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

# WELMEC Guide 7.4

## Examples of Software Examination

## Version 2026

For information:

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

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

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

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

Published by:
WELMEC Secretariat

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

# Examples of Software Examination

## Contents

## Foreword

This Guide offers worked examples to demonstrate the application of the Guides 7.2, 7.3 and 7.6 to examine measuring instruments.

# 1 Terminology

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

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

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

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

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

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

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

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

## 1.1 Abbreviations

| | |
|---|---|
| DoC | device of the consumer |
| HW | hardware |
| IIA1 | inadmissible influence via the administration of the operating system |
| IIA2 | inadmissible influence due to accidental modification |
| IIB1 | inadmissible influence via the boot process |
| IIC1 | inadmissible influence by obtaining confidential information |
| IID1 | inadmissible influence by downloading legally relevant software |
| III1 | inadmissible influence via user interfaces |
| III2 | inadmissible influence via hardware interfaces |
| IIN1 | inadmissible influence through legally non-relevant software |
| IIP1 | inadmissible influence on the measurement process by executing other functions |
| IIR1 | inadmissible influence by replacing physical parts within the measuring instrument |
| IIR2 | inadmissible influence by replacing or removing complete components |
| IIS1 | inadmissible influence through incorrect identification of software |
| IIT1 | inadmissible influence through man-in-the-middle attacks |
| LNR | legally non-relevant |
| LR | legally relevant |
| MCU | microcontroller unit |
| OS | operating system |
| SW | software |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |

# 2 How to use WELMEC Software Guides

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

**Guide 7.2** implements the core requirements based on the essential requirements of the MID [1] and NAWID [2] detailing that all assets need to be adequately protected. It is the starting point for any software examination.

