WELMEC Guide 7.4

Draft

Examples of software evaluation

Version 2025-01-13

WELMEC

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.

For information:

This draft Guide has not been made available for the Working Group Measuring Instruments (European Commission expert group E01349) for consideration for future referencing on the Europa Website. This is for internal use within the Drafting Group for the recast of 7.4 only.

Published by:
WELMEC Secretariat

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

Draft recast

Exemplary applications of WELMEC Guide 7.2

Table of contents

Foreword

The application of the risk-based requirements as specified by Guide 7.2 and evaluated by using either Guide 7.3 in case of an acceptable solution, or Guide 7.6 in case the manufacturer applies a custom solution can be daunting.

This Guide aims to help both manufacturer and assessor to establish what is required to ensure compliance with the software related requirements of the MID [1] and the NAWID [2] for measuring instruments using known technology.

Known technology can, at the moment, be characterized to use three typical instances of an asset, namely processed, stored and transmitted and having the following assets: software, software identification, parameters, measurement data, evidence of an intervention, inscriptions, and indications with the security properties integrity, authenticity, and availability.

Deleted: records

Please note that Guide 7.6 also describes a procedure on how to evaluate the software related requirements in case of New Technology. This Guide only aims to assist and does in no way hinder or prevent the use of New Technology.

The examples provided in this Guide applies to measuring instrument of Risk Class B and C.

The limitation to measuring instrument with known technologies of Risk Class B and C means that no instrument-specific attack vectors are considered in this Guide.

1 Introduction

For the application and evaluation of the risk-based requirements, it is required that the manufacturer lists the applicable assets within his instrument or components, and the instances of these assets. Furthermore, the manufacturer has to list the design features of his instrument, such as storage devices, interfaces, operating systems.

For the conformity assessment, the manufacturer also has to supply a risk assessment report to demonstrate conformity of the instrument with the essential requirements, see MID [1] Annex II, Module B 3c and NAWID [2] Annex II, Module B 1.3c.

With regard to the software related requirements this means that the report has to cover all threats against all instances of all the assets present and the proposed measures (also called solutions) to mitigate those threats through securing and protection of the assets.

Securing and protection aims to ensure that inadmissible influences on the assets are either impossible or an intervention is detected and acted upon, i.e. the integrity, authenticity, and availability of all assets has to be ensured at all times.

The evaluator has to check for each asset present in a measuring instrument or component whether the solutions to mitigate the threats either make inadmissible influences impossible or inadmissible influences are detected and acted upon.

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

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

Deleted: records of events

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

- For example, in case of wireless transmission to a cloud storage device, a hardware seal to ensure authenticity might not be adequate.

This guide provides examples of instrument aspects to be evaluated. If necessary, remarks are made to explain how the applied technology might influence the applicability of certain acceptable solutions.

The guide starts with a complete measuring instrument with no communication interfaces and no operating system as a base line for the software evaluation and summarize the steps that need to be taken by the manufacturer and the evaluator with the help of tables.

The complete table can be found in the Excel sheet (to be provided) provided on the WELMEC website that contains all the assets with their instances, and attack vectors.

Additional design functionality is sequentially added to this basic measuring instrument in the form of an operating system, interfaces (hardware and software), and external devices and the use of different components. In each case, only the threats introduced by each design functionality are evaluated. It is assumed that the measuring instrument complies with the base line requirements, e.g., only the effect of the add-ons is considered.

2 Details

2.1 Measuring instrument legend

Colour	Description
	Asset
	Component (or complete measuring instrument)
	Hardware design (e.g., hardware interfaces, devices)
	Software design (e.g., user-interface)
	Not legally relevant design (hardware or software)

