WELMEC 7.3
2020

WELMEC

European Cooperation in Legal Metrology

Reference Architectures

Based on WELMEC Guide 7.2

For information:
This guide is available to the Working Group Measuring Instruments for future reference on the Europa Website.

WELMEC

European Cooperation in Legal Metrology

WELMEC is 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 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 as to the best practice to be followed.

Published by:
WELMEC Secretariat

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

Reference Architectures

Contents

Foreword

The Guide in hand is based on WELMEC Guide 7.2 “Software” [1]. This Guide reflects the current position of WELMEC WG 7 Software.

Other WELMEC Working Groups may impose additional formal or technical requirements. Especially instrument specific requirements and additional requirements for the control of the measuring task after placed on the market or put into used need to be considered.

The Guide is purely advisory and does not itself impose any restrictions or additional technical requirements beyond those contained in the MID. 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.

Please note: This Guide is valid for Directive 2004/22/EC and 2014/32/EU [2, 3].

Introduction

The drivers for innovation are the increasingly globalized market place, the ever-increasing drive for efficiency and the rapidly developing consumer demands. New growth opportunities therefore come from providing new products and services, from technological breakthroughs, new processes and business models, non-technological innovation and innovation in the services sector [6].

Manufactures active in the legal metrology sector take part in this process. To accompany their activity in making available new products on the market barriers to innovation within the process of conformity assessment needs to be identified and solutions needs to be offered.

Discussions within WELMEC regarding this topic have formed the conviction that offering the manufacturers a template for their instrument design would be a great benefit to ensure that the envisioned innovative product is in line with the regulatory requirements. Simultaneously, such a template will provide the Notified Bodies with a scheme to match innovative product designs within the course of the conformity assessment process.

To this end the Guide at hand provides a generalized template of a measuring instrument based on the modular concept of WELMEC Guide 7.2 which reflects the structure of the Directive MID. Founded on this template architectural examples for innovative approaches in measuring instruments could be modelled. Models of specific reference architectures are already provided in the Guide and it is envisioned to add further reference architectures according to the needs of the stakeholders.

In these models it is indicate which part of WELMEC Guide 7.2 needs particular attention.

The level of detail 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, please see the cross reference in WELMEC Guide 7.2 [1].

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

For the terms used in this Guide please revere to the terminology section of WELMEC Guide 7.2 [1]. Definitions for all other terms are given below.

Mother Unit: Instrument or part of an instrument that fulfils applicable software requirements. One or more functionalities described in WELMEC Guide 7.2, however, are moved to a separate component. Separate component and mother unit together fulfil all requirements of WELMEC Guide 7.2.

Remote Connection: The term describes the making available of the modules to the mother unit (see there) via digital communication networks, e.g. the internet.

Display Software: Legally relevant software for displaying or printing measurement data (e.g. L6, S2) along with the relevant information (e.g. L1). Displayed or printed measurement data shall indicate an eventual violation of authenticity and integrity.

2 How to use this Guide

This section describes the organisation of the Guide and explains how to use it.

The aim of the Guide is to provide a template for mapping measuring instrument designs based on new technological developments to the requirements of WELMEC Guide 7.2. With these identified applicable requirements, fulfilment of the essential requirements from the MID may be shown. The Guide supports the innovations of manufacturers and the work of Notified Bodies by facilitating development work of manufacturers and the evaluation procedures of Notified Bodies.

When assessing a new technological development, the following procedure should be applied:

- Compare the instrument design with the generalized architecture of a measuring instrument and check if all components of the modular architecture are present, see Section 3.2.
- The result identifies deviations between the instrument design and the generalized architecture which need adaptation according to WELMEC Guide 7.2.
- Check if the examined instrument design is covered by one of the examples given in this Guide, see Sections 4. These examples provide guidance which specific requirements of WELMEC Guide 7.2 need to be fulfilled, see Section 4.x.5.
- If the examined instrument design is not covered by the examples, please contact WELMEC WG 7 “Software” with the modelled architecture according to Section 3.2 to have your approach analysed and maybe included in this Guide.
- If requirements according to this Guide are fulfilled, requirements for test of conformity and in-service control according to WELMEC Guide 7.2 are met, see Section 4.x.6.
- Within the process of conformity assessment, a risk analysis by the manufacturer is required. For each example specific attack vectors are provided, see Section 4.x.7. A list of common attack vectors which always should be considered is provided in Section 5.
- Apply the instrument specific software requirements of WELMEC Guide 7.2’s Extension I.

2.1 Overall structure of the Guide

The Guide is structured as follows: firstly, it reviews briefly the modular concept of WELMEC Guide 7.2 in chapter 3.1. From this foundation a generalized architecture for a software-based measuring instrument is derived in chapter 3.2. In this way technological concepts, e.g. for IoT devices, Cloud Computing etc., could be modeled and the question regarding their conformity to the essential requirements and the coverage by the technical interpretation of the WELMEC Guide 7.2 could be analyzed. For selected technological concepts so called **reference architectures** are provided in chapter 4 which constitute a confirm realization of this technological approach.