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

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

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

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

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

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

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

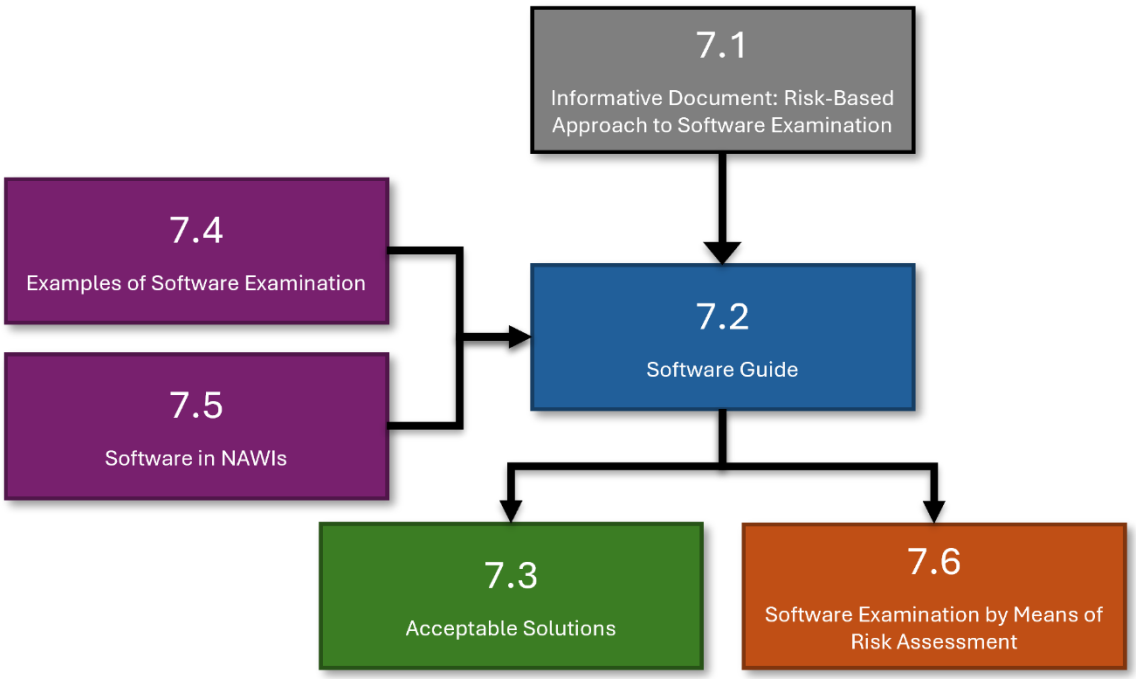


Figure 1: Relationship between the WELMEC Software Guides

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

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

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

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

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

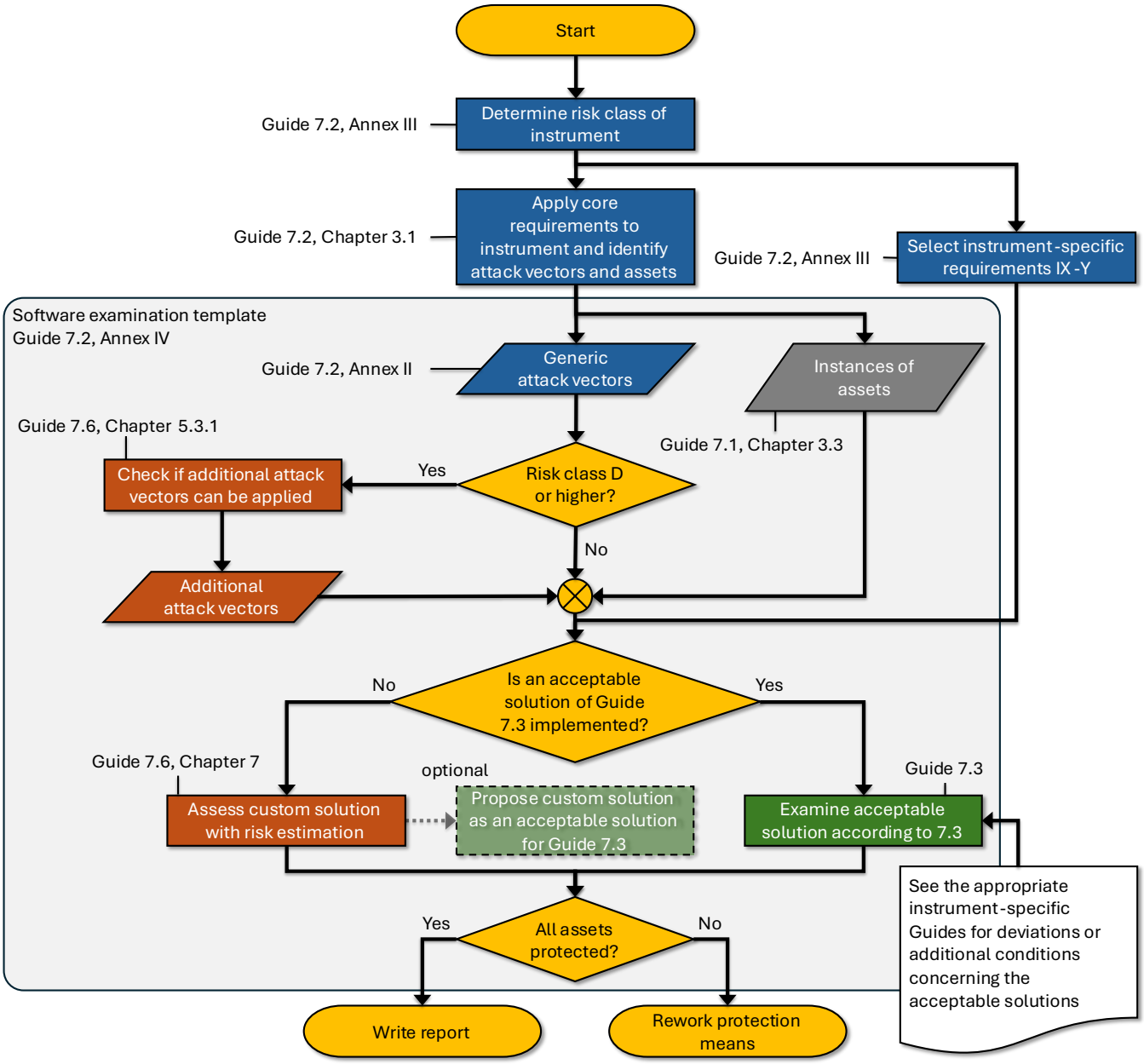


Figure 2: Workflow of the examination of the requirements using Guides 7.1, 7.2, 7.3, 7.6, and instrument-specific Guides (see the WELMEC website).

# 3 Introduction

This Guide provides mock software examinations of several measuring instruments. Each measuring instrument is based on a specific design functionality to demonstrate examinations of, for example, instruments with operating systems, external devices, and multiple components. Each mock software examination demonstrates how to examine the instrument in accordance with Guide 7.2 by describing the protection means employed

- against each attack vector,
- for each asset.

Each protection means is either

- an existing acceptable solution given in Guide 7.3,
- a custom solution that is risk-assessed for adequacy using Guide 7.6.

A template for a complete examination table that contains all assets and attack vectors, is provided in Annex IV of Guide 7.2.

The example measuring instruments in this Guide are of risk class B or C, therefore no additional attack vectors are considered.

This Guide uses a color scheme for measuring instruments, see below. An exemplary diagram is shown in *Figure 3*.

| | |
|---|---|
| | Asset |
| | Component (or complete measuring instrument, or devices) |
| | Hardware design (e.g., hardware interfaces) |
| | Software design (e.g., user interface) |
| | Legally non-relevant design (hardware or software) |

Table 1: Color scheme of the concepts and terms used to describe properties of a measuring instrument.

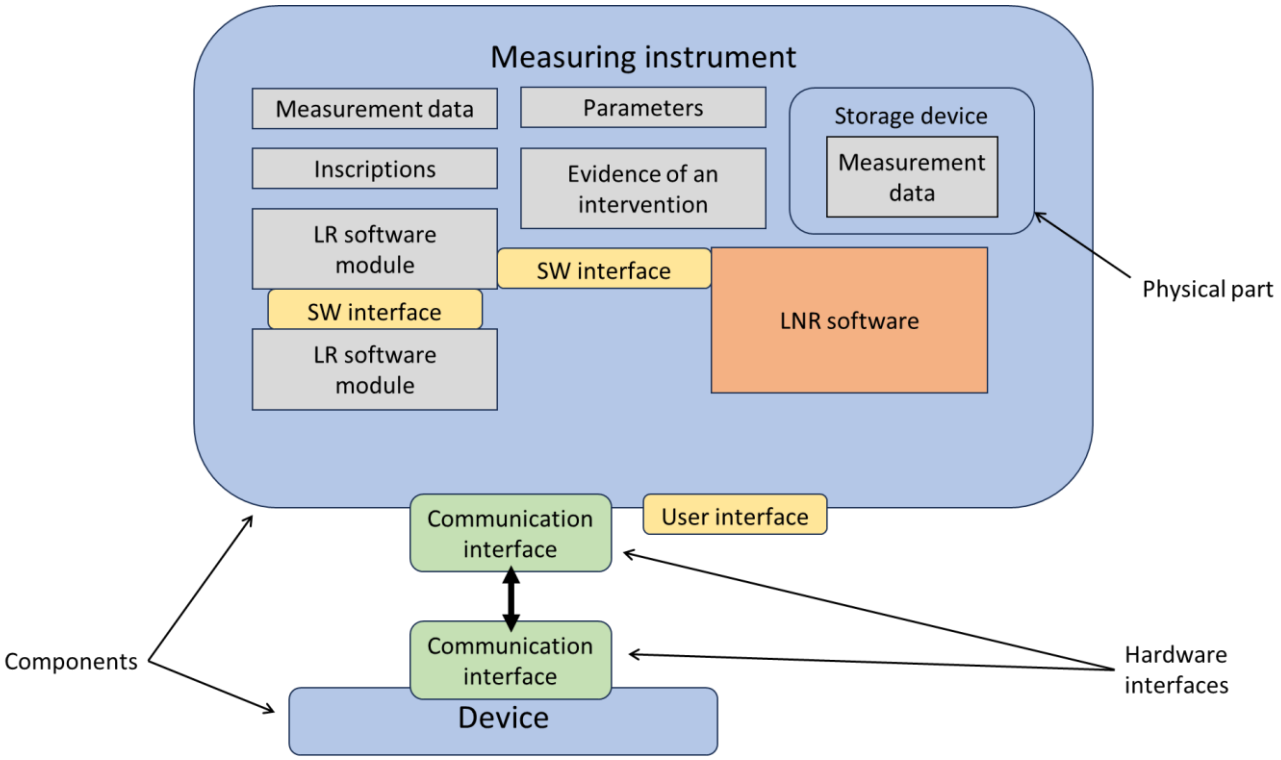


Figure 3: Representation of the different concepts and terms used to describe properties of a measuring instrument.

# 4 Examples

The following examples are meant for illustration of various applications of WELMEC Software Guides. They are non-binding and do not impose any requirements or restrictions.
The complete, filled-in software examination templates (see Annex IV of Guide 7.2) for each example are accessible to all WG7 members.

*Note*: This Guide uses both acceptable solutions taken from Guide 7.3 and custom solutions based on a risk analysis in accordance with Guide 7.6, to illustrate the examination. The manufacturer is free to implement any solution of his choice, be it an acceptable or a custom solution. The Guides do not restrict in any way the approach the manufacturer wants to use, provided it meets the requirements.

