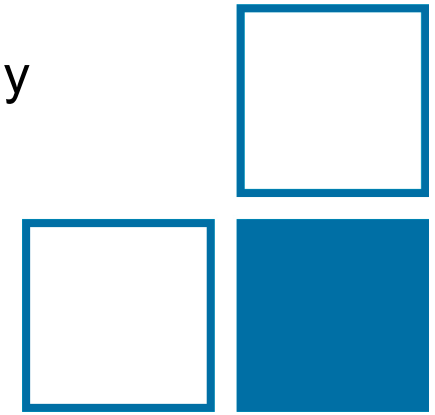
Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Nationales Metrologieinstitut

Part I: The Common Ground

Essential requirements and their technical interpretation.

IT Requirements for module B

3rd Workshop
Software and ICT related Challenges in Legal Metrology



21.06.2017

Federico Grasso Toro
PTB WG 8.51 - Metrological Software

Overview

- Purpose and structure of WELMEC 7.2, 2015: Software Guide.
- Usage of WELMEC 7.2, 2015: Software Guide.
- Example of WELMEC 7.2, 2015: Software Guide:
  - Basic requirements for universal computers (**Type-U**)
  - Requirements for special extensions (**L, T, S** and **D**)

WELMEC Guides

- WELMEC (European Cooperation in Legal Metrology) publishes guides to help harmonize conformity assessment within the EU and European Free Trade Association (EFTA).

- IT Requirements for Measuring Instruments, regulated in the *Measuring Instruments Directive* (MID) are detailed in WELMEC Guide 7.2.

- Currently, **WELMEC 7.2, 2015: Software Guide** is in force.

  (http://www.welmec.org/fileadmin/user_files/publications/WG_07/Guide_7.2_2015__Software.pdf)

- For many instruments subject to German National Legislation, Guide 7.2 has been recognized as describing the **state-of-the-art**.

WELMEC 7.2, 2015: Software Guide

- The Guide is based on the “Software Requirements and Validation Guide”, Version 1.00, 29 October 2004, developed and delivered by the European Growth Network “MID-Software”.

- The Network was supported from January 2002 to December 2004 by the EU commission, under the contract number **G7RT-CT-2001-05064**.

- The WELMEC 7.2, 2015 is purely advisory. It does not itself impose any restrictions or additional technical requirements, beyond those contained in MID.

WELMEC 7.2, 2015: Software Guide

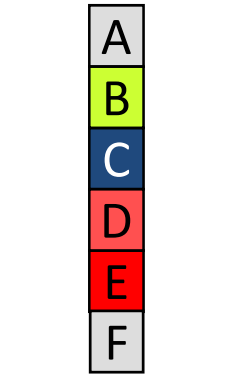
- Alternative approaches may be acceptable, but the guidance provided in this document represents the considered view of WELMEC as to a good practice to be followed.

- Although the Guide is oriented on instruments included in the regulations of the MID, the results are of a more general nature and may be applied beyond.

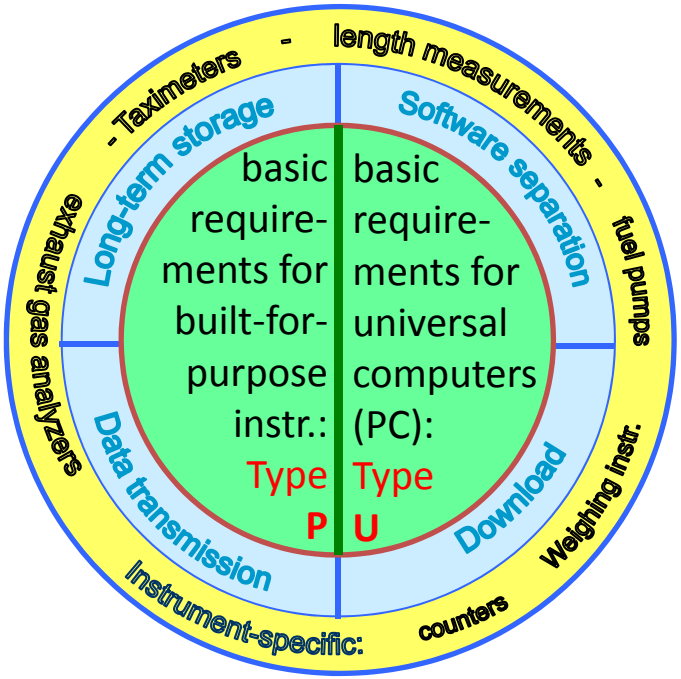
- The version 2015 considers the latest experience gained from the applications of the Guide.