Stringent demands for adequate risk assessment [5] when securing software can be found in the Directive (2014/32/EU) [2]. A list of common attack vectors, i.e. a scheme how threats could be realized, was developed in WELMEC WG 7 and is provided in chapter 5 to guaranty comparability of the analysis between the manufacturers and the

Notified Bodies. Additionally, specific attack vectors for the individual reference architectures are also given.

2.2 How to select the appropriate parts of the Guide

The main challenges for such a reference architecture are to encompass the fulfillment of the essential requirements, support easy verification and inspection of the meter in the market and exploration of contemporary risks and threats for measuring instruments via an adequate risk analysis.

To analyze if an envisioned measuring instrument design is in conformity with the essential requirements and could be covered by the technical interpretation of the WELMEC Guide 7.2 the generalized architecture for a software-based measuring instrument from chapter 3.2 should be applied. In this way a technological concept could be modeled and the question regarding its conformity to the essential requirements and the coverage by the technical interpretation of the WELMEC Guide 7.2 could be analyzed. With such an approach WELMEC WG 7 could be addressed, e.g. by the manufacturers or Notified Bodies.

Additionally, the Guide at hand provides reference architectures, which are architectural examples for technological challenges by using the generalized model of a measuring instrument in Section 4.

Therewith, the reference architectures provide the fulfillment of MID's Annex I software requirements by fulfilling the architecture relevant requirements from WELMEC Guide 7.2. Within those requirements and module B links to the test of conformity and in-service control, i.e. to the verification of the meter, are established by MID Annex I 8.2, 8.3, 7.2, 7.6 and Module B Nr.6. Furthermore, architecture specific attack vectors are proposed additionally to the general list of attack vectors as provided in chapter 5 for the risk assessment [4] as demanded as part of the conformity assessment [2].

To make a general reference architecture applicable for a specific class of instruments, it must fulfill additional instrument-specific requirements and needs tailoring to the risk class of the instrument.

The Guide at hand starts with architectures which use remote connection to legally relevant parts. Further architectures shall follow according to the needs of the stakeholders.

3 Generalized Architecture of a Measuring Instrument

3.1 Modular Concept of WELMEC Guide 7.2

WELMEC Guide 7.2 [1] provides technical interpretation of the essential requirements laid down in Annex I of MID (2014/32/EU) and module B. Its structure follows a generic modular concept which allows to describe a large variety of technological IT architectures (s. figure 1). This modular approach guaranties openness for new technologies, is future proof and hence supports innovations.

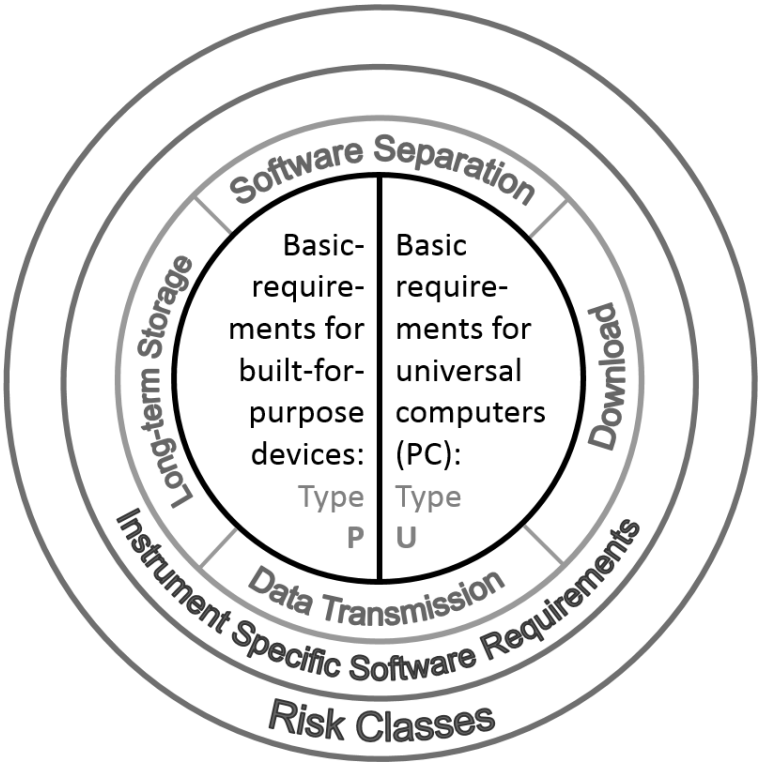

Figure 1: Modular structure of the WELMEC Guide 7.2 "*Software"* [1]

3.2 Derived Generalized Architecture of a Measuring Instrument

With the general modules and specific terms defined in the WELMEC Guide 7.2 [1] a refined modular structure could be established which resembles a generalized architecture of a measuring instrument (s. figure 2).