## 4.1 Basic measuring instrument

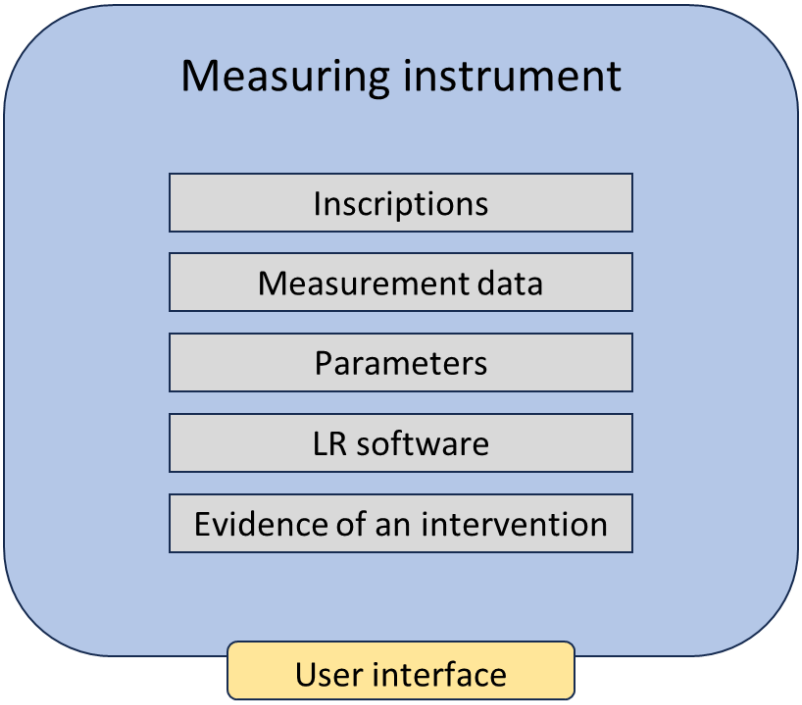


Figure 4: Basic measuring instrument.

### 4.1.1 Overview

The measuring instrument contains a main component that contains all assets necessary for providing measurement functionality, e.g., A/D conversion of sensor data, data processing, user interfaces, calculation and indication of the measurement result. The measuring instrument consists of a single component in one housing and it contains all assets. The assets consist of

- software,
- parameters,
- inscriptions,
- evidence of an intervention, and
- measurement data.

The measuring instrument has a user interface that can be used to set parameters and to initiate a measurement. The measurement result is only indicated and not stored.

### 4.1.2 Assessment of inadmissible influence

In *Figure 5*, the assets of the measuring instrument are examined for the applicable inadmissible influences. The examination was performed with the software examination template, see Annex IV of Guide 7.2. For the basic measuring instrument, only the generic attack vectors are considered.

In *Table 2*, a more detailed examination of an inadmissible influence (III1 – user interfaces) is provided. In this table, four different acceptable solutions, offered by Guide 7.3, are compared and examined.

**Assets-Threats-Matrix derived from WELMEC Guide 7.2: 2026**

**Threats consist of at least one asset and one corresponding statement of which security property (availability, integrity and/or authenticity) can be invalidated by the threat by means of an attack vector.**

| NA: Not applicable | RA: Risk analysis |
|---|---|
| AS: Acceptable solution | BO: RA and AS |

| Asset No. | Assets/Properties | Attack Vector No. | Inadmissible influence on the measurement process by executing other functions IIP1 | Inadmissible influence via user interfaces III1 | Inadmissible influence via the boot process IIB1 | Inadmissible influence via the administration of the operating system IIA1 | Inadmissible influence via legally non-relevant software IIN1 | Inadmissible influence by obtaining confidential information IIC1 | Inadmissible influence by replacing physical parts within the measuring instrument IIR1 | Inadmissible influence via hardware interfaces III2 | Inadmissible influence by downloading legally relevant software IID1 | Inadmissible influence by replacing or removing legally relevant components IIR2 | Inadmissible influence by man-in-the-middle attacks IIT1 | Inadmissible influence due to accidental modification IIA2 | Inadmissible influence by incorrect software identification IIS1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | +1 | -1 |
| 1 | software in main component | | 4.3.1.1 | 4.4.1.1/5.1 | NA | NA | NA | NA | 4.8.1.1 | NA | NA | NA | NA | NA | 4.6.1 |
| 2 | parameters in main component | | 4.3.1.1 | 4.4.1.1/5.1 | NA | NA | NA | NA | 4.8.1.1 | NA | NA | NA | NA | 4.4.2.1 | 4.6.1 |
| 3 | measurement data in main component | | 4.3.1.1 | 4.4.1.1/5.1 | NA | NA | NA | NA | 4.8.1.1 | NA | NA | NA | NA | 4.4.2.1 | 4.6.1 |
| 4 | measurement result in main component | | 4.3.1.1 | 4.4.1.1/5.1 | NA | NA | NA | NA | 4.8.1.1 | NA | NA | NA | NA | 4.4.2.1 | 4.6.1 |
| 5 | inscriptions for main component | | 4.3.1.1 | 4.4.1.1/5.1 | NA | NA | NA | NA | 4.8.1.1 | NA | NA | NA | NA | NA | 4.6.1 |
| 6 | evidence of an intervention in main component | | 4.3.1.1 | 4.4.1.1/5.1 | NA | NA | NA | NA | 4.8.1.1 | NA | NA | NA | NA | 4.4.2.1 | 4.6.1 |

Figure 5: Examination of combinations of assets and attack vectors for the basic measuring instrument based on the software examination template.

| **Chapter in Guide 7.3** | **4.4.2.1 (password)** | **4.4.2.3 (restricted permissions)** | **4.4.1.1 (command interpreter)** | **5.1 (audit trail)** |
|---|---|---|---|---|
| **Covered** | Asets: measurement data, parameters<br>Properties: all<br>Attack vectors: IIA2 | Assets: All<br>Properties: all<br>Attack vectors: III1, IIA2 | Assets: All<br>Properties: all<br>Attack vectors: III1, III2, IIN1, IIA2, IIC1 | Assets: All<br>Properties: all<br>Attack vectors: all |
| **Conditions** | - | An operating system is present. | - | - |
| **Summary** | A password only covers IIA2, because it prevents accidental changes. The user interface still needs to be protected against intentional misuse. | Not possible because there is no OS. | Depending on the implementation, the command interpreter can cover multiple inadmissible influences. | An audit trail is possible but a solution that prevents changes (instead of “only” offering evidence of an intervention) is preferrable for a user interface. |

Table 2: Detailed examination of the inadmissible influences via user interfaces (III1) on the assets.

Considering inadmissible influences via the user interface, the following acceptable solutions are implemented:

- All assets except parameters are protected with a command interpreter.
- The parameters can be set by the user (accepted by the command interpreter). To provide evidence of an intervention, an audit trail is implemented that records any changes to the parameters, i.e., implements protection.

Both solutions are therefore necessary to prevent inadmissible influence via the user interface and are inserted in the corresponding column (III1) in *Figure 5*.

The manufacturer needs to repeat this procedure for every combination of asset and attack vector to ensure that the measuring instrument is adequately protected. By completing the software examination template, the manufacturer can visualize and proof that the measuring instrument has been adequately protected against all inadmissible influences. The manufacturer has to supply the technical documentation to the examiner and it is recommended that the completed software examination template is part

of that technical documentation. The examiner needs to check that the technical documentation is correct and complete, and establish what needs to be examined.