WELMEC 7.2, 2015: Software Guide

Structure of the guide:

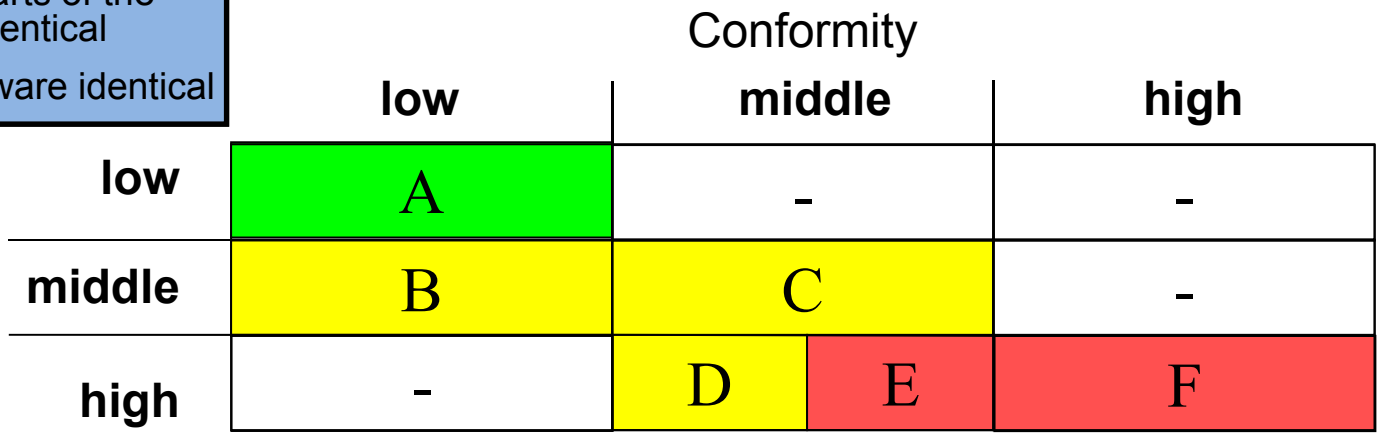


Risk Classes



WELMEC 7.2, 2015: Definition of Risk Classes

Conformity	
low:	functions identical
middle:	selected parts of the software identical
high:	whole software identical



Protection against manipulation	
low:	means no specific protection means
middle:	means against use of wide-spread simple tools (text editors, etc.)
high:	means against use of sophisticated software tools (debuggers, etc.)

Risk Classes A - F

Examination level

low

middle

high

Examination	
low:	functional test of the instrument
middle:	examination based on functional description of the software (documentation + selected practical tests)
high:	examination based on the source code

WELMEC 7.2, 2015: Assignments to Risk Class B

Conformity:

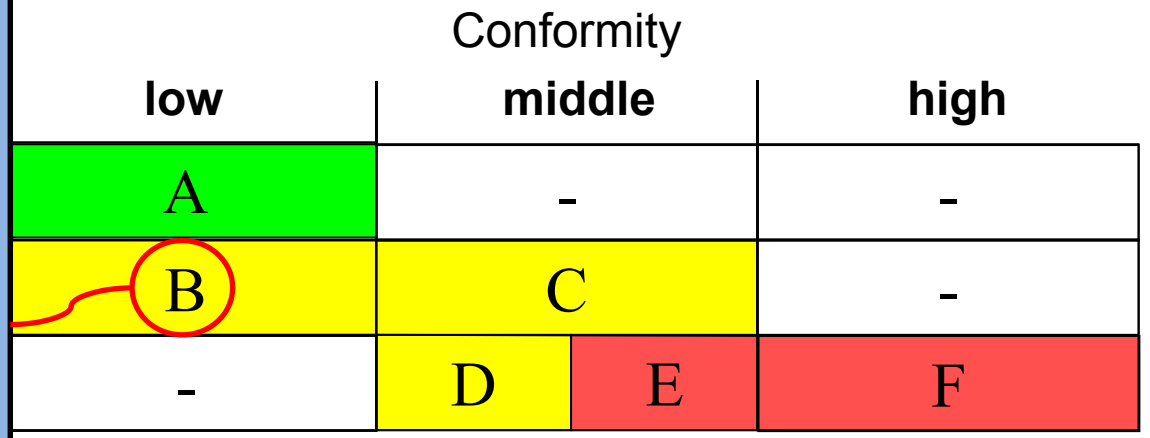
low: functions identical

Protection against manipulation:

middle: means against use of wide-spread simple tools

Examination:

middle: examination based on functional description of the software (documentation + selected practical tests)