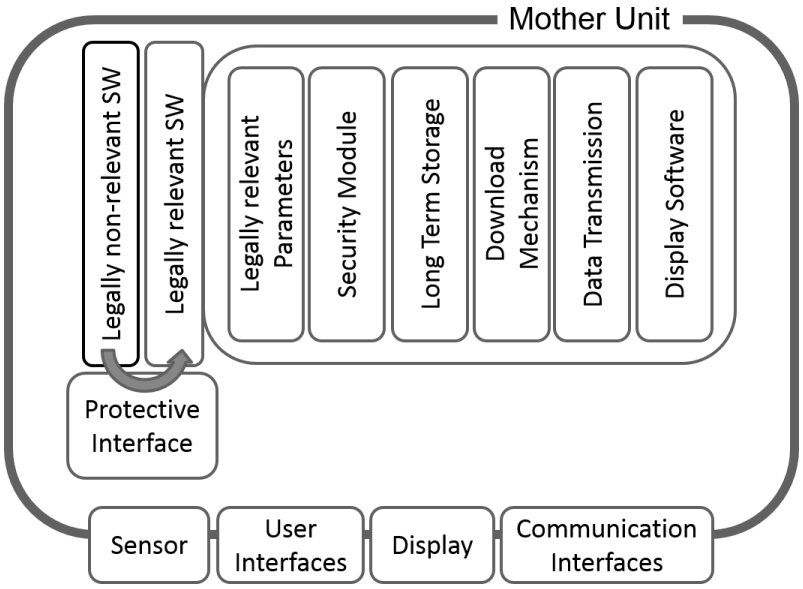

Figure 2: General Architecture resembling the refined modular structure of the WELMEC Guide 7.2 “Software”

Please note: The „Security Module“ integrates all legally relevant security measures e.g. for integrity, authenticity, checksum calculation, key and certificate management, software identifier, Logbook/file, etc.

This generalized measurement instrument should be utilized to define reference architectures. In this way a technological concept could be modeled and the question regarding its conformity to the essential requirements and the coverage by the technical interpretation of the WELMEC Guide 7.2 could be analyzed. With such an approach WG 7 could be addressed, e.g. by the manufacturers or Notified Bodies.

On that basis the Guide at hand provides architectural examples for technological challenges by using the generalized model and indicating which part of WELMEC Guide 7.2 ensures that this challenge covers the essential requirements according to MID’s Annex 1 and module B.

Instrument specific requirements must be added to the proposed architectures.
For an appropriate risk assessment, specific attack vectors are provided for each architecture which should be applied additionally to the generic attack vectors offered in chapter 5.

4 Remote Connection to Legally Relevant Components

In the following we distinguish between external modules and the residual modules in the mother unit. The term “remote connection” describes the making available of the modules to the mother unit via communication networks, e.g. the internet.
The boundary conditions in this Guide state, that the measurement instrument is provided by the manufacturer as a whole for conformity assessment according to module B. If parts of the instrument are provided by an external service provider, e.g. the external storage device etc., the role responsibilities laid down in the MID (2014/32/EU) do not change, i.e. the manufacturer who applies for the EU type examination stays responsible.

4.1 Remote connection of the Sensor

4.1.1 Specifying Description:

Measurement data are created externally by the digital sensor. The sensor is “paired” with the mother unit, its location is identifiable, and each sensor provides a unique identifier. Pairing is the process by which two devices exchange device information so that a secure link can be established. The process of pairing devices is aimed at creating a shared secret between two devices according to P8/U8.