## 4.2 Separated storage

### 4.2.1 Overview

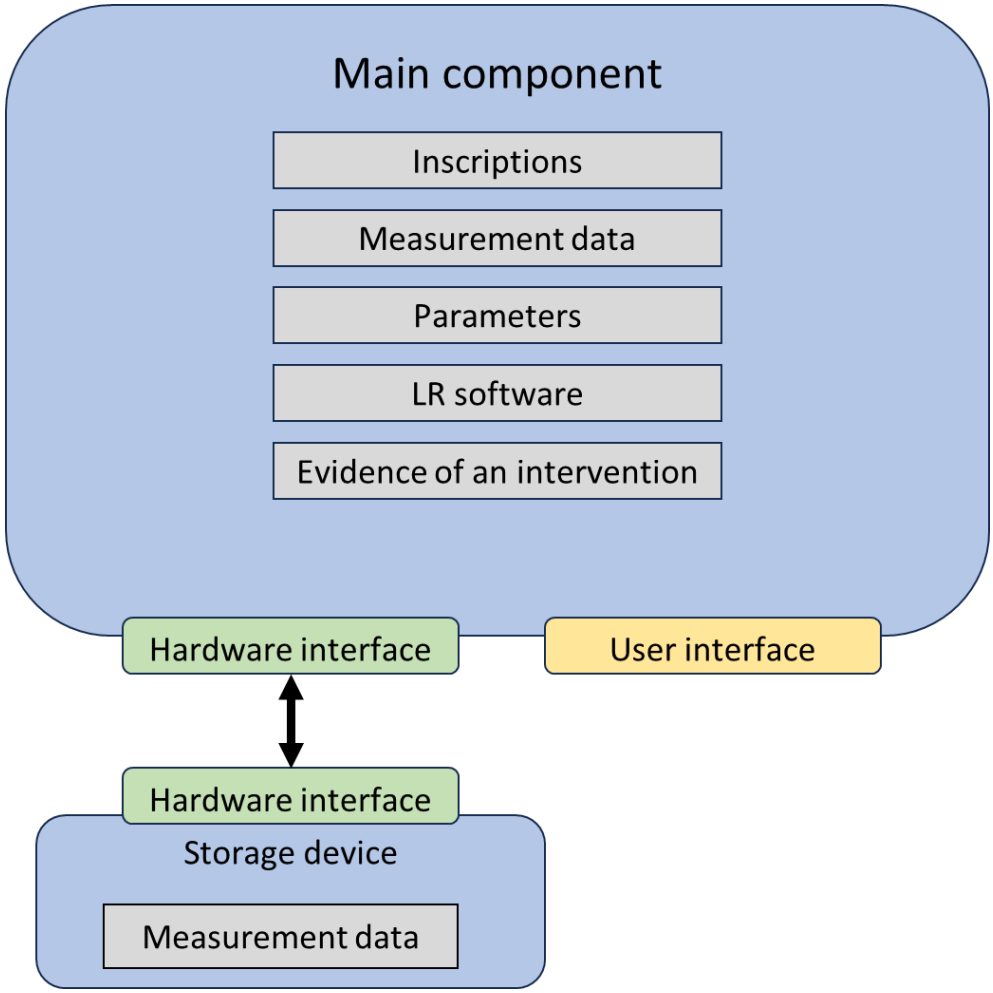


Figure 6: Measuring instrument with separate storage.

The measuring instrument contains a main component that contains all assets necessary for providing measurement functionality, similar to the basic measuring instrument in subchapter *4.1*. Additionally, measurement data are stored in a separate component. Both components communicate via hardware communication interfaces. Upon request by the main component, measurement results are transmitted back to the main component and indicated there.

### 4.2.2 Assessment of inadmissible influence

The procedure is the same as for the basic measuring instrument in subchapter *4.1*. However, the inadmissible influences III2 (hardware interfaces), IIR2 (replacing or removing complete components), and IIT1 (man-in-the-middle attacks) are now present and must be accounted for.

**Assets-Threats-Matrix derived from WELMEC Guide 7.2: 2026**

**Threats consist of at least one asset and one corresponding statement of which security property (availability, integrity and/or authenticity) can be invalidated by the threat by means of an attack vector.**

| NA: Not applicable | RA: Risk analysis |
|---|---|
| AS: Acceptable solution | BO: RA and AS |

| | Attack Vector | Inadmissible influence on the measurement process by executing other functions | Inadmissible influence via user interfaces | Inadmissible influence via the boot process | Inadmissible influence via the administration of the operating system | Inadmissible influence via legally non-relevant software | Inadmissible influence by obtaining confidential information | Inadmissible influence by replacing physical parts within the measuring instrument | Inadmissible influence via hardware interfaces | Inadmissible influence by downloading legally relevant software | Inadmissible influence by replacing or removing legally relevant components | Inadmissible influence by man-in-the-middle attacks | Inadmissible influence due to accidental modification | Inadmissible influence by incorrect software identification |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | No. | IIP1 | III1 | IIB1 | IIA1 | IIN1 | IIC1 | IIR1 | III2 | IID1 | IIR2 | IIT1 | IIA2 | IIS1 |
| Asset No. | Assets/Properties | | | | | | | | | | | | +1 | -1 |
| 1 | software in main component | 4.3.1.1 | 5.1 | NA | NA | NA | NA | 4.8.1.1 | 4.4.1.1 | NA | 4.1.1 | NA | NA | 4.6.1 |
| 2 | parameters in main component | 4.3.1.1 | 5.1 | NA | NA | NA | NA | 4.8.1.1 | 4.4.1.1 | NA | 4.1.1 | NA | 4.4.2.1 | 4.6.1 |
| 3 | measurement data in main component | 4.3.1.1 | 5.1 | NA | NA | NA | NA | 4.8.1.1 | 4.4.1.1 | NA | 4.1.1 | NA | 4.4.2.1 | 4.6.1 |
| 4 | measurement result in main component | 4.3.1.1 | 5.1 | NA | NA | NA | NA | 4.8.1.1 | 4.4.1.1 | NA | 4.1.1 | NA | 4.4.2.1 | 4.6.1 |
| 5 | inscriptions for main component | 4.3.1.1 | 5.1 | NA | NA | NA | NA | 4.8.1.1 | 4.4.1.1 | NA | 4.1.1 | NA | NA | 4.6.1 |
| 6 | evidence of an intervention in main component | 4.3.1.1 | 5.1 | NA | NA | NA | NA | 4.8.1.1 | 4.4.1.1 | NA | 4.1.1 | NA | 4.4.2.1 | 4.6.1 |
| 7 | meas. data transmitted main comp. -> storage | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | 4.1.1 | NA | NA |
| 8 | meas. data transmitted storage -> main comp. | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | 4.1.1 | NA | NA |
| 9 | measurement data in storage | 4.3.1.1 | NA | NA | NA | NA | NA | 4.8.1.1 | 4.4.1.1 | NA | 4.1.1 | NA | 4.4.2.1 | 4.6.1 |

Figure 7: Examination of combinations of assets and attack vectors for the measuring instrument with separate storage, based on the software examination template

