WELMEC 7.4
2019

WELMEC

European Cooperation in Legal Metrology

Exemplary Applications
of WELMEC Guide 7.2

WELMEC

European Cooperation in Legal Metrology

WELMEC is a co-operation 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 EC 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 : http://www.welmec.org

Exemplary Applications of WELMEC Guide 7.2

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. As the WELMEC guide 7.2 reflects the structure of MID, instrument specific requirements must be also considered. In this regard other WELMEC Working Groups may impose additional formal or technical requirements to the individual class of instruments.

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

This document provides technical guidance for the application of the Measuring Instruments Directive (MID).

It especially addresses software-equipped measuring instruments and is therefore applicable to a large variety of measuring instruments.

The guide at hand is intended to be used in conjunction with WELMEC guide 7.2. It provides exemplary acceptable solutions for specific architectures of instruments (see WELMEC guide 7.3 [4]) and indicates how these acceptable solutions fulfill the requirements laid down in WELMEC guide 7.2. In doing so, it also illustrates the requirements laid down WELMEC guide 7.2 on a technical level.

This guide only addresses acceptable solutions on the technical level and not on the architectural level (see WELMEC guide 7.3).

The level of detailedness is oriented on the needs of manufacturers of measuring instruments and of notified bodies (NB) which perform conformity assessments of measuring instruments according to module B.

By following the guide, a compliance with the software-related requirements of the MID can be assumed. It can be further assumed that all Notified Bodies accept this guide as a compliant interpretation of the MID with respect to software. To show how the requirements set up in this guide are related to the respective requirements in the MID, 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 general software-related terms used in this guide please refer to the terminology section of WELMEC guide 7.2 [1]. Definitions for all other terms are given below.

Mother Unit: Measuring instrument or part of a measuring 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.

2 How to use this guide

This guide describes specific configurations of measuring instruments as well as the hardware components and software modules of which the instruments consist. Each specific configuration, also referred to as an “acceptable solution”, is described individually. The guide also provides descriptions of associated requirements applicable to a specific configuration.

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 and addresses the functionality of selected modules of the concept. Secondly, specific technical realizations are discussed in chapter 4. For each of these, a list of applicable requirements is derived. Afterwards, it is demonstrated how the applicable requirements are fulfilled by the described realization. Chapter **Fehler! Verweisquelle konnte nicht gefunden werden.** lists the references as well as additional literature.

2.2 How to select the appropriate parts of the guide

When examining or developing a specific configuration of a measuring instrument, Notified Bodies and manufacturers alike are encouraged to refer to the chapter 4 for applicable examples. Not all possible configurations of an instrument can be presented in this guide. Therefore, readers should choose specific implementation details from different examples to suit their needs. Since all examples presented here are targeted at type U instruments of risk class C, compare with definitions in [1], most aspects of the acceptable solutions should be interchangeable or combinable.

3 Generalized Architecture of a Measuring Instrument

3.1 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 can be established which resembles a generalized architecture of a measurement instrument (s. figure 3-1).

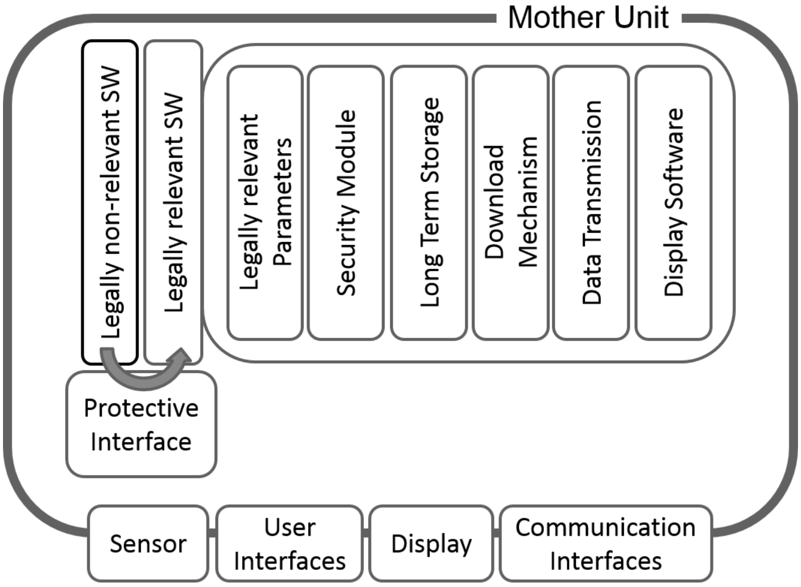

Figure 3-1: General Architecture resembling the refined modular structure of the WELMEC guide 7.2

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.