Risk Classes A - F

Examination level

low

middle

high

Examples

- Liquids other than water (P)
- AWI (P, except totalisers)
- Dimensional instruments (P)
- Exhaust gas analysers (P)

WELMEC 7.2, 2015: Assignments to Risk Class C

Conformity:

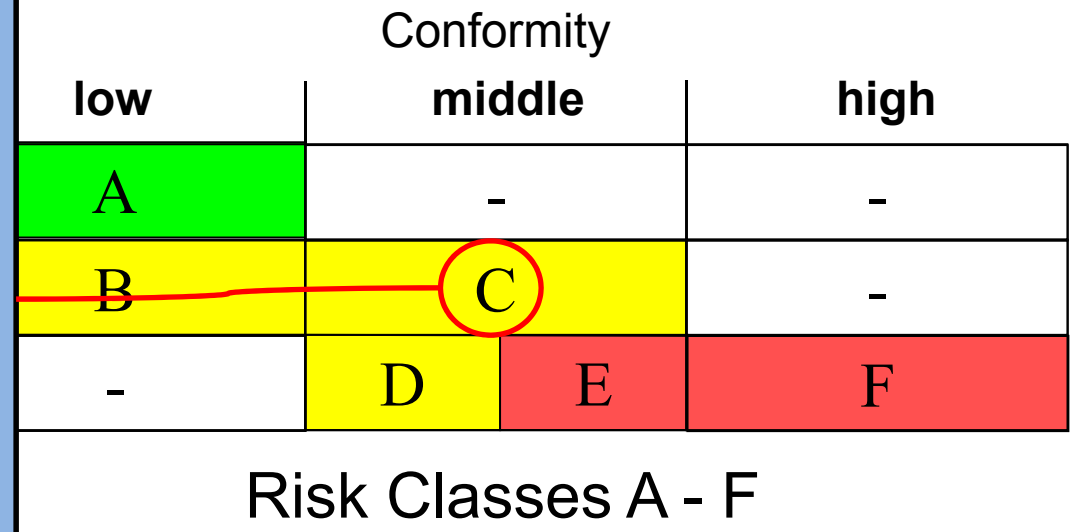
middle: selected parts of the software identical

Protection against manipulation:

middle: means against use of wide-spread simple tools

Examination:

middle: examination based on functional description of the software (documentation + selected practical tests)



Risk Classes A - F

Examination level

low

middle

high

Examples

- Utility meters (P)
- Liquids other than water (U) prelim.
- AWI (totalisers P and all of type U)
- Taximeters (P)
- Dimensional instruments (U)
- Exhaust analysers (U)

WELMEC 7.2, 2015: Assignments to Risk Class D

Conformity:

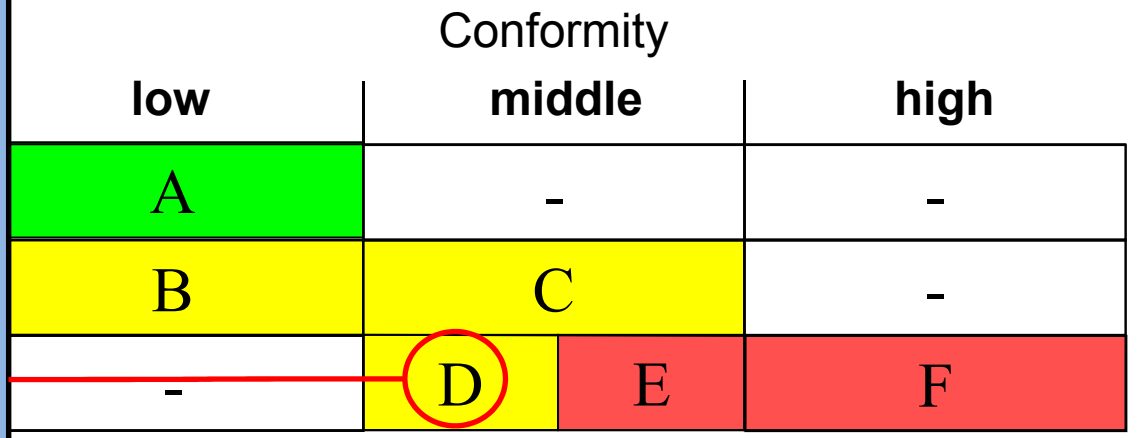
middle: selected parts of the software identical

Protection against manipulation:

high: means against use of sophisticated software tools (debuggers, etc.)

