						
Requirement	**Testing procedures**		**Passed**	**Failed**	**Not Applicable**	**Remarks***
S1		Is there a part of the software that contains all legally relevant software and parameters that is clearly separated from other parts of software?				
S2		Is information generated by the legally non-relevant software shown on a display or printout in a way that confusion with the information generated by the legally relevant software is avoided?				
S3		Is the data exchange between the legally relevant and legally non-relevant software carried out exclusively via a protective software interface?				
** Explanations are needed if there are deviations from software requirements.*						

6) Checklist for specific requirements extension D

Checklist for Requirements of Extension D						
Requirement	**Testing procedures**		**Passed**	**Failed**	**Not Applicable**	**Remarks***
D1		Do both phases of the software download, the transmission, and the subsequent installation of software, run automatically and do they not affect the protection of legally relevant software?				
D2		Are means employed to guarantee that the downloaded software is authentic?				
D3		Are means employed to guarantee that the downloaded software has not been inadmissibly changed during download?				
D4		Is it guaranteed by appropriate technical means that downloads of legally relevant software are adequately traceable within the instrument for subsequent controls?				
** Explanations are needed if there are deviations from software requirements.*						

13 Cross Reference for MID-Software Requirements to MID Articles and Annexes

(Related MID Version: DIRECTIVE 2014/32/EU, 26 February 2014)

13.1 Given software requirement, reference to MID

Requirement		**MID**	
No	**Denotation**	**Article / Annex No** (AI = Annex I)	**Denotation**
	Basic Type P		
P1	Manufacturer's Documentation	AI-9.3 AI-12 Article 18	Information to be borne by and to accompany the instrument Conformity Evaluation Technical Documentation
P2	Software Identification	AI-7.6 AI-8.3	Suitability Protection against corruption
P3	Influence via User Interface	AI-7.1	Suitability
P4	Influence via communication Interface	AI-7.1 AI-8.1	Suitability Protection against corruption
P5	Protection Against Accidental or Unintentional Changes	AI-7.1, AI-7.2 AI-8.4	Suitability Protection against corruption
P6	Protection Against Intentional Changes	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Suitability[17] Protection against corruption
P7	Parameter Protection	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Suitability Protection against corruption
P8	Software authenticity and Presentation of Results	AI-7.1, AI-7.2, AI-7.6 AI-8.3 AI-10.2, AI-10.3, AI-10.4	Suitability Protection against corruption Indication of result

[17] Note: As regards contents, paragraph 7.1 of MID-Annex I is not an issue of "Suitability" but of "Protection against corruption" (Paragraph 8)

Requirement		MID	
No	**Denotation**	**Article / Annex No** (AI = Annex I)	**Denotation**
	Basic Type U		
U1	Manufacturer's Documentation	AI-9.3 AI-12 Article 18	Information to be borne by and to accompany the instrument Conformity Evaluation Technical Documentation
U2	Software Identification	AI-7.6 AI-8.3	Suitability Protection against corruption
U3	Influence via user interfaces	AI-7.1	Suitability
U4	Influence via Communication Interface	AI-7.1 AI-8.1	Suitability Protection against corruption
U5	Protection against accidental or unintentional changes	AI-7.1, AI-7.2 AI-8.4	Suitability Protection against corruption
U6	Protection against Intentional Changes	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Suitability Protection against corruption
U7	Parameter Protection	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Suitability Protection against corruption
U8	Software authenticity and Presentation of Results	AI-7.1, AI-7.2, AI-7.6 AI-8.3 AI-10.2, AI-10.3, AI-10.4	Suitability Protection against corruption Indication of result
U9	Influence of other software	AI-7.6	Suitability
	Extension L		
L1	Completeness of stored data	AI-7.1 AI-8.4 AI-10.2	Suitability Protection against corruption Indication of result
L2	Protection against accidental or unintentional changes	AI-7.1, AI-7.2 AI-8.4	Suitability Protection against corruption
L3	Integrity of data	AI-7.1 AI-8.4	Suitability Protection against corruption
L4	Authenticity of stored data	AI-7.1 AI-8.4 AI-10.2	Suitability Protection against corruption Indication of result
L5	Confidentiality of keys	AI-7.1 AI-8.4	Suitability Protection against corruption
L6	Retrieval of stored data	AI-7.2 AI-10.1, AI-10.2, AI-10.3, AI-10.4	Suitability Indication of result
L7	Automatic storing	AI-7.1 AI-8.4	Suitability Protection against corruption
L8	Storage capacity and continuity	AI-7.1	Suitability
Lx	All of Extension L	AI-11.1	Further processing of data to conclude the trading transaction
	Extension T		
T1	Completeness of transmitted data	AI-7.1 AI-8.4	Suitability Protection against corruption
T2	Protection against accidental changes	AI-7.1, AI-7.2 AI-8.4	Suitability Protection against corruption
T3	Integrity of data	AI-7.1 AI-8.4	Suitability Protection against corruption
T4	Authenticity of transmitted data	AI-7.1 AI-8.4	Suitability Protection against corruption
T5	Confidentiality of keys	AI-7.1 AI-8.4	Suitability Protection against corruption
T6	Handling of corrupted data	AI-7.1 AI-8.4	Suitability Protection against corruption
T7	Transmission delay	AI-7.1 AI-8.4	Suitability Protection against corruption