3 Examples

3.1 Basic measuring instrument

3.1.1 Overview

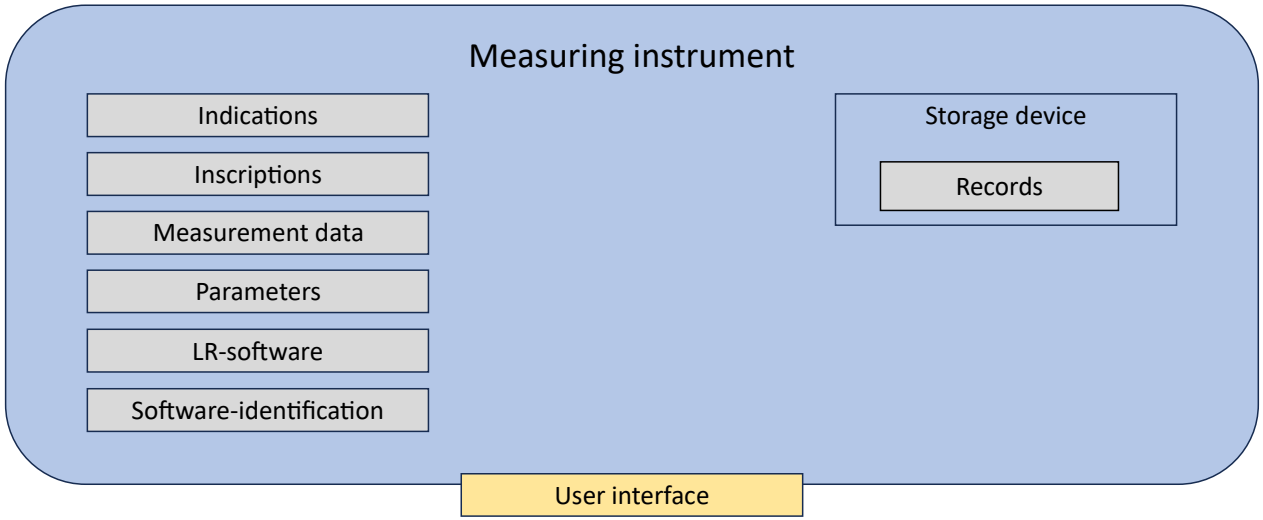

Figure 1: basic measuring instrument

The complete measuring instrument contains all components (e.g., the digital sensor and the digital data processing unit) in one housing and contains all assets. There is a storage device that contains software, software identification, parameters, stored measurement

Deleted: and records (including

data and logs. The indications are not stored, only processed. The measuring instrument has a user interface[1] which can be used to set LR parameters and to initiate a measurement. The measurement result is only displayed.

Due to the design of the instrument in this example, the following simplifications can be made

- The software identification is contained in the source code of the software and the securing and protection of the identification is part of the securing and protection of the software. Software and software identification are therefore evaluated as a single asset.
- The actual inscriptions are set as parameters and the securing and protection of the inscriptions is part of the securing and protection of the parameters. Inscriptions and parameters are therefore evaluated as a single asset.
- Considering stored assets, only the software (including the identification), parameters and measurement data are evaluated. The measurement result and the indications are not stored.

To conclude, we have

- processed assets: indications, measurement data, parameters (including inscriptions), software (including identification)and
- stored assets: software (including the identification), parameters and measurement data.

3.1.2 Assessment of inadmissible influences

	This combination of asset and threat is not possible (still open for discussion)
	This threat/asset is not applicable/present to/on this measuring instrument

				Processed			Stored			Transmitted			
Label	**Description**	**Assets**	**Measures**	**Integrity**	**Authenticity**	**Availability**	**Integrity**	**Authenticity**	**Availability**	**Integrity**	**Authenticity**	**Availability**	**Remarks**
IIP1	Execution of other functions	All	Securing & Protection										It is assumed that other legally relevant functions can

[1] Only a limited number of functions can be initiated through the user interface to simplify the example. In general, the user-interface will probably have more functionalities.

Deleted:)

Deleted: records are evaluated because in this example, stored records contain the parameters, inscriptions, and the

Deleted: , records

Deleted: records

Commented [ME1]: The order of attack vectors will be harmonized across all Guides during final editing.

													only impact asset availability.
III1	Through the user interface	All except parameters	Securing & Protection										
IIB1	Boot process	All	Securing & Protection										
IIA1	Administration of the O.S.	All	Securing & Protection										
IIN1	Not LR software	All	Securing & Protection										
III3	Software interfaces	All	Securing & Protection										
IIC1	Obtaining confidential information	All	Securing & Protection										
IIP2	Replacing parts	All	Securing & Protection										
III2	Hardware interfaces	All	Securing & Protection										
IIC3	Replacing or removing LR component	All	Securing & Protection										
IIT1	Man in the middle	All	Securing & Protection										
IIR1	Random errors	All	Securing										It is assumed that random errors cannot be secured against.