## 4.3 External Display

### 4.3.1 Overview

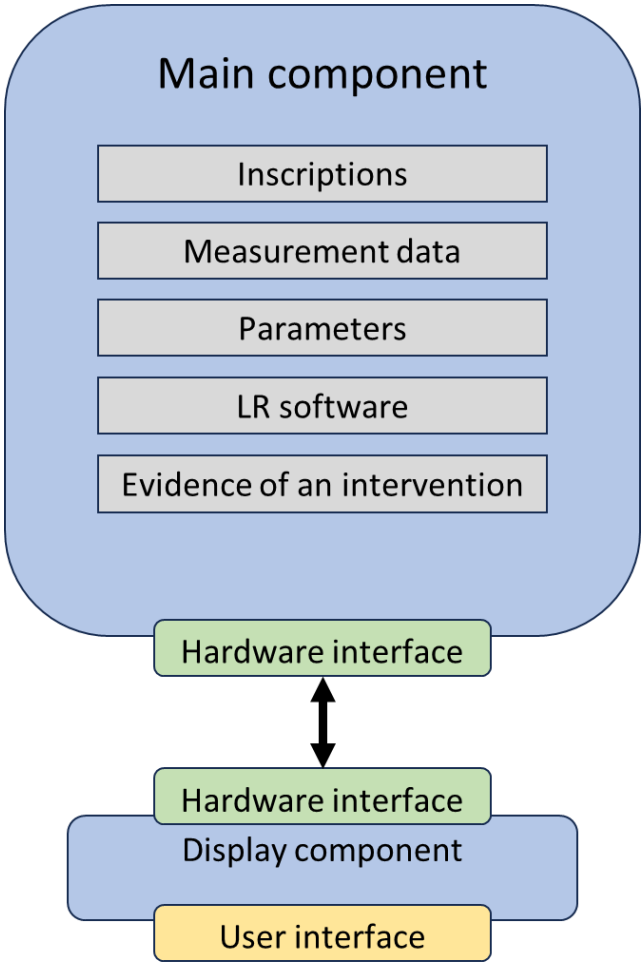


Figure 8: Measuring instrument with external display.

The measuring instrument contains a main component that realizes collection of sensor data, data processing and calculation of the measurement result. Indication of the result and the user interface are realized on a separate component. Assets on both components are protected by acceptable solutions from Guide 7.3. If the display component is disconnected, measurement results are stored on the main component until a connection to the display component has been reestablished. The user interface provides all functionality necessary to retrieve and indicate individual measurement results. The manufacturer has implemented a face recognition functionality for the user interface that has been assessed with a risk assessment in accordance with Guide 7.6.

*Note:* Relevant documents may specify if additional indications of the measurement result are also legally relevant or if only the primary indication is subject to legal control.

### 4.3.2 Assessment of inadmissible influence

The examination for this measuring instrument is similar to the measuring instrument in subchapter 4.2. Considering III1 (user interface), a risk assessment has been performed and must be examined.

**Assets-Threats-Matrix derived from WELMEC Guide 7.2: 2026**

**Threats consist of at least one asset and one corresponding statement of which security property (availability, integrity and/or authenticity) can be invalidated by the threat by means of an attack vector.**

| NA: Not applicable | RA: Risk analysis |
|---|---|
| AS: Acceptable solution | BO: RA and AS |

| Asset No. | Assets/Properties | Attack Vector No. | Inadmissible influence on the measurement process by executing other functions IIP1 | Inadmissible influence via user interfaces III1 | Inadmissible influence via the boot process IIB1 | Inadmissible influence via the administration of the operating system IIA1 | Inadmissible influence via legally non-relevant software IIN1 | Inadmissible influence by obtaining confidential information IIC1 | Inadmissible influence by replacing physical parts within the measuring instrument IIR1 | Inadmissible influence via hardware interfaces III2 | Inadmissible influence by downloading legally relevant software IID1 | Inadmissible influence by replacing or removing legally relevant components IIR2 | Inadmissible influence by man-in-the-middle attacks IIT1 | Inadmissible influence due to accidental modification IIA2 +1 | Inadmissible influence by incorrect software identification IIS1 -1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | software in main component | | 4.3.1.1 | NA | NA | NA | NA | NA | 4.8.1.1 | 4.4.1.1 | NA | 4.1.1 | NA | NA | 4.6.1 |
| 2 | parameters in main component | | 4.3.1.1 | NA | NA | NA | NA | NA | 4.8.1.1 | 4.4.1.1 | NA | 4.1.1 | NA | 4.4.2.1 | 4.6.1 |
| 3 | measurement data in main component | | 4.3.1.1 | NA | NA | NA | NA | NA | 4.8.1.1 | 4.4.1.1 | NA | 4.1.1 | NA | 4.4.2.1 | 4.6.1 |
| 4 | measurement result in main component | | 4.3.1.1 | NA | NA | NA | NA | NA | 4.8.1.1 | 4.4.1.1 | NA | 4.1.1 | NA | 4.4.2.1 | 4.6.1 |
| 5 | inscriptions for main component | | 4.3.1.1 | NA | NA | NA | NA | NA | 4.8.1.1 | 4.4.1.1 | NA | 4.1.1 | NA | NA | 4.6.1 |
| 6 | evidence of an intervention in main component | | 4.3.1.1 | NA | NA | NA | NA | NA | 4.8.1.1 | 4.4.1.1 | NA | 4.1.1 | NA | 4.4.2.1 | 4.6.1 |
| 7 | meas. result transmitted main comp. -> disp. | | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | 4.1.1 | NA | NA |
| 8 | software in display component | | 4.3.1.1 | RA | NA | NA | NA | NA | 4.8.1.1 | 4.4.1.1 | NA | 4.1.1 | NA | NA | 4.6.1 |
| 9 | measurement result in display component | | 4.3.1.1 | RA | NA | NA | NA | NA | 4.8.1.1 | 4.4.1.1 | NA | 4.1.1 | NA | NA | 4.6.1 |
| 10 | evidence of an intervention in display component | | 4.3.1.1 | RA | NA | NA | NA | NA | 4.8.1.1 | 4.4.1.1 | NA | 4.1.1 | NA | NA | 4.6.1 |

Figure 9: Examination of combinations of assets and attack vectors for the measuring instrument with external display, based on the software examination template.

## 4.4 Operating system

### 4.4.1 Overview

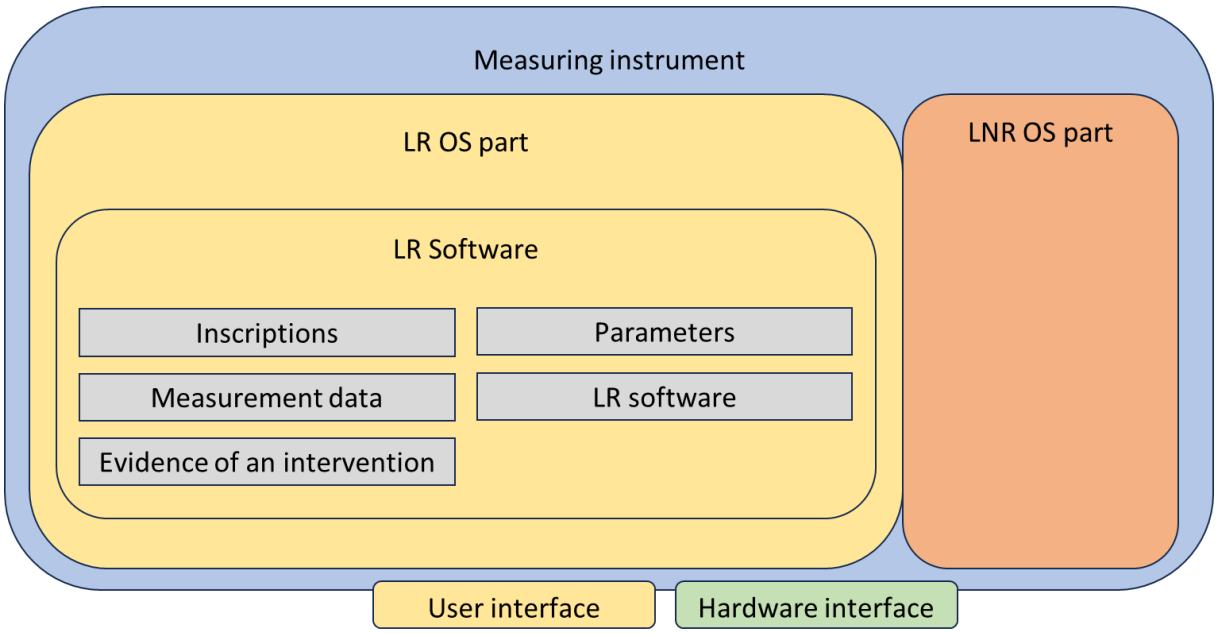


Figure 10: Measuring instrument with an operating system.