4.1.2 Specifying Architecture:

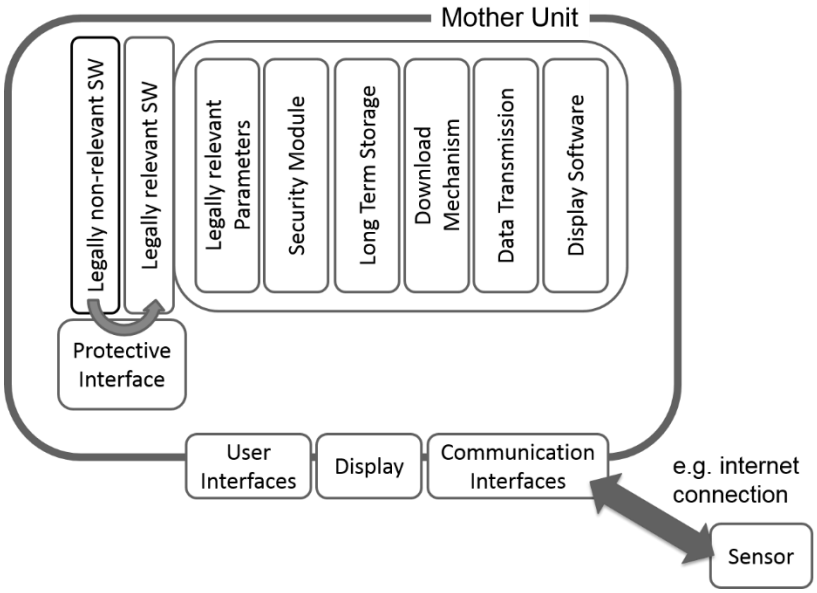

Figure 3: Reference architecture for the remote connection of the sensor

4.1.3 Boundary Conditions:

The measurement instrument is provided by the manufacturer as a whole for conformity assessment according to module B, i.e. the sensor is also provided by the manufacturer. Changes of the sensor hardware are tracked in a logbook. The basic requirements regarding the type of instrument (P or U) are fulfilled individually by the mother unit and the separated part. Availability of all components, i.e. completeness

of the measurement instrument is required and is guaranteed if MID's Annex I is fulfilled.

4.1.4 Specific Requirements:

- It is guaranteed that the remote component is paired with the mother unit according to P8/U8.
- If the external unit is replaced by a similar unit which was not paired with the mother unit the measuring Instrument should not function and re-verification with the similar external unit which was paired with the mother unit according to P8/U8 is required.
- Identification of the external unit and the corresponding mother unit must be possible.
- If there are several approved remote sensors available, the identifiers of the remote sensors are legally relevant parameters to guaranty that a change of the sensor provides an evidence of an intervention.

4.1.5 Requirements from WELMEC Guide 7.2 covering this Architecture configuration:

Fulfillment of requirements by following extension T: Transmission of Measurement Data via Communication networks.

Requirement	Description
T1	Completeness of transmitted data
T2	Protection against accidental or unintentional changes
T3	Integrity of Data
T4	Authenticity of transmitted data
T5	Confidentiality of keys,
T6	Handling of corrupted data
T7	Transmission delay
T8	Availability of transmission services

Table 4.1.5: Architecture relevant configuration

4.1.6 Requirements in the field for test of conformity and in-service control:

Requirement	Fulfillment is assumed, …
MID Annex I 8.2 "provide evidence of an intervention"	if P/U are fulfilled in combination with the required extensions.
MID Annex I 8.3 "software identification shall be easily provided"	if P/U are fulfilled in combination with the required extensions.
MID Annex I 7.2 "no unreasonable demands of the user"	if P/U are fulfilled in combination with the required extensions.

Table 4.1.6: Requirements for test of conformity and in-service control

4.1.7 Specific Attack Vectors to be considered in the risk assessment:

Beside the general list of attack vectors provided in chapter 5 the following should be considered for this specific architecture:

- **A_Tampering_and_Injection:** An attacker manipulates the communication between the sensor and the mother unit, harms the integrity of measurement data.
- **A_Spoofing:** An attacker pretends to be one of the communication partners (either sender or receiver), harms authenticity of measurement data.

4.2 Remote Connection to the Stored Measurement Data

4.2.1 Specifying Description:

The first storage of the measurement data is done remotely. There is no local copy of the measurement data in the mother unit.

4.2.2 Specifying Architecture:

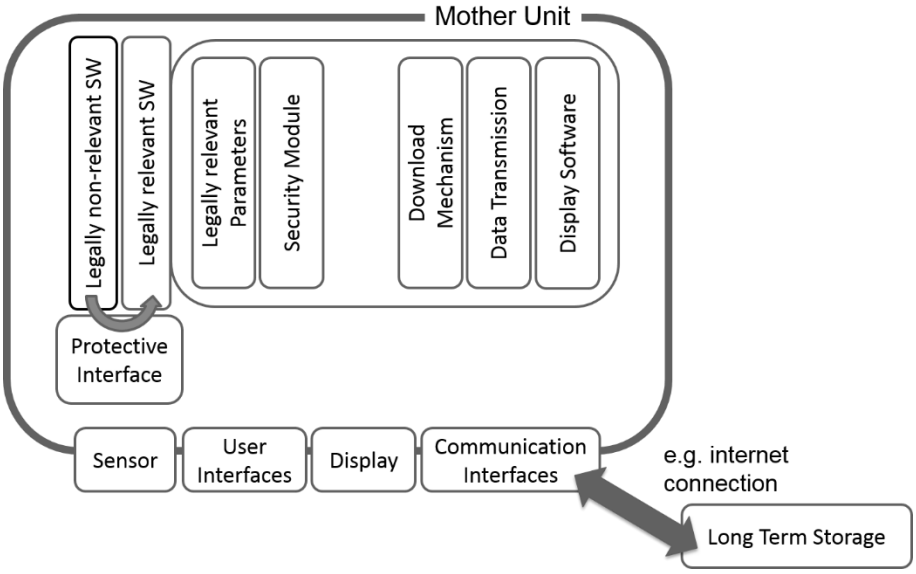

Figure 4: Reference architecture for the remote connection of measurement data

4.2.3 Boundary Conditions:

The measurement instrument is provided by the manufacturer as a whole for conformity assessment according to module B, i.e. the external storage device is also provided by the manufacturer. If parts of the instrument are provided by an external service provider, e.g. the external storage device, the role responsibilities laid down in the MID (2014/32/EU) do not change, i.e. the manufacturer who applies for the EU type examination stays responsible. The basic requirements regarding the type of instrument (P or U) are fulfilled individually by the mother unit and the separated part. Availability of all components, i.e. completeness of the measurement instrument is required and is guaranteed if MID's Annex I is fulfilled. The remote storage unit does not contain legally relevant software. All integrity measures for the remotely stored data are provided by the mother unit.

