A Project funded by the European Union and Implemented and led by CMI

WELMEC 7.2, 2015
Software Guide

Pavel Klenovský, Czech Metrology Institute

TWINNING

INTRODUCTION

- Guide WELMEC 7.2,2015 provides technical guidance for the application of the Measuring Instruments Directive (MID), especially for software-equipped measuring instruments.

- Guide WELMEC 7.2,2015 is addressed for notified body, but for programmers of measuring instruments too.

- Guide are related to the respective requirements in the MID, a cross reference has been included in this guide as an annex (Chapter 12, page 107)

- Free download: *www.welmec.org*

Structure of WELMEC 7.2, 2015

Basic configurations of measuring instruments

Type P

Built-for-purpose Measuring Instrument

Type U

Measuring Instruments using a Universal Computer

Requirements for IT configurations (Extensions)

L
Long-term Storage of Measurement Data

T
Transmission of Measurement Data via Communication Networks

S
SW Separation

D
Download of legally relevant SW

Instrument Specific Software Requirements (MID)

I1 – Water Meters

I2 – Gas Meters and Volume Conversion Devices

I3 – Active Electrical Energy Meters

I4 – Thermal Energy Meters

I5 – Measuring Systems for the Continuous and Dynamic Measurement of Quantities of Liquids Other than Water

I6 – Weighing Instruments (AWI), (WELMEC 2.3 is for NAWI)

I7 – Taximeters

Built-for-purpose Measuring Instrument (Type P)

- The embedded IT system (firmware).
- The SW is exclusively constructed for the measuring purpose.
- The user interface is dedicated to the measuring purpose.
- The SW environment is invariable and there are no internal or external means for programming or changing the SW in its embedded status.
- An operating system (OS) or subsystems of it may be included if:
  - All communication is under control of legally relevant SW.
  - It does not allow loading or changing programs, parameters or data or running programs.

Measuring Instruments using a Universal Computer (Type U)

- **HW Configuration:**
  - A modular general-purpose computer-based system.
    - Stand alone
    - Part of closed network (Ethernet) or open network (Internet)
  - The sensor is normally external to the computer unit and linked to it by a communication connection.
  - The user interface offers further functions, which are not under legal control, besides the operating mode for the measurement task.
  - Storage may be fixed (HDD), removable (USB), or remote.

- **SW Configuration:**
  - Operating system.
  - Other software applications may also reside on the system at the same time.

Selection of configuration of measuring instrument

Decision on Instrument Type		(P)
1	Is the entire application software constructed for the measuring purpose?	(Yes)
2	Are the requirements for the inclusion of an operating system or subsystems of it fulfilled?	(Yes)
3	Is the user prevented from accessing the operating system if it is possible to switch to an operating mode not subject to legal control?	(Yes)
4	Are the implemented programs and the software environment invariable (apart from updates)?	(Yes)
5	Are there any means for programming?	(No)

- Table is on page 103, WELMEC Guide 7.2,2015.
- If and only if all answers to the 5 questions can be given as in the (P) column, then the measuring instrument is Type P. In all other cases the measuring instrument is Type U.

Requirements for IT configurations (Extensions)

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

- Table is on page 103, WELMEC Guide 7.2,2015.

- Required extensions are optional not compulsory.

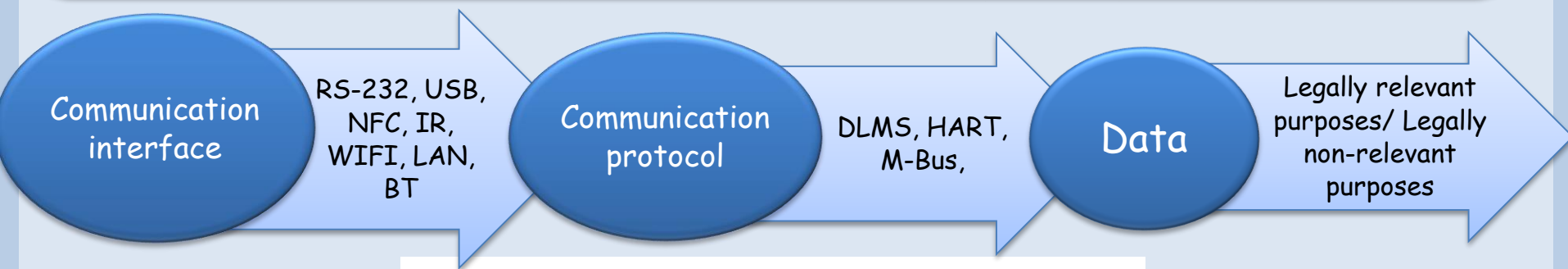# L: Long-term Storage of Measurement Data