The measuring instrument contains a sensor with a digital output connected to a small embedded PC inside a sealed housing. An operating system runs on the embedded PC, on which runs an application for the visualization of the measurement result and error logging. Inadmissible influence during booting and operation of the operating system is prevented by the configuration of the operating system in accordance with acceptable solutions from Guide 7.3.

### 4.4.2 Assessment of inadmissible influence

The main focus of this example are influences via the operating system, such as booting and administration. The potential effects of both are addressed by means of acceptable solutions.

**Assets-Threats-Matrix derived from WELMEC Guide 7.2: 2026**

**Threats consist of at least one asset and one corresponding statement of which security property (availability, integrity and/or authenticity) can be invalidated by the threat by means of an attack vector.**

| NA: Not applicable | RA: Risk analysis |
|---|---|
| AS: Acceptable solution | BO: RA and AS |

| Asset No. | Assets/Properties | Attack Vector No. | Inadmissible influence on the measurement process by executing other functions | Inadmissible influence via user interfaces | Inadmissible influence via the boot process | Inadmissible influence via the administration of the operating system | Inadmissible influence via legally non-relevant software | Inadmissible influence by obtaining confidential information | Inadmissible influence by replacing physical parts within the measuring instrument | Inadmissible influence via hardware interfaces | Inadmissible influence by downloading legally relevant software | Inadmissible influence by replacing or removing legally relevant components | Inadmissible influence by man-in-the-middle attacks | Inadmissible influence due to accidental modification | Inadmissible influence by incorrect software identification |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | IIP1 | III1 | IIB1 | IIA1 | IIN1 | IIC1 | IIR1 | III2 | IID1 | IIR2 | IIT1 | IIA2 | IIS1 |
| | | | | | | | | | | | | | | +1 | -1 |
| 1 | software in main component | | 4.3.1.1 | 5.1 | 4.2.1.1 | 4.2.2.1 | 4.3.2.1 | NA | 4.8.1.1 | 4.4.3.1 | NA | NA | NA | NA | 4.6.1 |
| 2 | parameters in main component | | 4.3.1.1 | 5.1 | 4.2.1.1 | 4.2.2.1 | 4.3.2.1 | NA | 4.8.1.1 | 4.4.3.1 | NA | NA | NA | 4.4.2.1 | 4.6.1 |
| 3 | measurement data in main component | | 4.3.1.1 | 5.1 | 4.2.1.1 | 4.2.2.1 | 4.3.2.1 | NA | 4.8.1.1 | 4.4.3.1 | NA | NA | NA | 4.4.2.1 | 4.6.1 |
| 4 | measurement result in main component | | 4.3.1.1 | 5.1 | 4.2.1.1 | 4.2.2.1 | 4.3.2.1 | NA | 4.8.1.1 | 4.4.3.1 | NA | NA | NA | 4.4.2.1 | 4.6.1 |
| 5 | inscriptions for main component | | 4.3.1.1 | 5.1 | 4.2.1.1 | 4.2.2.1 | 4.3.2.1 | NA | 4.8.1.1 | 4.4.3.1 | NA | NA | NA | NA | 4.6.1 |
| 6 | evidence of an intervention in main component | | 4.3.1.1 | 5.1 | 4.2.1.1 | 4.2.2.1 | 4.3.2.1 | NA | 4.8.1.1 | 4.4.3.1 | NA | NA | NA | 4.4.2.1 | 4.6.1 |

Figure 11: Examination of combinations of assets and attack vectors for the measuring instrument with an operating system, based on the software examination template.

## 4.5 Software download

### 4.5.1 Overview

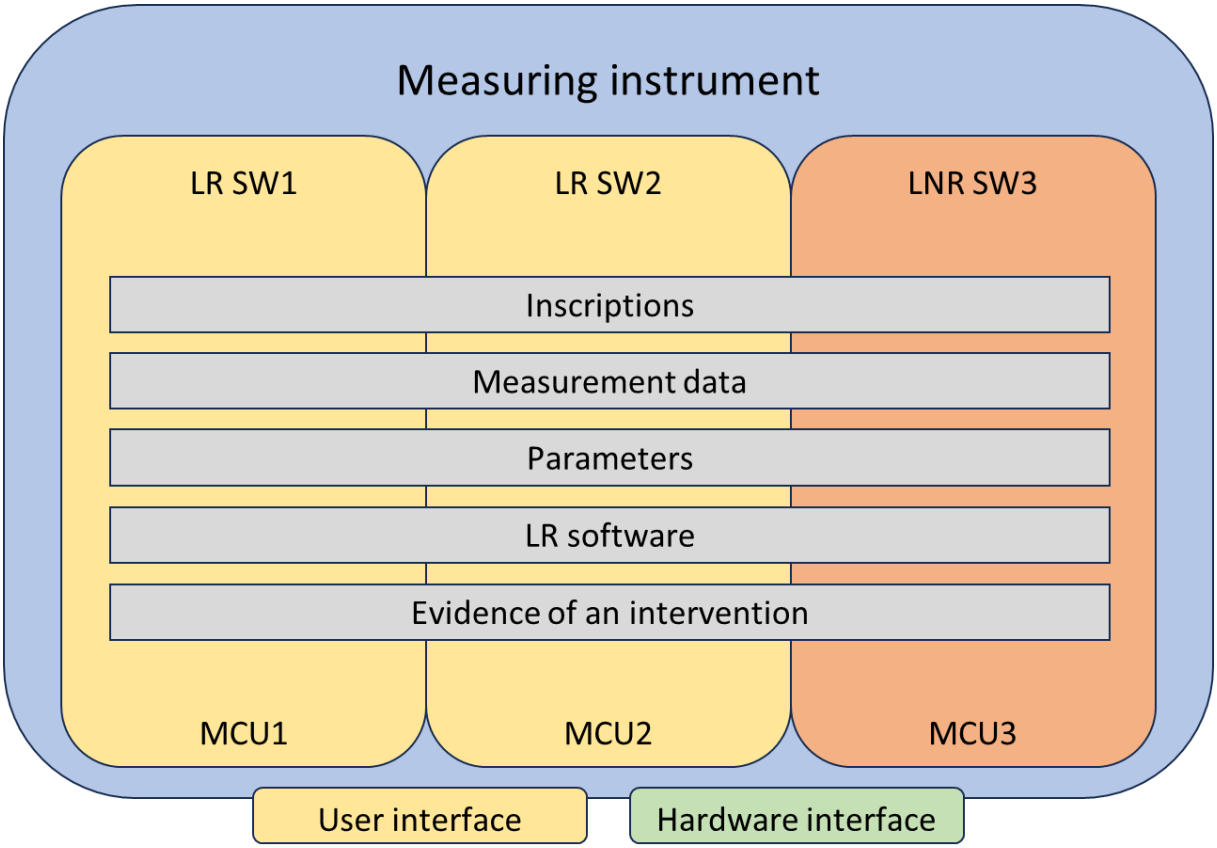


Figure 12: Measuring instrument with download functionality.