Requirement		MID	
No	**Denotation**	**Article / Annex No** (AI = Annex I)	**Denotation**
T8	Availability of transmission services	AI-7.1 AI-8.4	Suitability Protection against corruption
	Extension S		
S1	Realisation of software separation	AI-7.6, AI-10.1	Suitability Indication of result
S2	Mixed indication	AI-7.1, AI-7.2, AI-7.6 AI-10.2	Suitability Indication of result
S3	Protective software interface	AI-7.6	Suitability
	Extension D		
D1	Download mechanism	AI-8.2, AI-8.4	Protection against corruption
D2	Authentication of downloaded software	AI-7.6 AI-8.3, AI-8.4 AI-12	Suitability Protection against corruption Conformity evaluation
D3	Integrity of downloaded software	AI-7.1, AI-8.4	Suitability Protection against corruption
D4	Traceability of legally relevant Software Download	AI-7.1, AI-7.6 AI-8.2, AI-8.3 AI-12	Suitability Protection against corruption Conformity evaluation
	Extension I (Instrument-specific Software Requirements)		
I1-1, I2-1, I3-1, I4-1, I5-1	Fault Recovery	AI-6 MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	Reliability Specific Requirements for Utility Meters
I1-4, I2-3, I3-4, I4-4, I5-4	Back-up facilities	AI-6 MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	Reliability Specific Requirements for Utility Meters
I1-9, I2-9, I3-9, I4-9	Internal resolution, suitability of the indication	MI-002-5.3, MI-003-5.2	Specific Requirements for Utility Meters
I1-6, I2-6, I3-6, I4-6	Inhibit resetting of cumulative measurement values	AI-8.5	Protection against corruption
I1-2, I2-2, I3-2, I4-2, I5-2	Dynamic behaviour	AI-7.6	Suitability Protection against corruption
I2-10	Battery lifetime	MI-002-5.2	Specific Requirements for Gas Meters
I2-12	Electronic volume converters	MI-002-9.1	Specific Requirements for Gas Meters
I2-11	Test element	MI-002-5.5	Specific Requirements for Gas Meters
I6-1	Fault detection	MI-006-IV, MI-006-V	Discontinuous and continuous Totalisers
I6-2	Back-up facilities Fault detection	MI-006-IV, MI-006-V	Discontinuous and continuous Totalisers

13.2 Interpretation of MID Articles and Annexes by MID-Software Requirements

MID			Software Guide
Article / Annex No (AI = Annex I)	**Denotation**	**Comment**	**Requirement No**
	Article Part		
1, 2, 3		No specific software relevance	
4(b)	Definitions, Arrangement of sub-assemblies	Transmission of measurement data ... Basic Guides applicable to sub-assemblies	T P, U
5 to 9		No specific software relevance	
10	Technical documentation	Documentation of design, manufacture and operation. Enable assessment of conformity. General description of the instrument. Description of electronic devices with drawings, flow diagrams of the logic, general software information. Location of seals and markings. Conditions for compatibility with interfaces and sub-assemblies.	P1, U1
11 to 27		No specific software relevance	
	Annex I		
AI-1 to AI-5		No specific software relevance	
AI-6	Reliability	Fault detection, back-up, restoring, restart	I1-1, I1-2, I2-1, I2-2, I3-1, I3-2, I4-1, I4-2, I6-1, I6-2
AI-7	Suitability	No features to facilitate fraudulent use; minimal possibilities for unintentional misuse.	P3 – P8, U3 - U8, L1 – L5, L7, L8, T1 – T8, S2, D3, D4, I1-4, I2-8, I3-5, I4-4
AI-8	Protection against corruption		
AI-8.1		No influences by the connection of other devices.	P4, U4
AI-8.2		Securing; evidence of intervention	P6, P7, U6, U7, D1, D4
AI-8.3		Identification of software; evidence of intervention	P2, P6, P7, P8 U2, U6, U7, U8, D2, D4
AI-8.4		Protection of stored or transmitted data	P5 - P7, U5 - U7, L1 - L5, T1 - T8 D1 - D3
AI-8.5		No reset of cumulative registers	I1-3, I2-4, I3-4, I4-3
AI-9	Information to be borne by and to accompany the instrument		