A detailed description of the generalized architecture is given in WELMEC guide 7.3 “Reference Architectures Based on WELMEC Guide 7.2” [4].

This generalized architecture is used here to identify exemplary configurations of measuring instruments for which acceptable solutions are presented. By following the generalized architecture, it is ensured that the presented exemplary applications do not contradict each other and provide a unified level of detailedness.

4 Exemplary Applications

Requirement U1 is always fulfilled by a complete documentation. U1 does not impose additional technical restrictions on the measuring instrument and is, therefore, not referred to in the examples below.

4.1 External Storage Unit Connected to a “Mother Unit”

4.1.1 Assumptions Regarding the “Mother Unit”

- The “mother unit” without external storage unit shall fulfill the requirements U1 to U9 of WELMEC guide 7.2, issue 2018.
- The “mother unit” can only be operated together with the external storage unit when the connection is physically sealed.

4.1.2 Applicable Requirements for the External Storage Unit

- “Mother unit” and storage unit shall together fulfill the requirements L1 to L8.
- In case the external storage unit has its own legally relevant software, it shall fulfill the requirements U2, U4, U5, U6, U7, U8 and U9, in combination with the “mother unit”. (U2: Requirement applies to the software identification of the external storage unit as well as to the software identification of “mother unit”.)
- In case the external storage unit has a user interface (e.g. an on/off switch), it shall fulfill U3, in combination with the “mother unit”.
- In case the external storage unit has its own legally relevant Software, Extensions D and S shall be checked if applicable.

4.1.3 Description of the Acceptable Solution

The following acceptable solution is specifically targeted on Type U instruments of risk class C. For a different basic configuration or a different risk class the acceptable solution needs to be adapted accordingly.

A multi-dimensional measuring instrument consists of two laser sensors that scan the two-dimensional profile of objects transported on a conveyor belt. The speed of the belt is measured by a third sensor. The sensors are physically sealed and connected to a central processor unit via cable on which a serial protocol is used for data communication. All cable connections are, likewise, physically protected against tampering. The processor unit is equipped with a real-time clock and a built-in display on which the calculated volume of the measured objects is indicated. Each new object is assigned a unique identifier and a time stamp by the processor unit. Once a measurement value (length, width, height of the smallest cube fitting the measured object) has been shown on the display together with the unique identifier and the time stamp, a CRC32 with a secret start vector is calculated and appended to the measurement dataset.

For long-term storage, an external storage unit, that contains legally relevant software, is connected to the processor unit via a serial communication link. The link is sealed when both components are put into use. The storage unit receives measurement datasets from the processor unit and acknowledges each received dataset. The storage unit provides the processor unit with feedback for each stored dataset, indicating if storing was successful or if an error (failure, storage full, memory corrupt, etc.) has occurred. The processor unit is also capable of providing the user with stored measurement results. She can search for datasets by entering a time stamp or a unique identifier via a keypad. Upon request through the serial protocol, the storage unit retrieves a measurement result specified by its unique identifier and sends it to the processor unit. The processor unit then checks the integrity of the dataset and shows the result to the user. Should the data be corrupt, a warning message is shown. The processor unit is capable of indicating the software version number of the storage unit (queried via the serial protocol) upon command.