The measuring instrument contains 3 different microprocessor units for processing (MCU1, MCU2, and MCU3). MCU1 contains legally relevant SW (further “SW1”) that is responsible for the whole download process and is fixed (not possible to be changed or updated without breaking a seal). MCU2 contains legally relevant SW (further “SW2”) that provides all legally relevant functionalities, and MCU3 contains legally non-relevant SW (further “SW3”). SW1 and SW2 are individually identified, and their identification can be indicated on a display upon command.

### 4.5.2 Assessment of inadmissible influence

This example focuses on the download process and the transmission of software that is downloaded. As such, IID1 and IIT1 must be considered. The example implements the traced update procedure and uses TLS to protect the software during transmission.

**Assets-Threats-Matrix derived from WELMEC Guide 7.2: 2026**

**Threats consist of at least one asset and one corresponding statement of which security property (availability, integrity and/or authenticity) can be invalidated by the threat by means of an attack vector.**

| NA: Not applicable | RA: Risk analysis |
|---|---|
| AS: Acceptable solution | BO: RA and AS |

| Asset No. | Assets/Properties | Attack Vector No. | Inadmissible influence on the measurement process by executing other functions | Inadmissible influence via user interfaces | Inadmissible influence through the boot process | Inadmissible influence via the administration of the operating system | Inadmissible influence via legally non-relevant software | Inadmissible influence by obtaining confidential information | Inadmissible influence by replacing physical parts within the measuring instrument | Inadmissible influence via hardware interfaces | Inadmissible influence by downloading legally relevant software | Inadmissible influence by replacing or removing legally relevant components | Inadmissible influence by man-in-the-middle attacks | Inadmissible influence due to accidental modification | Inadmissible influence by incorrect software identification |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | IIP1 | III1 | IIB1 | IIA1 | IIN1 | IIC1 | IIR1 | III2 | IID1 | IIR2 | IIT1 | IIA2 | IIS1 |
| | | | | | | | | | | | | | | +1 | -1 |
| 1 | software in main component | | 4.3.1.1 | 5.1 | NA | NA | 4.3.2.1 | NA | 4.8.1.1 | 4.4.1.1 | 5.3.1 | 4.1.1 | NA | 4.4.2.1 | 4.6.1 |
| 2 | parameters in main component | | 4.3.1.1 | 5.1 | NA | NA | 4.3.2.1 | NA | 4.8.1.1 | 4.4.1.1 | 5.3.1 | 4.1.1 | NA | 4.4.2.1 | 4.6.1 |
| 3 | measurement data in main component | | 4.3.1.1 | 5.1 | NA | NA | 4.3.2.1 | NA | 4.8.1.1 | 4.4.1.1 | 5.3.1 | 4.1.1 | NA | 4.4.2.1 | 4.6.1 |
| 4 | measurement result in main component | | 4.3.1.1 | 5.1 | NA | NA | 4.3.2.1 | NA | 4.8.1.1 | 4.4.1.1 | 5.3.1 | 4.1.1 | NA | 4.4.2.1 | 4.6.1 |
| 5 | inscriptions for main component | | 4.3.1.1 | 5.1 | NA | NA | 4.3.2.1 | NA | 4.8.1.1 | 4.4.1.1 | 5.3.1 | 4.1.1 | NA | NA | 4.6.1 |
| 6 | evidence of an intervention in main component | | 4.3.1.1 | 5.1 | NA | NA | 4.3.2.1 | NA | 4.8.1.1 | 4.4.1.1 | 5.3.1 | 4.1.1 | NA | 4.4.2.1 | 4.6.1 |
| 7 | transmitted software (download) | | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | 4.5.3 | NA | NA |

Figure 13: Examination of combinations of assets and attack vectors for the measuring instrument with a software download feature, based on the software examination template.

## 4.6 EVSE with indication on the device of the consumer (DoC)

### 4.6.1 Overview

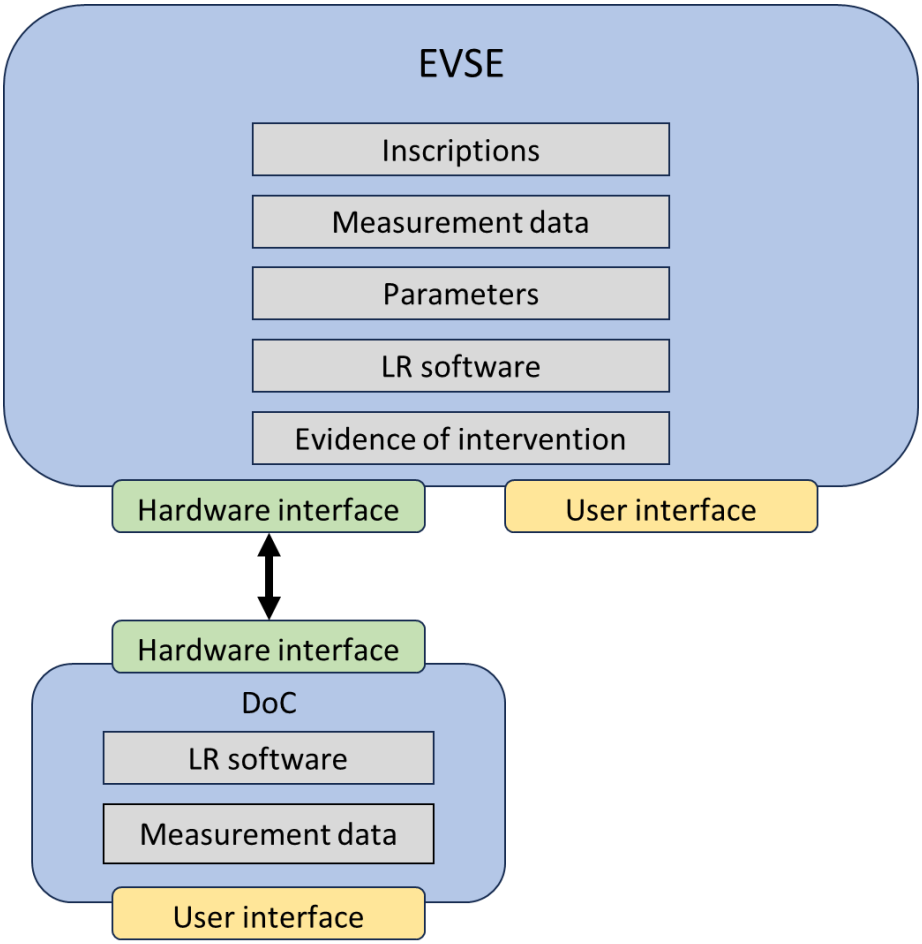


Figure 14: EVSE with a device of the consumer (DoC) to indicate the measurement data.