Commented [ME2]: A definition for "part" will be added to the terminology of Guide 7.2 to explain that "part" is any legally relevant physical property of a component that can be modified or removed.

		All	Protection										Random errors can only influence asset integrity.

Table 1: Combinations of assets, security properties and attack vectors that are assumed to be impossible with explanations.

				Processed			Stored			Transmitted			
Label	**Description**	**Assets**	**Measures**	**Integrity**	**Authenticity**	**Availability**	**Integrity**	**Authenticity**	**Availability**	**Integrity**	**Authenticity**	**Availability**	**Remarks**
IIP1	Execution of other functions	All	Securing & Protection			Custom			Custom				See[2]
III1	Through the user interface	All except parameters	Securing & Protection	4.2.3 protective interface									
III1	Through the user interface	parameters	Securing	4.2.1.1.6 password									
III1	Through the user interface	parameters	Protection	5.1 audit trail									
IIB1	Boot process	All	Securing & Protection										No OS
IIA1	Administration of the O.S.	All	Securing & Protection										No OS
IIN1	Not LR software	All	Securing & Protection										No NLR software
III3	Software interfaces	All	Securing & Protection										No NLR software

[2] Other functions are not assumed to affect integrity of assets for discrete measurements.

IIC1	Obtaining confidential information	All	Securing & Protection										No confidential information
IIP2	Replacing parts	All	Securing & Protection				4.2.5.1.2 hardware seal on the storage medium						Only the storage device can be replaced
III2	Hardware interfaces	All	Securing & Protection										No hardware interfaces
IIC3	Replacing or removing LR component	All	Securing & Protection										No components
IIT1	Man in the middle	All	Securing & Protection										No transmission
IIR1	Random errors	All	Securing										
		All except software	Protection	4.1.1 CRC with secret start value and an audit trail			4.1.1 CRC with secret start value and an audit trail						
		software	Protection	4.1.1.3 checksum over software with secret start value and an audit trail			4.1.1.3 checksum over software with secret start value and an audit trail						

Table 1: Coverage of inadmissible influences for the basic measuring instrument

Commented [ME3]: A definition for "part" will be added to the terminology of Guide 7.2 to explain that "part" is any legally relevant physical property of a component that can be modified or removed.

For the open fields, the manufacturer must mitigate the threat by either an acceptable solution or a custom solution (risk analysis).

Note: This guide uses certain acceptable or custom solutions to illustrate the procedure. The manufacturer is free to implement any solution of his choice, be it an acceptable solution from Guide 7.3 or a new solution that must be assessed via risk assessment. The guides do not restrict in any way the approach the manufacturer wants to use, provided it meets the requirements.

Below, an example is given how inadmissible influence can be evaluated.

We evaluate the inadmissible influence through the user interface (III1) on the assets. The following acceptable solutions are evaluated.

	4.2.1.1.6 Password	4.2.3.2 (Restricted rights for the user interface)	4.2.3 (protective interface)	5.1 (audit trail)
Covered	Assets: all Instances: all Properties: all Measures: securing	Assets: all Instances: all Properties: all Measures: protection and securing	Assets: all[3] Instances: all Properties: all Measures: depends on implementation	Assets: all Instances: stored Properties: all Measures: protection
Conditions	-	OS	-	-
Summary	Only secures the assets, protection is not covered	Not possible because there is no OS	Depending on the implementation, the protective interface can cover multiple inadmissible influences	Does not secure the assets

For this instrument, we will assume the following: all assets except parameters are protected and secured against inadmissible influences from the user interface because a protective interface was implemented (no inadmissible influence from the user interface on the assets is possible). The parameters can be set by the user, so a password is needed to secure them as well as a solution to protect them separately from all other assets, already covered by the protective interface. Further, it is assumed that there is an audit trail that records any changes to the parameters, i.e., implements protection.

The manufacturer can now fill out the corresponding row (see rows for III1 in Table 2).

[3] Parameters are dealt with by a different acceptable solution in this example.

The manufacturer needs to repeat this procedure for every cell in the table that is blank to ensure that the measuring instrument is adequately secured and protected, as illustrated in Table 2.