- Long-term storage includes the time from when a measurement is physically completed to the point in time when all processes to be done by the legally relevant software are finished.

- It may also be applied to long-term storage of the data thereafter.

Type of storage	Using	Example
Integrated storage	Type: P,U	RAM, FLASH, EEPROM, HDD,
Storage for universal computer	Type U	Storage can be removed from the device or contents can be copied anywhere inside or outside the computer.
Removable or remote (external) storage	Type: P, U	USB stick, SD card, remote databases connected via network

T: Transmission of Measurement Data via Communication Networks

- The specific requirements of this section only apply if measurement data is transmitted via communication networks to a distant device where it is further processed and/or used for legally relevant purposes.
- This extension does not apply if there is no subsequent measurement data processing.
- Closed network: All devices in the network are subject to legal control
- Open network: Arbitrary participants (devices with arbitrary functions) can be connected to the network.

Communication interface → RS-232, USB, NFC, IR, WIFI, LAN, BT → Communication protocol → DLMS, HART, M-Bus, → Data → Legally relevant purposes/ Legally non-relevant purposes

SW of measuring instrument

Others processing of data

Border of validation SW in measuring instrument
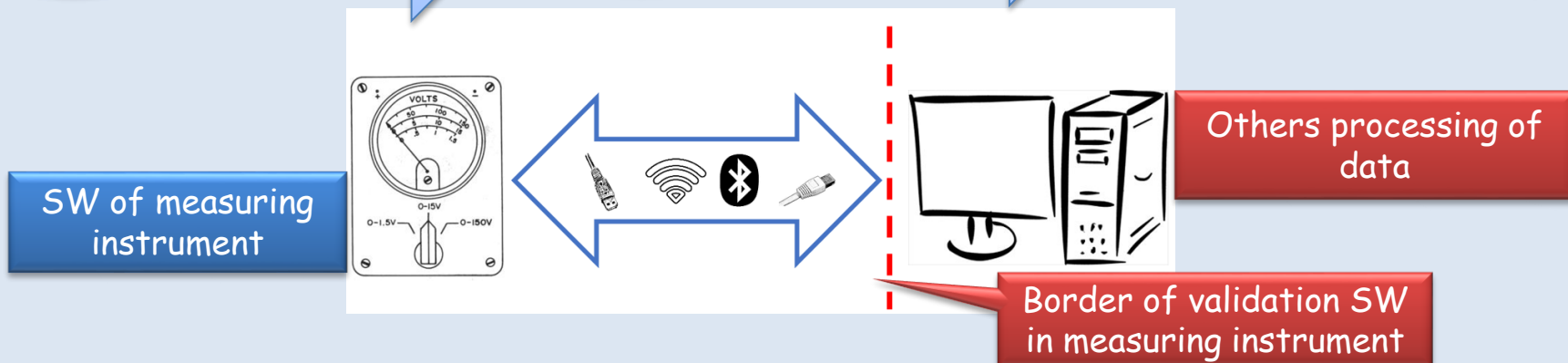
S: SW Separation

SW separation is an optional design method that allows to separate legally relevant SW (LRS) from legally non-relevant SW (LNRS).

Type SW	Content	Example
LRS	All Metrologic part, calculation of measurement values or have an impact on it, functions such as displaying data, data security, data storage, software identification, performing software download, data transmission or storing, verifying received or stored data	Data on LCD, Display of Identification SW, transmission of data,
LNRS	Others part of SW which has not influence to LRS	language menu, backlight of LCD,

Type of separation SW	Description	Example
Low level	SW separation is realized independently from the operating system	1 MCU → 2 SW
High level	The software modules to be separated are realized as independent objects in terms of the operating system	2 MCU → 2 SW

D: Download of Legally Relevant SW

This extension shall be used if instruments are equipped with facilities for a SW download without breaking a seal.