MID			Software Guide
Article / Annex No (AI = Annex I)	**Denotation**	**Comment**	**Requirement No**
AI-9.1		Measuring capacity (rest of items non-relevant for software)	L8
AI-9.2		No specific software relevance	
AI-9.3		Instructions for installation, ..., conditions for compatibility with interface, sub-assemblies or measuring instruments.	P1, U1
AI-9.4 to AI-9.8		No specific software relevance	
AI-10	Indication of result		
AI-10.1		Indication by means of a display or hard copy.	U8, L6, S2
AI-10.2		Significance of result, no confusion with additional indications.	P8, U8, L1, L4, L6, S2
AI-10.3		Print or record easily legible and non-erasable.	P8, U8, L6, S2
AI-10.4		For direct sales: presentation of the result to both parties.	P8, U8, S2
AI-10.5		For utility meters: display for the customer.	I1-3, I2-3, I3-3/4, I4-3
AI-11	Further processing of data to conclude the trading transaction		
AI-11.1		Record of measurement results by a durable means.	L1 - L8
AI-11.2		Durable proof of the measurement result and information to identify a transaction.	L1, L6
AI-12	Conformity evaluation	Ready evaluation of the conformity with the requirements of the Directive.	P1, P2, U1, U2, D2, D4
	Annexes A1 to H1		
A1 to H1		No requirements to features of instruments	
	Annex MI-001		
MI-001-1 to MI-001-6		No specific software relevance	
MI-001-7.1.1, MI-001-7.1.2	Electromagnetic immunity	Fault detection Back-up facilities Wake-up facilities and restoring	I1-1, I1-2
MI-001-7.1.3 to MI-001-9		No specific software relevance	
	Annex MI-002		
MI-002-1 to MI-002-2		No specific software relevance	
MI-002-3.1	Electromagnetic immunity	Fault detection Back-up facilities Wake-up facilities and restoring	I2-1, I2-2
MI-002-3.1.3 to MI-002-5.1		No specific software relevance	
MI-002-5.2	Suitability	Acceptable solution for monitoring battery lifetime	I2-5
MI-002-5.3	Suitability	Internal resolution	I2-3

MID			Software Guide
Article / Annex No (AI = Annex I)	**Denotation**	**Comment**	**Requirement No**
MI-002-5.4 to MI-002-8		No specific software relevance	
MI-002-5.5	Suitability	Test element	I2-7
MI-002-5.6 to MI-002-8		No specific software relevance	
MI-002-9.1	Volume conversion devices Suitability	Acceptable solution for monitoring the gas volume converter	I2-6
MI-002-9.2 to MI-002-10		No specific software relevance	
	Annex MI-003		
MI-003-1 to MI-003-4.2		No specific software relevance	
MI-003-4.3	Permissible effect of transient electromagnetic phenomena	Fault detection Back-up facilities Wake-up facilities and restoring	I3-1, I3-2
MI-003-5.1		No specific software relevance	
MI-003-5.2	Suitability	Internal resolution	I3-3
MI-003-5.3 to MI-003-7		No specific software relevance	
	Annex MI-004		
MI-004-1 to MI-004-4.1		No specific software relevance	
MI-004-4.2	Permissible influences of electromagnetic disturbances	Fault detection Back-up facilities Wake-up facilities and restoring	I4-1, I4-2
MI-004-4.3 to MI-004-7		No specific software relevance	
	Annex MI-005		
	Annex MI-006		
MI-006-IV, MI-006-V	Discontinuous and continuous Totalisers	Fault detection Back-up facilities	I6-1, I6-2
	Annex MI-007		
MI-007-8	Permissible influences of electromagnetic disturbances	Back-up facilities	I7-1
	Annex MI-008		
	Annex MI-009		
	Annex MI-010		

14 References and Literature

[1] Software Requirements and Validation Guide, Version 1.00, 29 October 2004, European Growth Network "*MID-Software",* contract number G7RT-CT-2001-05064, 2004

[2] 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), Official Journal of the European Union L 96/149, 29.3.2014

[3] Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments. Official Journal of the European Union L 135/1, 30.4.2004

[4] Internet Security Glossary, http://www.ietf.org/rfc/rfc2828.txt

[5] ISO/IEC JTC1/SC7 3941, 2008-03-14, http://pef.czu.cz/~papik/doc/MHJS/pdf/IT-VOCABULARY.pdf

15 Revision History

No.	Date	Significant Changes
1	May 2005	Guide first issued.
2	April 2007	Addition and enhancement of terms in Section 2 Editorial changes in Sections 4.1 and 5.1 Amendment of a clarification for software identification in Section 4.2, Requirement P2 and Section 5.2, Requirement U2. Amendment in Requirement L8, Specifying Note 1. Addition of an explanation to Requirement S1, Specifying Note 1. Replacement of Requirement D5 by a remark. Change of the Risk Class for Measuring Systems for Liquids other than Water. Change of Risk Classes for Weighing Instruments. Various minor editorial changes in the document. Addition of this revision table.
3	March 2008	Addition of exceptions for the indication of the software identification: new requirements I1-5, I2-9, I3-6, I4-5, and I5-1.
4	May 2009	Restriction of the application area of software download, clarification of identification requirements in connection with software download Revision of requirements P2 and U2: Deletion of void text fragments.