The manufacturer must prove, with a risk assessment according to Guide 7.6, that his custom solution to protect and secure the assets through the execution of other functions covers all assets in all instances.

With the help of this tool the manufacturer can visualise if the measuring instrument has been adequately secured and protected. The manufacturer has to supply the technical documentation to the evaluator and it is recommended that the table above is part of that technical documentation.

The evaluator needs to check if the technical documentation is correct and complete and establish what needs to be evaluated.

- A custom solution to prevent inadmissible influences through executing other functions for which Guide 7.6 has to be used to check if this solution is implemented correctly and is adequate.
- A number of acceptable solutions for which Guide 7.3 has to be used to check if this solution is implemented correctly, meets the conditions and is adequate.

3.2 Separated storage

3.2.1 Overview

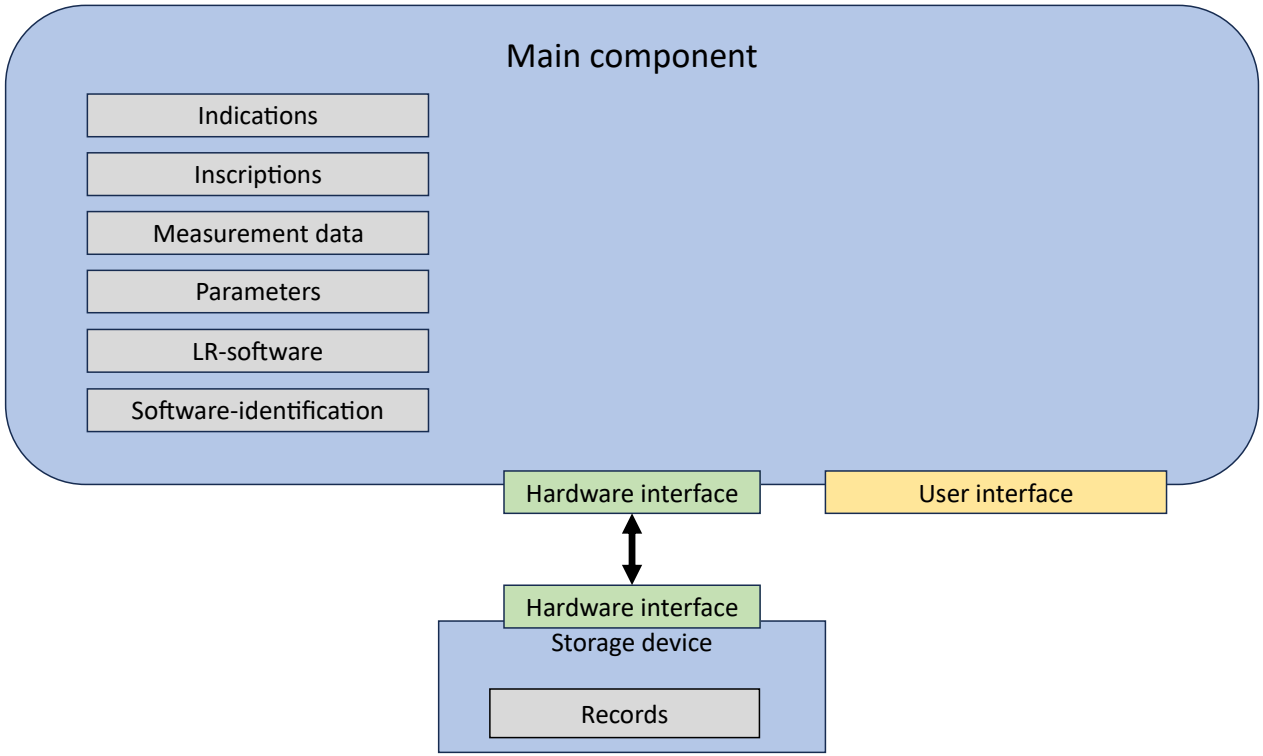

Figure 2: Measuring instrument with separated storage

The instrument consists of a main component that contains all assets necessary for providing measurement functionality except long-term storage, e.g. A/D conversion of sensor data, data processing, user interface, calculation and indication of the measurement result. Measurement data are stored in a separate component. Both components communicate via hardware communication interfaces. Upon request of the main component, measurement results are transmitted back to the main component and indicated there.