The entire SW to be downloaded may be legally relevant or there may be a separation between legally relevant and legally non-relevant SW. Legally non-relevant SW can be possible downloaded only if is applied extension S (separation SW).

Before downloaded new legally relevant SW, it must firstly be approved. Then the downloading and distribution of new version of legally relevant SW is permitted.

Definition of Risk Classes

Risk Class	SW Protection	SW Examination	SW Conformity
A	Low	Low	Low
B	Middle	Middle	Low
C	Middle	Middle	Middle
D	High	Middle	Middle
E	High	High	Middle
F	High	High	High

- Definition of Risk class is on pages 14 to 16 of WELMEC Guide 7.2, 2015.
- Most used are Risk Classes B,C,D.
- Risk Class E is control of Source Code.
- Risk Classes A and F are actually not using but are open for future.
- Definition Class Risk for measuring instruments under MID are in chapter 10 of WELMEC Guide 7.2, 2015.

The definition of requirement

Risk Class B	Risk Class C	Risk Class D

P4: Influence via communication interface

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

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

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

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

Validation Guidance:

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

Functional checks:

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

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

Additions for Risk Classes E

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

Source code of the legally relevant software.

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

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

- Risk Classes
- Name and description of requirement
- Specifying Notes
- Required Documentation
- Validation Guidance
- Example of an Acceptable Solution
- Risk Class E
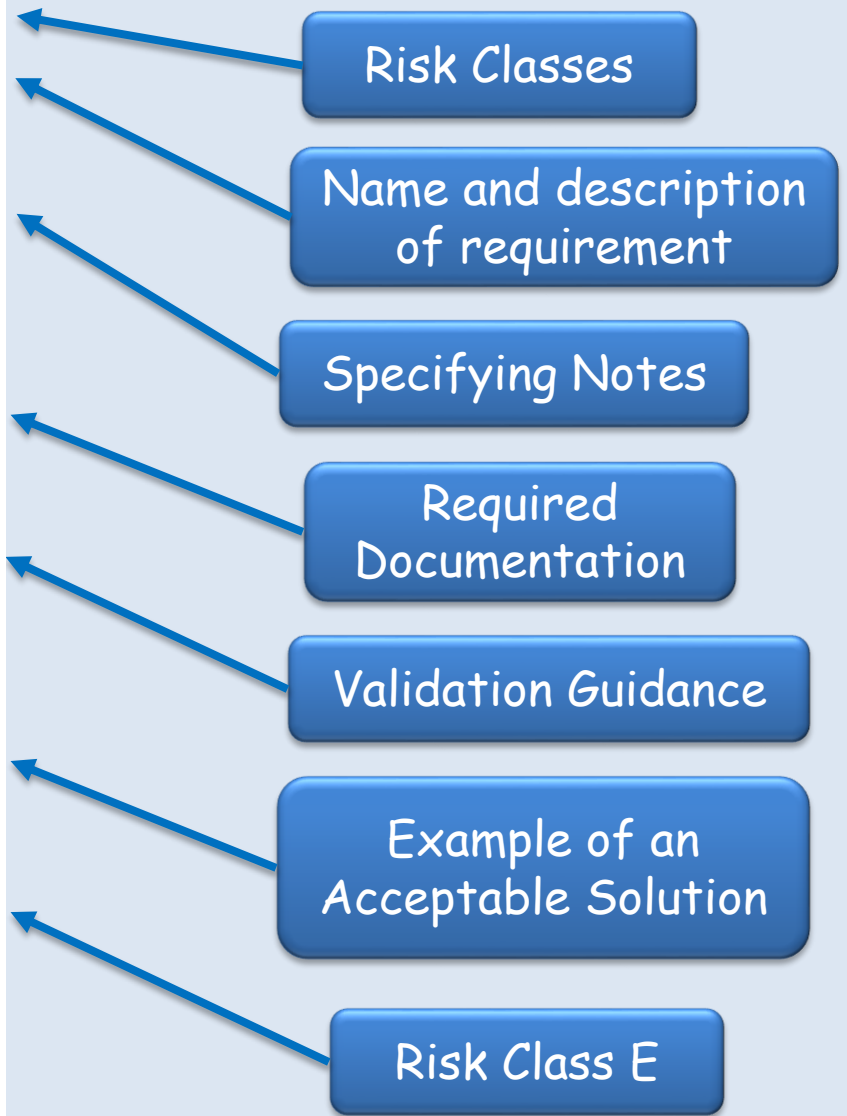
Basic Requirements for Type P