4.2.4 Specific Requirements:

None.

4.2.5 Requirements from WELMEC Guide 7.2 Covering this Architecture Configuration:

Fulfillment of the following requirements make the process independent from a specific hardware of the remote storage device.

Fulfillment of requirements by following extension L: Long-term Storage of Measurement Data.

Requirement	Description
L1	Completeness of measurement data stored
L2	Protection against accidental or unintentional changes
L3	Integrity of data
L4	Authenticity of measurement data stored
L5	Confidentiality of keys
L6	Retrieval, verification, and indication of stored data
L7	Automatic storing
L8	Storage capacity and continuity

Table 4.2.5: Architecture relevant configuration

4.2.6 Requirements in the field for test of conformity and in-service control:

Requirement	Fulfillment is assumed
MID Annex I 8.2 “provide evidence of an intervention”	if P/U are fulfilled in combination with the required extensions.
MID Annex I 8.3 “software identification shall be easily provided”	if P/U are fulfilled in combination with the required extensions.
MID Annex I 7.2 “no unreasonable demands of the user”	if P/U are fulfilled in combination with the required extensions.

Table 4.2.6: Requirements for test of conformity and in-service control

4.2.7 Specific Attack Vectors to be Considered in the Risk Assessment:

Beside the general list of attack vectors provided in chapter 5 the following should be considered for this specific architecture:

- **A_Tampering_and_Injection**: An attacker manipulates the communication between the long-term storage unit and the mother unit, harms the integrity of measurement data.
- **A_Spoofing**: An attacker pretends to be one of the communication partners (either sender or receiver), harms authenticity of measurement data.

4.3 Remote connection to the Legally Non-Relevant Software

4.3.1 Specifying Description:

Legally none-relevant software is provided externally by an internet-based service, hosted by the manufacturer. There is only legal relevant software on the mother unit.

4.3.2 Specifying Architecture:

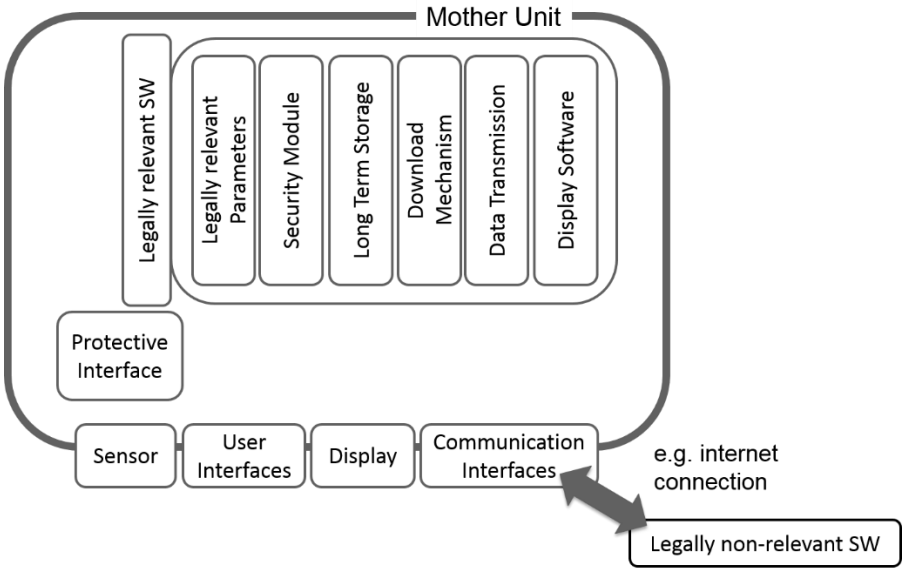

Figure 5: Reference architecture for the remote connection of legally non-relevant Software

4.3.3 Boundary Conditions:

The measurement instrument is provided by the manufacturer as a whole for conformity assessment according to module B, i.e. the technical structure containing the legally non-relevant software is provided by the manufacturer. If parts of the instrument are provided by an external service provider, e.g. the technical structure containing the legally non-relevant software, the role responsibilities laid down in the MID (2014/32/EU) do not change, i.e. the manufacturer who applies for the EU type examination stays responsible. The basic requirements regarding the type of instrument (P or U) are fulfilled individually by the mother unit and the separated part. Availability of all components, i.e. completeness of the measurement instrument is required and is guaranteed if Annex I is fulfilled.