Deleted: Records

Deleted: records of

3.2.2 Assessment of inadmissible influences

The procedure is similar to the basic measuring instrument in section 3.1. The table of inadmissible influences has to be expanded by the influences III2 (hardware interfaces), IIC3 (replacing or removing components) and IIT1 (man in the middle) due to the connection between both components.

The other inadmissible influences that were applied to the basic measuring instrument still apply here but are considered solved in the same manner. Therefore, only the new inadmissible influences are analysed.

				Processed			Stored			Transmitted			
Label	**Description**	**Assets**	**Measures**	**Integrity**	**Authen-ticity**	**Availabil-ity**	**Integrity**	**Authen-ticity**	**Availabil-ity**	**Integrity**	**Authen-ticity**	**Availabil-ity**	**Re-marks**
IIP1	Execution of other func-tions	All	Securing & Protection										As be-fore (exam-ple 3.1)
III1	Through the user interface	All	Securing & Protection										As be-fore (exam-ple 3.1)
IIB1	Boot process	All	Securing & Protection										As be-fore (exam-ple 3.1)
IIA1	Administration of the O.S.	All	Securing & Protection										As be-fore (exam-ple 3.1)

IIN1	Not LR software	All	Securing & Protection										As before (example 3.1)
III3	Software interfaces	All	Securing & Protection										As before (example 3.1)
IIC1	Obtaining confidential information	All	Securing & Protection										As before (example 3.1)
IIP2	Replacing parts	All	Securing & Protection	4.2.5.1.1 hardware seals			4.2.5.1.1 hardware seals						
III2	Hardware interfaces	All	Securing & Protection	4.2.3.1 protective interface			4.1.1.1 checksum with secret start value for stored and transmitted assets excluding the software with an audit trail or event counter						
IIC3	Replacing or removing LR component	All	Securing & Protection	4.2.5.1.1 hardware seals			4.2.3.3.4 cryptographically paired						
IIT1	Man in the middle	All	Securing & Protection				4.1.1.1 checksum with secret start value for stored and transmitted assets excluding the software with an audit trail or event counter			4.1.1.1 checksum with secret start value for stored and transmitted assets excluding the software with an audit trail or event counter			Only affects assets outside the main component
IIR1	Random errors	All	Securing										As before (example 3.1)

			Protection										As before (example 3.1)