P1	Documentation	Description of SW
P2	SW Identification	Version of SW (01.02)
P3	Influence via user interface	keyboard, button/s, LCD
P4	Influence via communication interface	USB, IR, RS-232, RS-485, WIFI,BT,NFC
P5	Protection against accidental or unintentional changes	SW detect changes caused by physical effects (electromagnetic interference, temperature, vibration, etc.), inadequate manipulation with user interface
P6	Protection against intentional changes	Unauthorized manipulation, protection of measuring data, memories, registers
P7	Parameter protection	Protection of calibration parameters, specific parameters, passwords, event logger

P1 Documentation

- Brief description of measuring instrument.

- Description of HW part of measuring instrument,
  (Photo of PCB with description).

- Manual of the measuring instrument.

- Description of legally relevant SW.
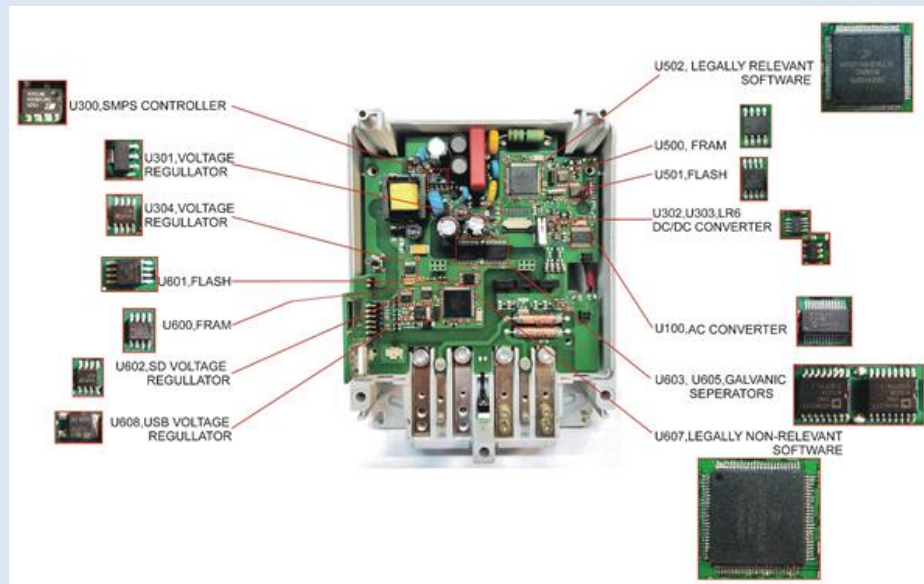
P2 SW Identification

- Identification of SW: numbers, characters, alphabet, their combinations or strings.
  - 01.01 , V01, v01.03.02,
- Identification of the legally relevant SW should be easily presented without requiring an additional tool.
- Identification should be covered by securing means.
- Clear description of the visualization of identification of the legally relevant SW
- Description of structure Identification
  - *01.02: 01 (Major), 02 (Minor)*

P3 Influence via user interface

- User interface: Everything what is inextricably connected with the measuring instrument
  - LCD, button/s, keyboard etc.

- Documentation should contain description of all commands and their effect on legally relevant SW, device-specific parameters and measurement data.

- Interface should have not inadmissibly influence the legally relevant SW.