4.1.4 Mapping between requirements and features of the acceptable solution

No.	Requirement	Acceptable Solution (Risk class C)
U2	Software identification	The software version number of the processor unit is shown upon startup. The software version of the storage unit can be retrieved via the serial protocol and is indicated in a special menu.
U3	Influence via the user interface	The user interface of the processor unit is designed so that no inadmissible influence on software, parameters or measurement data can occur. The storage unit has no user interface.
U4	Influence via communication interface	There are no open communication interfaces.
U5	Protection against accidental or unintentional changes	Once per day a CRC32 checksum with a secret start vector of the software and type-specific parameters of the processor unit is calculated and compared with a reference value. A similar process can be triggered for the external storage unit via the serial protocol. If either of the checks fails, a warning is shown to the user and no further measurements are possible. The instrument-specific parameters are calibration data for the distance and speed sensors. These are stored in a special flash memory within the processor unit. The integrity of the flash memory is checked once per day and after startup and reboot by means of a CRC32 checksum. If the check fails a warning is shown to the user and no further measurements are possible.
U6	Protection against intentional changes	See U5. In addition, the housing of all components and all communication connections are sealed. The calculated CRC32 of the legally relevant software and type-specific parameters is indicated on the integrated display upon command.
U7	Parameter protection	There are no commands to modify instrument-specific parameters through the interfaces.
U8	Presentation of measurement data.	The measurement data are presented by legally relevant software. There is no legally non-relevant software on the instrument.
U9	Influence of other software	There is no legally non-relevant software on the instrument.
L1	Completeness of measurement data stored	Stored datasets always comply with the format specified above. Incomplete datasets are discarded by the storage unit and an error message is sent to the processor unit.
L2	Protection against accidental or unintentional changes	Each dataset is transmitted together with its CRC32 checksum. The checksum is checked before retrieval. The result of the check is shown alongside the retrieved measurement result.
L3	Integrity of data	Each dataset is transmitted together with its CRC32 checksum. The checksum is checked before retrieval. The result of the check is shown alongside the retrieved measurement result.
L4	Authenticity of measurement data stored	Since storage unit and processor unit are connected by a sealed cable, no additional means of verifying the origin of the measurement data are necessary.
L5	Confidentiality of keys	The secret start vector used for checksum calculation of measurement data acts as a cryptographic key. It is stored in the executable code of the processor unit. There are no commands to read out or modify the start vector via the interfaces.
L6	Retrieval, verification, and indication of stored data	The software on the storage unit verifies each dataset before retrieval. The software on the processor unit displays the retrieved measurement results and informs the user about damaged or modified datasets.
L7	Automatic storing	Once a measurement is complete, its result is sent to the storage unit without intervention of the user. The next measurement can only be started if the storing operation has succeeded.
L8	Storage capacity and continuity	The storage unit has a sufficient capacity to store measurement results for two consecutive verification periods. Measurement results older than two verification periods are deleted automatically. Should memory become full nonetheless, a warning is issued to the user and no further measurements are possible

Table 4-1: Technical requirements and acceptable solutions description for the external storage unit.

4.2 External Display Unit Connected to a “Mother Unit”

4.2.1 Assumptions Regarding the “Mother Unit”

- The “mother unit” without external display unit shall fulfill the requirements U1, U2, U3 to U7, as well as U9 of WELMEC guide 7.2, issue 2018.
- To present the identification of the “mother unit” required in U2, an interface to the display unit exists.
- In case the display unit can be separated from the "mother unit" without breaking a seal, then the interface of the "mother unit", usually used for connecting the display unit, shall fulfill requirement U4. The data transfer between "mother unit" and display unit shall meet requirements T1 to T8.

4.2.2 Applicable Requirements for the Display Unit

- "Mother unit" and display unit shall together fulfill requirements U2 and U8.
- In case the external display unit has its own legally relevant software, it shall fulfill the requirements U2, U4, U5, U6, U7 and U9, in combination with the "mother unit". (U2: Software identification of the external display unit, in addition to software identification of the "mother unit").
- In case the external display unit has a user interface (e.g. an on/off switch), it shall fulfill U3, in combination with the "mother unit".
- Extensions D and S shall be checked if applicable.
- The data transfer between "mother unit" and display unit shall meet requirements T1 to T8.

4.2.3 Description of the Acceptable Solution

The following acceptable solution is specifically targeted on Type U instruments of risk class C. For a different basic configuration or a different risk class the acceptable solution needs to be adapted accordingly.