3.3 External Display

3.3.1 Overview

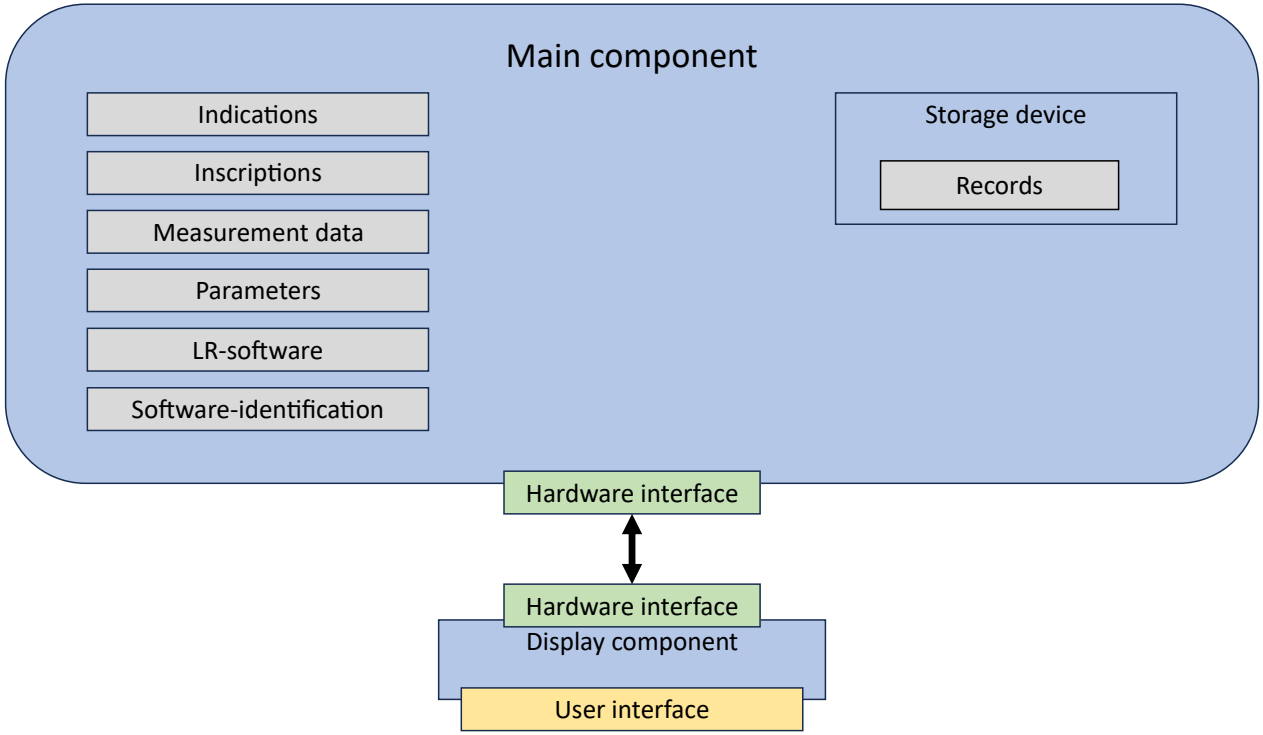

Figure 3: Measuring instrument with external display

The instrument consists of a main component that realizes collection of sensor data, data processing, 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 and secured according to acceptable solutions from Guide 7.3. If the display component is disconnected, measurement results are stored on the main component until a connection with display component has been reestablished. The user interface provides all functionality necessary to retrieve and indicate individual measurement results.

3.3.2 Assessment of inadmissible influences

The other inadmissible influences that were applied to the basic measuring instrument still apply here but are considered solved in the same manner. Therefore, only the new inadmissible influences are analysed.

				Processed			Stored			Transmitted			
Label	**Description**	**Assets**	**Measures**	**Integrity**	**Authenticity**	**Availability**	**Integrity**	**Authenticity**	**Availability**	**Integrity**	**Authenticity**	**Availability**	**Remarks**
IIP1	Execution of other functions	All	Securing & Protection										Not evaluated
III1	Through the user interface	All	Securing & Protection										Not evaluated
IIB1	Boot process	All	Securing & Protection										No OS
IIA1	Administration of the O.S.	All	Securing & Protection										No OS
IIN1	Not LR software	All	Securing & Protection										No NLR software
III3	Software interfaces	All	Securing & Protection										No NLR software
IIC1	Obtaining confidential information	All	Securing & Protection										No confidential information
IIP2	Replacing parts	All	Securing & Protection	4.2.5.1.1 hardware seals			4.2.5.1.1 hardware seals						

III2	Hardware interfaces	All	Securing & Protection	4.2.3.1 protective interface			4.1.1.1 checksum with secret start value for stored and transmitted assets excluding the software with an audit trail or event counter						
IIC3	Replacing or removing LR component	All	Securing & Protection	4.2.3.3.4 cryptographically paired									
IIT1	Man in the middle	All (except indication)	Securing & Protection							4.1.1.1 checksum with secret start value for stored and transmitted assets excluding the software with an audit trail or event counter	4.2.5.1.1 hardware seals		
IIT1	Man in the middle	indication	Securing & Protection							4.1.1.1 checksum with secret start value for stored and transmitted assets excluding the software with an audit trail or event counter	4.2.5.1.1 hardware seals	Mentioned separately to address the example explicitly	
IIR1	Random errors	All	Securing										
			Protection										Not evaluated