P3 Influence via user interface

- Example of description for commands user interface
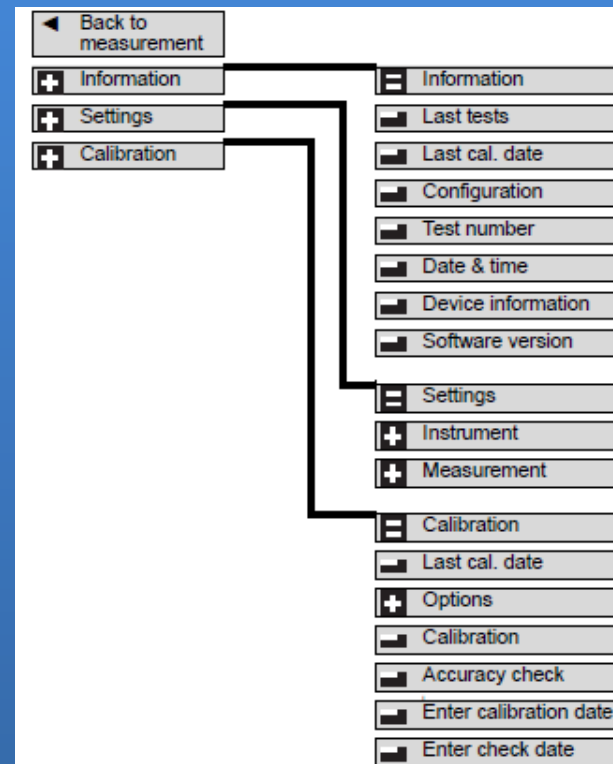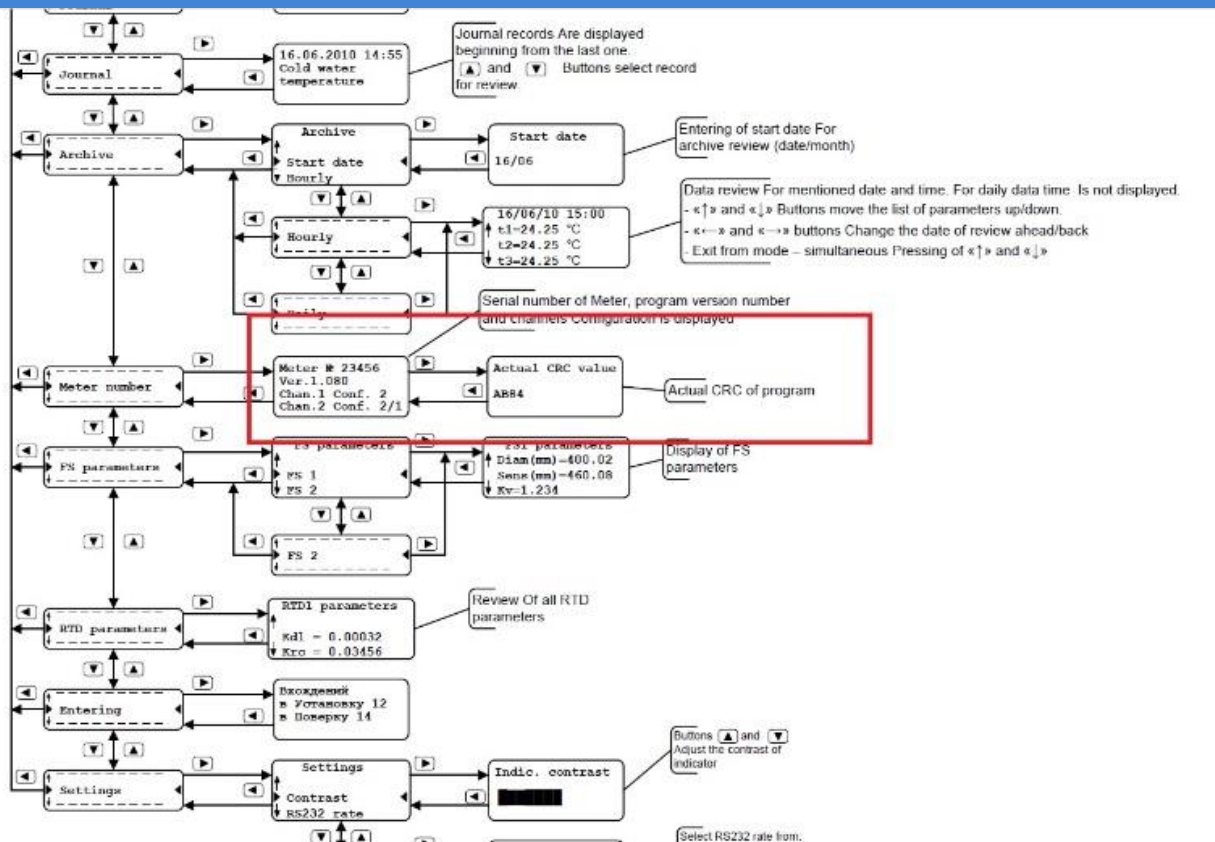
P4 Influence via communication interface