A gas meter[1] is equipped with three ultrasonic sensors to measure the volume of gas flowing through a pipe. The sensors are physically sealed and connected via cable to a central processor unit which uses a serial protocol for data communication. All cable connections are, likewise, physically protected against tampering. The total volume measured is stored in a dedicated, continuously increasing register. Once installed, the instrument measures the flow of gas without need for manual input. Setting of calibration parameters can only be done when the housing of the device is open. The processor unit has a single LED to indicate that a new error has been added to the log.

To show the current measurement result, a display can be connected to a serial port of the processor unit. Upon connection, all entries of the error log need to be scrolled through, by issuing commands (forward, backward) to the processor unit which replies accordingly, before measurement result is shown. The serial interfaces of both the processor unit and the display unit are protected by a software filter module that discards any incoming inadmissible commands. When connected, the processor unit supplies the current volume and time stamp to the display, which automatically indicates the result.

[1] Note: The gas meter described here is not suitable as a utility measuring instrument.

4.2.4 Mapping between requirements and features of the acceptable solution

No.	Requirement	Acceptable Solution (Risk class C)
U2	Software identification	The software version number of the display unit is shown upon startup. The software version of the processor unit is calculated and sent to the display when they are connected. The software version number of the processor unit is shown alongside the measurement result.
U3	Influence via the user interface	The processor unit does not have a user interface. The display unit's user interface consists of two buttons which can only trigger the two allowed commands "previous entry" and "next entry".
U4	Influence via communication interface	The serial communication interfaces of processor unit and display unit are protected by software filter modules which discard all inadmissible commands.
U5	Protection against accidental or unintentional changes	Once per day a CRC32 checksum of the software and type-specific parameters of the processor unit is calculated and compared with a reference value. A similar process is triggered for the external display unit when it is connected to the processor unit. If one of the checks fails, an entry is added to the error log and the LED on the outside of the processor unit is turned on. The LED is only turned off, once a user has scrolled through all the entries in the error log. The instrument-specific parameters are calibration data for the ultrasonic sensors. These are stored in a special flash memory within the processor unit. The integrity of the flash memory is checked once per day by means of a CRC32 checksum. If the check fails, an entry is likewise added to the error log.
U6	Protection against intentional changes	See U5. In addition, the serial communication interfaces fulfill U4.
U7	Parameter protection	There are no commands to modify instrument-specific parameters through the interfaces.
U8	Presentation of measurement data.	The measurement data are presented by legally relevant software. There is no legally non-relevant software on the instrument.
U9	Influence of other software	There is no legally non-relevant software on the instrument.
T1	Completeness of transmitted data	Datasets sent from the processor unit to the display unit always comply with the format specified above.
T2	Protection against accidental or unintentional changes	Each dataset is transmitted together with its CRC32 checksum. The checksum is checked by the display unit. The result of the check is shown alongside the retrieved measurement result.
T3	Integrity of data	Each dataset is transmitted together with its CRC32 checksum. The checksum is checked by the display unit. The result of the check is shown alongside the retrieved measurement result.
T4	Authenticity of transmitted data	Since the CRC used for protecting the transmitted data against modification is based on a secret start vector, it ensures authenticity of transmitted data, too.
T5	Confidentiality of keys	The secret start vector used for checksum calculation of measurement data acts as a cryptographic key. It is stored in the executable code of the processor unit and of the display unit. There are no commands to read out or modify the start vector via the user interface or the communication interface.
T6	Handling of corrupted data.	If the CRC check of the received data within the display unit fails, an error is shown alongside the (possibly garbled) measurement result.
T7	Transmission delay	If the display unit is connected to the processor unit, but measurement data is late, no measurement result is shown. The display will indicate a general error message, the measurement result within the processor unit is not affected by such a delay.
T8	Availability of transmission services	If the display unit is connected to the processor unit, but no measurement data is received, no measurement result is shown. The display will indicate a general error message, the measurement result within the processor unit is not affected by a broken communication link.

Table 4-2: Technical requirements and acceptable solutions description for the external display unit.

5 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

[4] Draft WELMEC guide 7.3 “Reference Architectures Based on WELMEC Guide 7.2”

6 Revision History

Issue	Date	Significant Changes
0	August 2018	Initial Version
1	October 2018	Revised version after Working Group 7 meeting. All references to parts and parts certificates were removed.
2		

Table 10-1: Revision history