3.4 Operating system

3.4.1 Overview

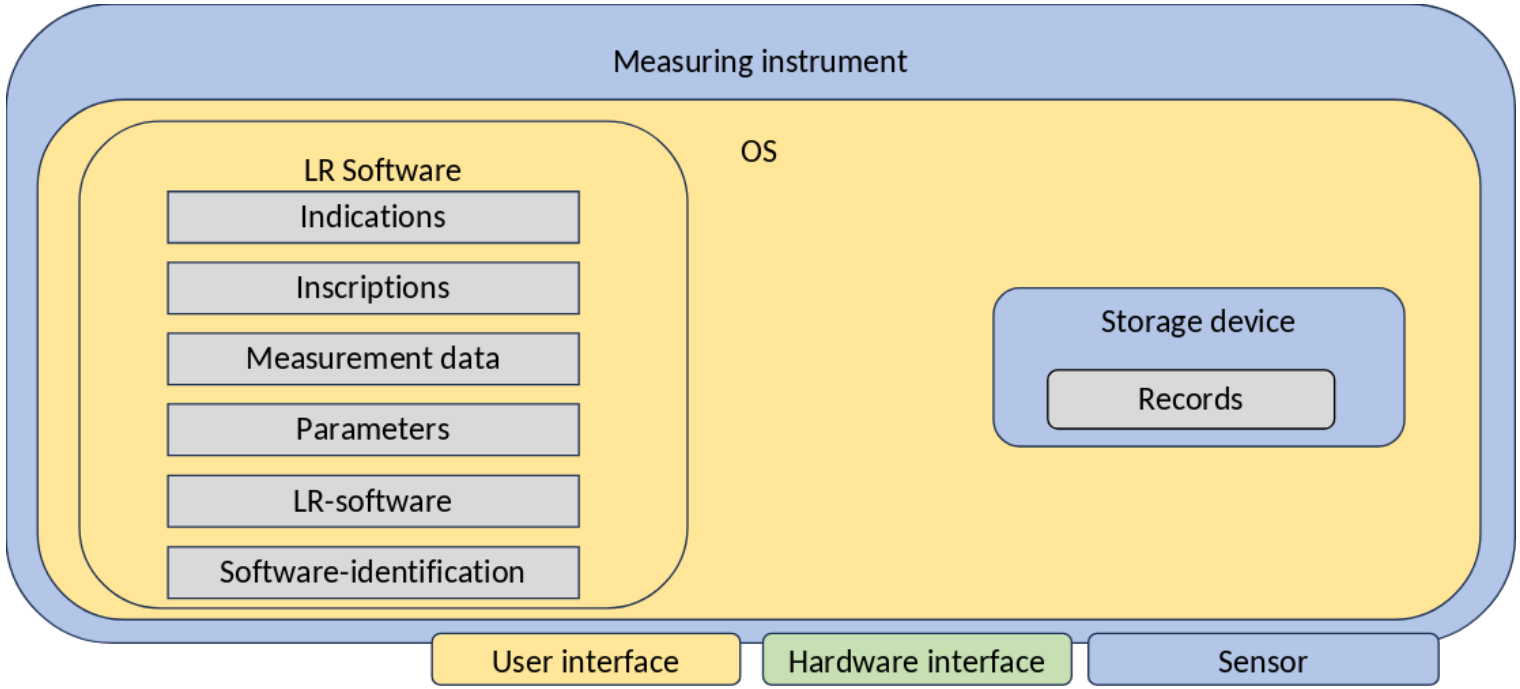

Figure 4: Measuring instrument with an operating system

The instrument consists of a sensor with a digital output connected to a small, embedded PC inside a sealed housing. On the embedded PC runs an operating system, on which an application for visualization of the measurement result and error logging runs. 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.

3.4.2 Assessment of inadmissible influences

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

				Processed			Stored			Transmitted			
Label	**Description**	**Assets**	**Measures**	**Integrity**	**Authenticity**	**Availability**	**Integrity**	**Authenticity**	**Availability**	**Integrity**	**Authenticity**	**Availability**	**Remarks**
IIP1	Execution of other functions	All	Securing & Protection										Not evaluated
III1	Through the user interface	All	Securing & Protection										Not evaluated
IIB1	Boot process	All	Securing & Protection	4.2.2.1.3 securing the OS configuration with BIOS settings									
IIA1	Administration of the O.S.	All	Securing & Protection	4.2.2.2.1 access rights configuration (requires OS)									
IIN1	Not LR software	All	Securing & Protection										No NLR software
III3	Software interfaces	All	Securing & Protection										No NLR software
IIC1	Obtaining confidential information	All	Securing & Protection										No confidential information

IIP2	Replacing parts	All	Securing & Protection	4.2.5.1.1 hardware seals									
III2	Hardware interfaces	All	Securing & Protection										Not evaluated
IIC3	Replacing or removing LR component	All	Securing & Protection										Not evaluated
IIT1	Man in the middle	All	Securing & Protection										Not evaluated
IIR1	Random errors	All	Securing										
			Protection										Not evaluated