- Communication: interfaces, protocols, application SW

- Documentation should contain description of all commands and their effect on legally relevant SW, device-specific parameters and measurement data.

- Check of un-allowed commands.

P4 Influence via communication interface

P5&P6 Protection against changes

- **P5 Protection against accidental or unintentional changes**
  - Warning before deleting measurement data.
  - Reset of totalizers.

- **P6 Protection against intentional changes**
  - Securing against unauthorized exchange of the memory that contains the software or legally relevant parts.
  - Using checksum or alternative methods (message digest):
    - Should cover the legally relevant SW only.
    - Should be recalculated and compared with the nominal value periodically.
    - Should be possible to show it for inspection purposes.

P5&P6 Protection against changes

- A CRC (Cyclic Redundancy Check) **checksum** is a small-sized information derived from a block of digital data for the purpose of detecting errors.
  - **CRC-16 (7DFB)**
  - **CRC-32 (82F63B78)**
  - **CRC-64 (42F0E1EBA9EA3693)**

- A cryptographic **hA cryptographic hash** function is a **hash** function which takes an input (or 'message') and returns a fixed-size alphanumeric string. The string is called the '**hash** value', 'message digest', 'digital fingerprint', 'digest' or 'checksum').

- **Hash function** allows one to easily verify that some input data maps belong to a given hash value, if the input data are unknown it is deliberately difficult to reconstruct it (or equivalent alternatives) by knowing the stored hash value (SHA – Secure Hash Algorithm – issued by NIST USA). **MD5 (128 bit Hash) 32 characters in HEXA code.**
  - **SHA-1 (160 bit Hash) 40 characters in HEXA code.**
  - **SHA-256 (256 bit Hash) 64 characters in HEXA code.**

P5&P6 Protection against changes

P5&P6 Protection against changes

MD5 on LCD

P7 Parameter protection

- **Specific parameters:**
  - Calibration constants.
  - Important parameters before start in real field.
  - Securing parameters.
  - Secure of totalizers.
  - Passwords and rights.

- **Protection of specific parameters:**
  - Not possible change without break seal.
  - Protected by checksum.
  - HW jumper under seal.
  - Securing by passwords.
  - If are used passwords, then should be applied event logger, which is not possible deleted or change without break seal.

Basic Requirements for Type U

U1	Documentation	Description of SW
U2	SW Identification	Version of SW, libraries and other files related with legally relevant SW
U3	Influence via user interface	Commands entered via user interface
U4	Influence via communication interface	Commands input via communication interface
U5	Protection against accidental or unintentional changes	SW detect changes caused by physical effects (electromagnetic interference, temperature, vibration, etc.), inadequate manipulation with user interface
U6	Protection against intentional changes	Unauthorized manipulation, protect of measuring data, memories, operation system
U7	Parameter protection	Protect of all device-specific parameters against unauthorized modification
U8	Presentation of measurement data	Authenticity of the measurement data
U9	Influence of other SW	Separation SW

U1 Documentation

- Brief description of legally relevant functions, meaning of data etc.

- Description of HW system (*topology block diagram, type of PC, type of network*).

- Manual of measuring instrument.