4.3.4 Specific Requirements:

None.

4.3.5 Requirements from WELMEC Guide 7.2 Covering this Architecture Configuration:

No requirements on the legally non-relevant software if the extensions S is applied.

4.3.6 Requirements in the field for test of conformity and in-service control:

Requirement	Fulfillment is assumed
MID Annex I 8.2 “provide evidence of an intervention”	if P/U are fulfilled in combination with the required extensions.
MID Annex I 8.3 “software identification shall be easily provided”	if P/U are fulfilled in combination with the required extensions.
MID Annex I 7.2 “no unreasonable demands of the user”	if P/U are fulfilled in combination with the required extensions.

Table 4.3.6: Requirements for test of conformity and in-service control

4.3.7 Specific Attack Vectors to be Considered in the Risk Assessment:

Beside the general list of attack vectors provided in chapter 5, the following should be considered for this specific architecture:

None.

4.4 Remote Connection to the Legally Relevant Software

4.4.1 Specifying Description:

Part of the legally relevant software is provided externally by an internet-based service hosted by the manufacturer. Please note that this Guide provides general models. Therefore, instrument specific requirements may apply to the part of the legally relevant software that could be remotely accessed.

4.4.2 Specifying Architecture:

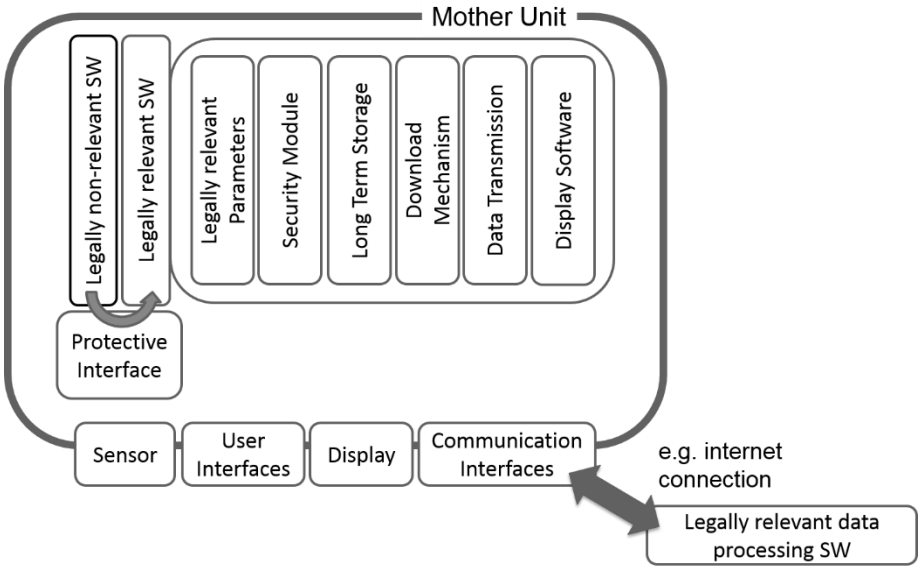

Figure 6: Reference architecture for the remote connection to the legally relevant software.

4.4.3 Boundary Conditions:

The measurement instrument is provided by the manufacturer as a whole for conformity assessment according to module B, i.e. technical structure containing the legally relevant data processing software is provided by the manufacturer. If parts of the instrument are provided by an external service provider, e.g. the technical structure containing the legally relevant data processing software, the role responsibilities laid down in the MID (2014/32/EU) do not change, i.e. the manufacturer who applies for the EU type examination stays responsible. The basic requirements regarding the type of instrument (P or U) are fulfilled individually by the mother unit and the separated part. Availability of all components, i.e. completeness of the measurement instrument is required and is guaranteed if MID's Annex I is fulfilled.

4.4.4 Specific Requirements:

- Identification of the external software unit and the corresponding mother unit must be possible (P2/U2).
- If there are several approved remote software components available, the identifiers of the remote component are legally relevant parameters to

guaranty that a change of the component provides an evidence of an intervention.

4.4.5 Requirements from WELMEC Guide 7.2 Covering this Architecture Configuration:

Fulfillment of the following requirements makes the process independent from a specific hardware the external part is located on.
Fulfillment of requirements by following extension T: Transmission of Measurement Data via Communication Networks.

Requirement	Description
T1	Completeness of transmitted data
T2	Protection against accidental or unintentional changes
T3	Integrity of Data
T4	Authenticity of transmitted data
T5	Confidentiality of keys,
T6	Handling of corrupted data
T7	Transmission delay
T8	Availability of transmission services

Table 4.4.5: Architecture relevant configuration

4.4.6 Requirements in the field for test of conformity and in-service control:

Requirement	Fulfillment is assumed
MID Annex I 8.2 “provide evidence of an intervention”	if P/U are fulfilled in combination with the required extensions.
MID Annex I 8.3 “software identification shall be easily provided”	if P/U are fulfilled in combination with the required extensions.
MID Annex I 7.2 “no unreasonable demands of the user”	if P/U are fulfilled in combination with the required extensions.