5	May 2011	Revision of chapter 5 (part U): Advancement with respect to operating systems Replacement of the term “component” by other appropriate terms through the guide to avoid misunderstandings Addition of requirement D1 in section 9.2 by introduction of a sealable setting for the download mechanism Refinement of the specifying notes of requirements P2 and U2 in section 4.2 and 5.2, respectively, with regard to software identification Extension of examples of acceptable solutions in requirement L2 (section 6.2) and in requirement U8 (section 5.2)
6	March 2015	Major revision: - Character of the guide: The guide is considered a purely technical document that interprets software-related essential requirements. Statements that do not correspond to this principle have been removed. - Addressees of the guide: The guide addresses software developers and examiners, but may be used as well by other parties, in particular Market Surveillance Authorities, wherever and whenever it is appropriate. - It has turned out that the implementation of the two latter updates requires much editorial work in detail. These changes will lead to a better readability of the guide, but not change technical specifications. - Software identification (P2/U2): It shall not be anymore required in the guide 7.2 that the software identifier has to be provided by the software itself. It is sufficient to require that the software identifier has to be provided by the instrument in a secured way. - Differentiation between identification and integrity (P2/U2, P6/U6): MID annex 1 distinguishes between identification of software (annex 1, cl. 7.6) and integrity, e.g. protection of software (annex 1, cl. 8.4). The differentiation does not lead to weaker requirements. - Support of conformity-to-type checks: The technical means required for integrity of software are considered suitable also to be used for the check of conformity to type. The means required are e.g. checksums or equivalent means at different levels for all instruments in risk class C and higher. - Risk classes: Risk class C has been changed so that now the whole legally relevant software is considered fixed for instruments in risk class C. In this way, ambiguities which part of software is considered fixed have been removed. In risk class C and higher identity of software on the bit level (e.g. by checksums) must be implemented. - Risk classification of instruments with universal devices (U type instruments): Due to a basically higher risk associated with U type instruments, their classification into

		risk class B is considered inappropriate. U type instruments can only be classified into risk class C upwards. - Acceptable security measures for high Risk Classes (D and higher): Concerning algorithms and minimum key lengths, the requirements or recommendations of the national and international institutions responsible for data security have to be taken into consideration (e.g. NIST (USA), DCSSI (France), CESG (United Kingdom), CCN (Spain), NCSC (Netherlands), BSI (Germany)). - Legally relevant software: It is not seen anymore the necessity to differentiate between legally relevant software and fixed legally relevant software. All protection requirements in annex I are valid for legally relevant software.
7	March 2018	Expansion of P7 by an acceptable solution that ensures, that the contents of the event logger are shown on the display is added. Expansion of U8 and inclusion of a corresponding P8 to describe pairing and handshaking between units in a more general way. Improved clarity of extension S by removing the definition for low level / high level separation.
8	April 2019	Editorial changes concerning translation comparison and housekeeping, clarification of the application of extension T, corrections in P6, U6, T2, T6 and L2 Reorganization between “Acceptable Solutions” and “Specifying Notes” on each requirement. The two instrument-specific annexes 10.2 Gas Meters and Volume Conversion Devices and 10.3 Active Electrical Energy Meters have been completely revised. Chapter 11.1 “Information to be included in the type examination certificate” was adapted.
9	October 2020	Revision of the annexes 10.1 Water meter, 10.4 Thermal energy meters, 10.5 Measuring systems for the continuous and dynamic measurement of quantities of liquids other than water and 10.7 Taximeters.
10	July 2021	Implementation of the changes of the terminology subgroup presented in the WG 7 meeting in 2021. Reworded validation guidance for risk classes E (“appropriate” -> “correct”), as presented in the WG 7 meeting in 2019.
11	March 2022	Addition of “Extension O”, detailing new requirements for measuring instruments with operating systems. Subsequently, the whole Guide has been updated to incorporate the new extension. Multiple requirements in the whole document have been clarified to increase the readability and make them less ambiguous. The technical specifications remain the same. The template of the test report has been updated.

Table 15-1: Revision history