The measuring instrument consists of an Electronic Vehicle Supply Equipment (EVSE) and a personal device of the consumer. The EVSE contains an embedded firmware without an operating system. The device of the consumer runs an application[1] with the purpose to indicate measurement data.

Before starting a charging session, the EVSE checks availability and authenticity of the app on a consumer device via a cryptographic handshake. During the session, the EVSE sends the current measurement value to the app via a TLS-encrypted TCP-connection. The TLS-encryption ensures the authenticity of transmitted measurement data. The TCP-protocol stack in the app checks the integrity of transmitted data. If the check fails, the packet is transmitted again. Otherwise, the app acknowledges reception of the measurement data and indicates them. The EVSE terminates the measurement if no acknowledgement is received after a predefined period.

[1] This could also be a software library that encapsulates all legally relevant functions and is embedded into other applications.

The operating system of the consumer device or legally relevant software on the consumer device cannot influence the transmitted measurement data due to the encryption and it is automatically detected if the app is no longer running due to the immediate confirmation of received measurement data.

After initiation of the handshake, the app checks its own integrity by means of a checksum with a secret start vector. The app function is limited to indicating the measurement data and showing its software identifier upon request. The app does not contain device-specific parameters.

The communication flow is illustrated *Figure 15*.

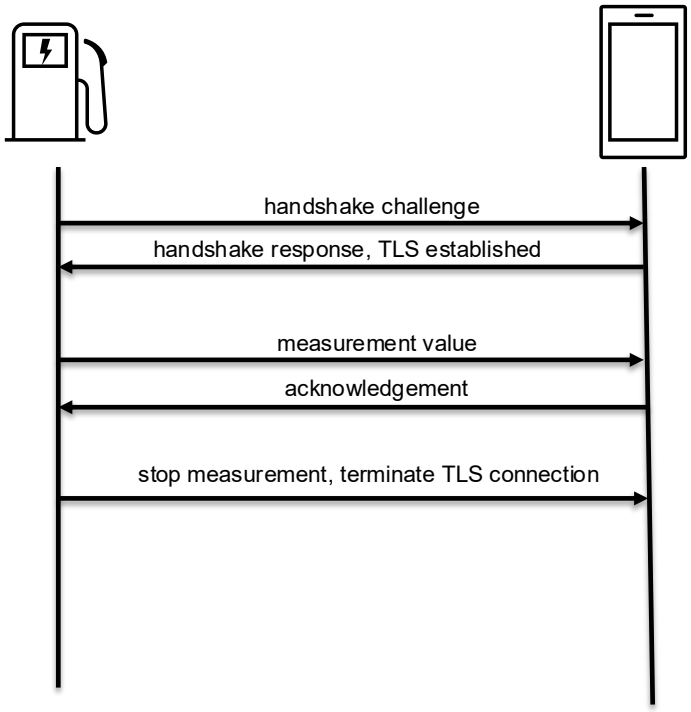


Figure 15: Communication flow between the EVSE and the DoC.

### 4.6.2 Assessment of inadmissible influences

In this example, the focus is on the examination of the application on the device of the consumer and the connection to the EVSE. In particular, the software and measurement data on the DoC are protected by the software on the EVSE that monitors the behavior of the DoC via the TLS connection.

**Assets-Threats-Matrix derived from WELMEC Guide 7.2: 2026**

**Threats consist of at least one asset and one corresponding statement of which security property (availability, integrity and/or authenticity) can be invalidated by the threat by means of an attack vector.**

| NA: Not applicable | RA: Risk analysis |
|---|---|
| AS: Acceptable solution | BO: RA and AS |

| Asset No. | Assets/Properties | Attack Vector No. | Inadmissible influence on the measurement process by executing other functions IIP1 | Inadmissible influence via user interfaces III1 | Inadmissible influence via the boot process IIB1 | Inadmissible influence via the administration of the operating system IIA1 | Inadmissible influence via legally non-relevant software IIN1 | Inadmissible influence by obtaining confidential information IIC1 | Inadmissible influence by replacing physical parts within the measuring instrument IIR1 | Inadmissible influence via hardware interfaces III2 | Inadmissible influence by downloading legally relevant software IID1 | Inadmissible influence by replacing or removing legally relevant components IIR2 | Inadmissible influence by man-in-the-middle attacks IIT1 | Inadmissible influence due to accidental modification IIA2 +1 | Inadmissible influence by incorrect software identification IIS1 -1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | software in EVSE | | 4.3.1.1 | 4.4.1.1 | NA | NA | NA | 4.4.1.1 | 4.8.1.1 | 4.4.1.1 | NA | 4.5.2 | NA | 4.4.1 | 4.6.1 |
| 2 | parameters in EVSE | | 4.3.1.1 | 4.4.1.1 | NA | NA | NA | 4.4.1.1 | 4.8.1.1 | 4.4.1.1 | NA | 4.5.2 | NA | 4.4.1 | 4.6.1 |
| 3 | measurement data in EVSE | | 4.3.1.1 | 4.4.1.1 | NA | NA | NA | 4.4.1.1 | 4.8.1.1 | 4.4.1.1 | NA | 4.5.2 | NA | 4.4.1 | 4.6.1 |
| 4 | measurement result in EVSE | | 4.3.1.1 | 4.4.1.1 | NA | NA | NA | 4.4.1.1 | 4.8.1.1 | 4.4.1.1 | NA | 4.5.2 | NA | 4.4.1 | 4.6.1 |
| 5 | inscriptions for component EVSE | | 4.3.1.1 | 4.4.1.1 | NA | NA | NA | 4.4.1.1 | 4.8.1.1 | 4.4.1.1 | NA | 4.5.2 | NA | 4.4.1 | 4.6.1 |
| 6 | evidence of an intervention in EVSE | | 4.3.1.1 | 4.4.1.1 | NA | NA | NA | 4.4.1.1 | 4.8.1.1 | 4.4.1.1 | NA | 4.5.2 | NA | 4.4.1 | 4.6.1 |
| 7 | measurement data transmitted from EVSE to BYOD | | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | 4.5.3 | NA | NA |
| 8 | software in BYOD | | NA | 4.4.1.1 | NA | 4.5.4 | 4.5.4 | 4.7.1 | NA | 4.4.1.1 | NA | 4.5.2 | NA | 4.4.1 | 4.6.1 |
| 11 | measurement result in BYOD | | NA | 4.4.1.1 | NA | 4.5.4 | 4.5.4 | 4.7.1 | NA | 4.4.1.1 | NA | 4.5.2 | NA | 4.4.1 | 4.6.1 |

Figure 16: Examination of combinations of assets and attack vectors for the measuring instrument consisting of EVSE and DoC, based on the software examination template.

# 5 References

[1] Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments (recast) Text with EEA relevance, OJ L 96, 29.3.2014, p. 149–250.

[2] Directive 2014/31/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of non-automatic weighing instruments (recast) Text with EEA relevance, OJ L 96, 29.3.2014.