Table 4.4.6: Requirements for test of conformity and in-service control

4.4.7 Specific Attack Vectors to be Considered in the Risk Assessment:

Beside the general list of attack vectors provided in chapter 5 the following attack vectors should be considered for this specific architecture:

- **A_Tampering_and_Injection:** An attacker manipulates the communication between the remote processing unit and mother unit, harms the integrity of measurement data
- **A_Spoofing:** An attacker pretends to be one of the communication partners (either sender or receiver), harms authenticity of measurement data.

-

4.5 Remote Connection to the Legally Relevant Display

4.5.1 Specifying Description:

Measurement data are displayed externally. The display is “paired” with the mother unit, its location is identifiable, and each display provides a unique identifier. Pairing is the process by which two devices exchange device information so that a secure link can be established. The process of pairing devices is aimed at creating a shared secret between two devices according to P8/U8.
Please note that this Guide provides general models. Therefore, instrument specific requirements may apply to the legally relevant display that could be remotely accessed, e.g. MID Annex I 10.5.

4.5.2 Specifying Architecture:

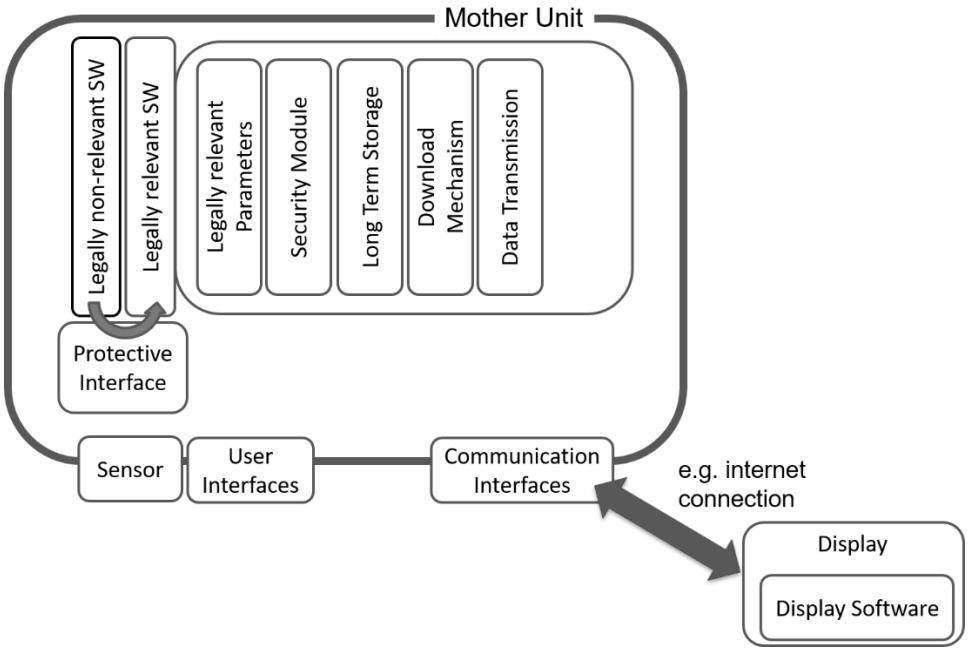

Figure 7: Reference architecture for the remote connection of the display

4.5.3 Boundary Conditions:

The measurement instrument is provided by the manufacturer as a whole for conformity assessment according to module B, i.e. the display is also provided by the manufacturer. If parts of the instrument are provided by an external service provider, e.g. the display, the role responsibilities laid down in the MID (2014/32/EU) do not change, i.e. the manufacturer who applies for the EU type examination stays responsible. Changes of the display hardware are tracked in a logbook. The basic requirements regarding the type of instrument (P or U) are fulfilled individually by the mother unit and the separated part. Availability of all components, i.e. completeness of the measurement instrument is required and is guaranteed if MID’s Annex I is

fulfilled, e.g.the utility meters must have a display that is accessible without tools to the consumer.

4.5.4 Specific Requirements:

- It is guaranteed that the remote component is paired with the mother unit according to P8/U8.
- If the external unit is replaced by a similar unit which was not paired with the mother unit the measuring Instrument should not function and re-verification with the similar external unit which was paired with the mother unit according to P8/U8 is required.
- Identification of the external unit and the corresponding mother unit must be possible.
- If there are several approved remote displays available, the identifiers of the remote displays are legally relevant parameters to guaranty that a change of the display provides an evidence of an intervention.

4.5.5 Requirements from WELMEC Guide 7.2 covering this Architecture configuration:

Fulfillment of requirements by following extension T: Transmission of Measurement Data via Communication networks.