- Overview of the configuration of the operating system, security aspects of the operating system (*protection, user accounts, privileges*).
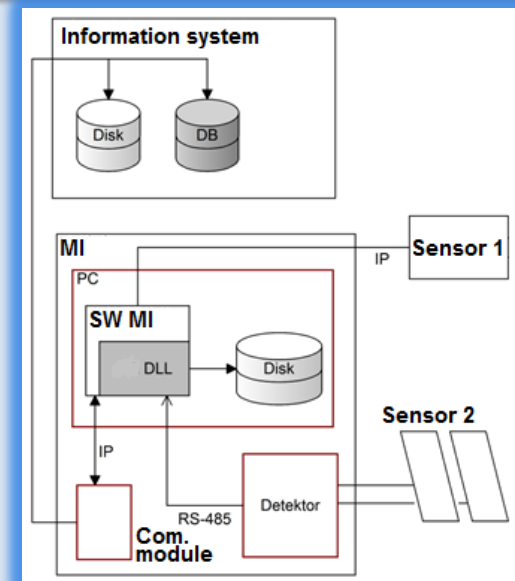
U2 SW Identification

- The legally relevant identifier(s) shall be unique for each legally relevant software an instrument is equipped with.

- The legally relevant identifiers shall be easily presented without requiring an additional tool.

- Identification shall include drivers and components of operating systems that have been modified or specifically programmed for a legally relevant task. Standard components used unchanged may be excluded from identification.

- If the legally relevant functions and the account of the measuring task are protected by a specific configuration of the operating system, the relevant configuration files shall have its own identifier.

```
Start-up time (UTC): 2017-02-24 15:13:24
ME dll file version: 1.1
ME dll file calculated hash: 8ED7113B5BB9701C5A421EE0274AE0F9
ME dll file given hash: 8ED7113B5BB9701C5A421EE0274AE0F9
ME dll is valid.
```

U3 Influence via user interface

- Description of commands and their effect on legally relevant software, device-specific parameters and measurement.

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

- Description of how the legally relevant software, device-specific parameters and measurement data are protected from functions of the operating system offered to the user.

- (Risk Class D) Description of protections means against other inputs including functions of the operating system offered to the user.

U4 Influence via communication interface

- Description of commands and their effect on legally relevant software, device-specific parameters and measurement data.

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

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

U5&U6 Protection against changes

- Description of measures that have been taken to detect and protect the legally relevant software and device-specific parameters from unintentional changes.
- Description of the checksum method and of reactions in case of non-matching.
- Description of how and where the nominal checksum(s), or the alternative indications of change status, are deposited.
- Description of methods how the mass storages are protected from exchange, if applicable.
- Description of used securing features of operating system.
- Description of how the checksum or an alternative indication are presented.
- (Risk Class D) In general, a universal computer is only usable if additional hardware can be used to support securing.

```
Start-up time (UTC): 2017-02-24 15:13:24
ME dll file version: 1.1
ME dll file calculated hash: 8ED7113B5BB9701C5A421EE0274AE0F9
ME dll file given hash: 8ED7113B5BB9701C5A421EE0274AE0F9
ME dll is valid.
```

Parameter protection & Presentation of measurement data

- **U7 Parameter protection:**
  - Device specific parameters could be manipulated using simple tools on universal computers, they shall be stored in secured HW.
  - The documentation shall describe the device-specific parameters, whether they may be set and how they are set and how they are secured.
  - Check that all relevant parameters are secured.

- **U8 Presentation of measurement data:**
  - Describe how authenticity of the measurement data is guaranteed.
  - Check that presented measurement data is generated and performed by legally relevant software.
  - Check through visual control if the presentation of measurement data is easily distinguishable from other information that may also be presented.

Requirements for Extension L

L1	Completeness of measurement data stored	List and description of data stored
L2	Protection against accidental or unintentional changes	Similarly to P5
L3	Integrity of data	Similarly to P6
L4	Authenticity of measurement data stored	Measurement data stored should be possible correctly assign to appropriate measurement
L5	Confidentiality of keys	Keys should be kept secret and protect against compromise (unveil)
L6	Retrieval, verification and indication of stored data	Description functions of SW for displaying measurement data stored
L7	Automatic storing	Measurement data should be stored automatically
L8	Storage capacity and continuity	Description capacity of storage and management of storing measurement data

Requirements for Extension T

T1	Completeness of transmitted data	List and description of transmitted data
T2	Protection against accidental or unintentional changes	Similarly to P5
T3	Integrity of data	Similarly to P6
T4	Authenticity of transmitted data	Transmitted data should be possible correctly assign to appropriate measurement
T5	Confidentiality of keys	Keys should be kept secret and protect against compromise (unveil)
T6	Handling of corrupted data	Description of the detection of corrupted data.
T7	Transmission delay	Description of the concept, how measurement is protected against transmission delay.
T8	Availability of transmission services	Description of protection measures against transmission interruption or other failures.