3.5 Software download

3.5.1 Overview

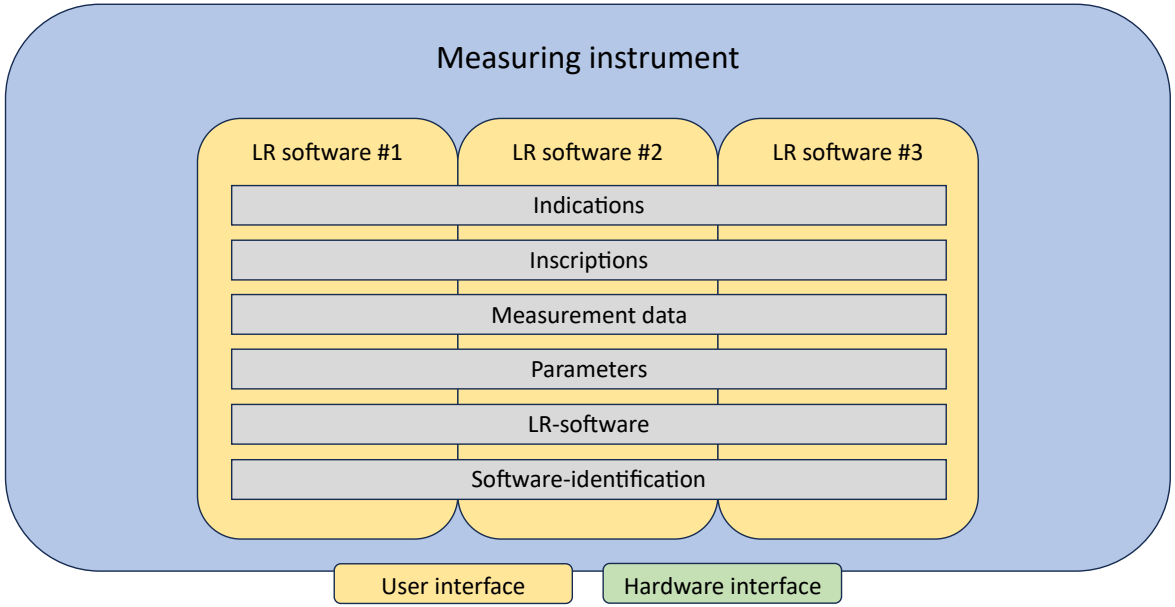

Figure 5: Measuring instrument with download functionality

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

3.5.2 Assessment of inadmissible influences

				Processed			Stored			Transmitted			
Label	**Description**	**Assets**	**Measures**	**Integrity**	**Authenticity**	**Availability**	**Integrity**	**Authenticity**	**Availability**	**Integrity**	**Authen-ticity**	**Availa-bility**	**Remarks**
IIP1	Execution of other functions	All	Securing & Protection										Not evaluated
III1	Through the user interface	All	Securing & Protection										Not evaluated
IIB1	Boot process	All	Securing & Protection										No OS
IIA1	Administration of the O.S.	All	Securing & Protection										No OS
IIN1	Not LR software	All	Securing & Protection										No NLR software
III3	Software interfaces	All	Securing & Protection										No NLR software
IIC1	Obtaining confidential information	All	Securing & Protection										No confidential information
IIP2	Replacing parts	All	Securing & Protection										No parts
III2	Hardware interfaces	All except stored measurement data	Securing & Protection	4.2.3.1 protective interface									
III2	Hardware interfaces	stored measurement data	Securing & Protection	4.2.5.3.1 fixed legally relevant download manager + 4.1.1.3 checksum over software with a secret start value and an audit trail or event counter									Records realized as audit rail
IIC3	Replacing or removing LR component	All	Securing & Protection										Not evaluated

Deleted: records

Deleted: Records

IIT1	Man in the middle	software	Securing & Protection	4.2.3.1 protective interface						4.1.2.3 electronic signature over transmitted software		4.1.2.4 retransmissions for transmitted software	Transmisison of software implies download
IIR1	Random errors	All	Securing										
			Protection										Not evaluated