Requirement	Description
T1	Completeness of transmitted data
T2	Protection against accidental or unintentional changes
T3	Integrity of Data
T4	Authenticity of transmitted data
T5	Confidentiality of keys,
T6	Handling of corrupted data
T7	Transmission delay
T8	Availability of transmission services

Table 4.5.5: Architecture relevant configuration

4.5.6 Requirements in the field for test of conformity and in-service control:

Requirement	Fulfillment is assumed, …
MID Annex I 8.2 “provide evidence of an intervention”	if P/U are fulfilled in combination with the required extensions.
MID Annex I 8.3 “software identification shall be easily provided”	if P/U are fulfilled in combination with the required extensions.
MID Annex I 7.2 “no unreasonable demands of the user”	if P/U are fulfilled in combination with the required extensions.

Table 4.5.6: Requirements for test of conformity and in-service control

An detailed acceptable solution could be found in WELMEC Guide 7.4 chapter 4.2

4.5.7 Specific Attack Vectors to be considered in the risk assessment:

Beside the general list of attack vectors provided in chapter 5 the following should be considered for this specific architecture:

- **A_Tampering_and_Injection:** An attacker manipulates the communication between the display and the mother unit, harms the integrity of measurement data.
- **A_Spoofing:** An attacker pretends to be one of the communication partners (either sender or receiver), harms authenticity of measurement data.

5 List of Attack Vectors used during Risk Assessment

Rapid technological development opens up new opportunities but also risks in radically changing how measuring instruments function in society. Therefore, more stringent demands for adequate risk assessment [5] when securing software can be found in the Directive (2014/32/EU) [2]. The risk analysis, which considers contemporary threats and guarantees comparability throughout Europe, would also increase the competence of all partners involved. A list of common attack vectors, i.e. a scheme how threats could be realized, is provided here to guaranty comparability of the analysis between the manufacturers and the Notified Bodies.

5.1 Common Attack Vectors

For an appropriate Risk Assessment procedure which is agreed upon in WELMEC Working Group 7 please refer to the documents provided by the WELMEC Library [5].

The following list of attack vectors is intentionally kept generic. Specific attack vectors are provided for each configuration.

- **A_PASSWORD:** An attacker retrieves the admin password by trying possible combinations.
- **A_CRYPTO_RET**: An attacker retrieves cryptographic material from the instrument.
- **A_BOOT:** An attacker manipulates the boot process of the device and subsequently installs malicious code.
- **A_RTC:** An attacker falsifies stored data by manipulating the device‘s real-time clock.
- **A_IF_DEBUG:** An attacker exploits debug interfaces that have not been deactivated.
- **A_INT_SERIAL:** An attacker exploits a vulnerability of a proprietary serial protocol.
- **A_INT_PLUGNPLAY:** An attacker exploits a vulnerability of a plug-and-play-interface such as USB.
- **A_WEB_XSS:** An attacker executes a cross-site scripting attack on a webserver.
- **A_WEB_DOS:** An attacker executes a denial-of-service attack on a webserver.
- **A_SW_REPLACE:** An attacker replaces the legally relevant software.
- **A_SW_RUNTIME_CONFIGFILES:** An attacker manipulates the software during the runtime by modifying unprotected configuration files.
- **A_SW_RUNTIME_INTERFACE:** An attacker manipulates the software during the runtime by exploiting vulnerabilities of external interfaces.
- **A_DATA_GEN:** An attacker generates false measurement data.
- **A_DATA_DEL**: An attacker deletes stored measurement data.

5.2 Additional Sources for Attack Vectors

Current attack vectors and new emerging threats may be identified by using any of the following resources. Manufacturers should be asked to consult well-known online databases when identifying new attack vectors.

- https://cve.mitre.org/
- https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-thematic-landscapes

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

For the interpretation of MID Articles and Annexes by MID-Software requirements please see WELMEC Guide 7.2 [1].

7 References and Literature

[1] WELMEC Guide 7.2 “Software”, https://www.welmec.org/documents/guides/72/

[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

[5] Esche M. and Thiel F.:
Software Risk Assessment for Measuring Instruments in Legal Metrology,
Federated Conference on Computer Science and Information Systems (FedCSIS), pages 1113 – 1123,
DOI: 10.15439/2015F127, ISSN 2300-5963, (2015)
https://fedcsis.org/proceedings/2015/pliks/127.pdf
Also available from the WELMEC Library:
https://www.welmec.org/welmec/library/

[6] Innovation, European Commission, https://ec.europa.eu/growth/industry/innovation_en

8 Revision History

No.	Date	Significant Changes
1	May 2019	Guide first issued.
2	May 2020	• Chapter 4.5 *Remote Connection to the Legally Relevant Display* was added. • In the introduction of chapter 4 and in the boundary conditions of 4.2.3 - 4.5.3. a remark was added, explaining the role responsibilities in case parts of the instrument are provided by an external service provider.

Table 8-1: Revision history