Requirements for Extension L & T

Requirements for Extension S

S1	Realization of SW separation	Naming of all components that belong to the legally relevant SW
S2	Mixed identification	Distinguish between information from LRS and LNRS
S3	Protective SW interface	Securing of communication between LRS and LNRS
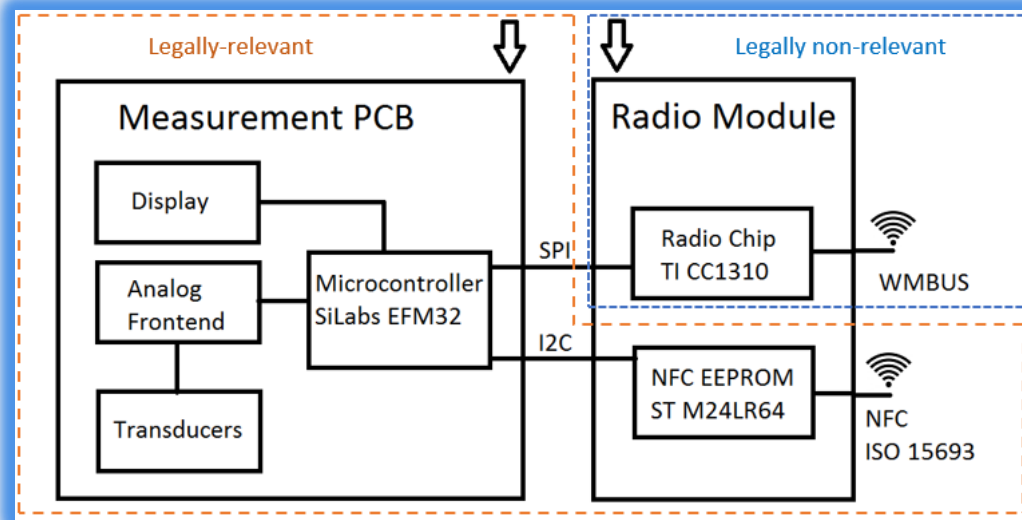
Requirements for Extension D

D1	Download mechanism	Description of method for download process
D2	Authentication of transmitted SW	Description of method for authenticity for transmitted SW
D3	Integrity of downloaded SW	Description of means for protect against not allowed changes
D4	Traceability of legally relevant SW download	Event logger for downloaded of LRS

Requirement for SW of specific Measuring Instruments

I1	Water Meters	Type P – Risk Class C
I2	Gas Meters and Volume Conversion Devices	
I3	Active Electrical Energy Meters	
I4	Thermal Energy Meters	
I5	Measuring Systems for the Continuous and Dynamic Measurement of Quantitates of Liquids other than Water	Risk Class C
I6	Weighing Instruments (AWI)	Type P: Risk Class B (except totalizers) Type U + totalizers Type P+U: Risk C
I7	Taximeters	Type P: Risk Class C Type U: Risk Class D
I8	*Material Measures*	Without definition of Risk Class
I9	*Dimensional Measuring Instruments*	Type P: Risk Class B Type U: Risk Class C
I10	*Exhaust Gas Analyzers*	

Requirement for SW of specific Measuring Instruments

Fault Recovery	I1, I2, I3, I4, I6
Back-up facilities	I1, I2, I3, I4, I6, I7
Inhibit resetting of cumulative measurement values	I1, I2, I3, I4
Dynamic behavior	I1, I2, I3, I4
Internal resolution, suitability of the indication	I2, I3
Battery lifetime	I2
Electronic volume converters	I2
Test element	I2
Imprinted Software Identifier	I1, I2, I3, I4, I5

Twinning Project "Strengthening the capacities of the Bureau of Metrology for internal market integration"
Twinning ref. MK 12 IPA EC 01 16 TWL

A Project funded by the European Union and Implemented and led by CMI

pklenovsky@cmi.cz