Examination:

middle: examination based on functional description of the software (documentation + selected practical tests)



Risk Classes A - F

Examination level

low

middle

high

Examples

- Liquids other than water (U), special applications, prelim.
- Taximeters (U)

WELMEC 7.2, 2015: Assignments to Risk Class F

Conformity:

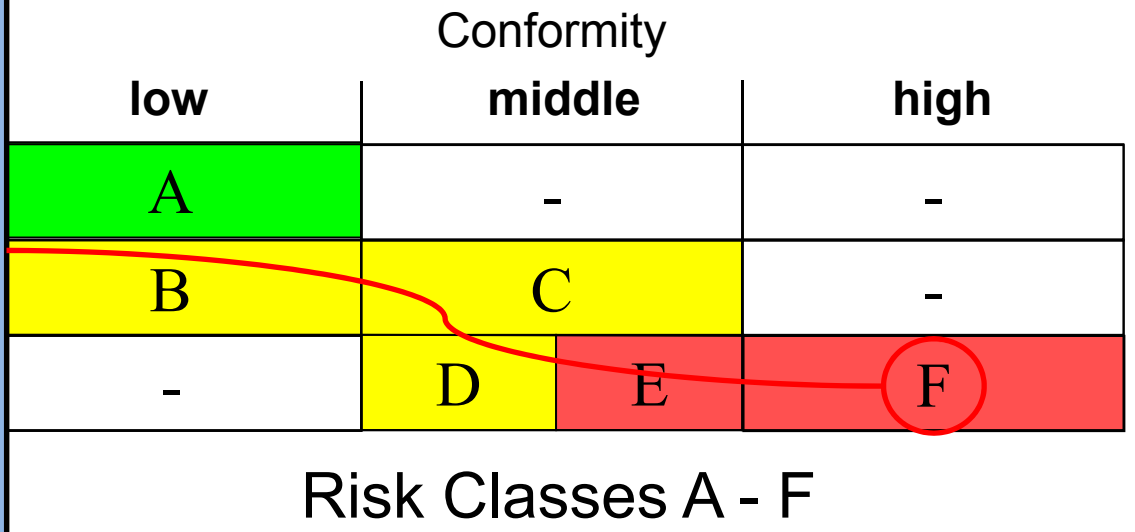
middle: selected parts of the software identical

Protection against manipulation:

high: means against use of sophisticated software tools (debuggers, etc.)

Examination:

high: examination based on the source code



Examination level

- **low**
- **middle**
- **high**

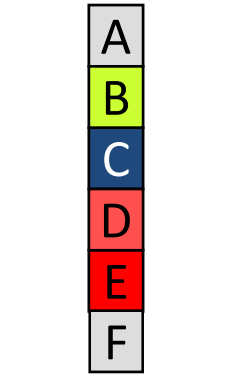
Examples (national)

- Speed Measuring, *Traffic-Robots* (U).

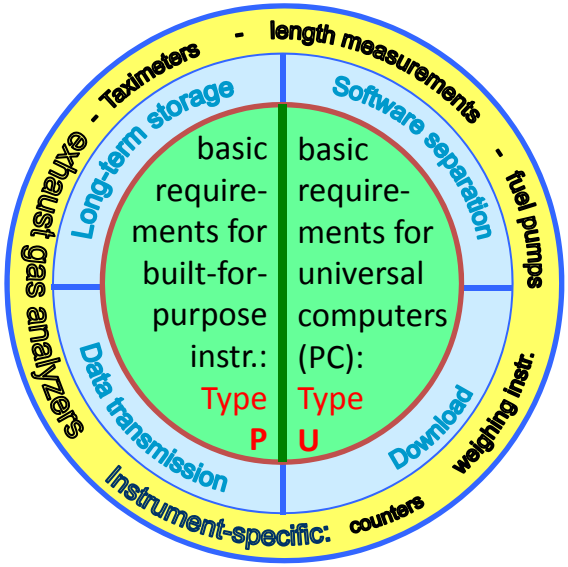
Usage of WELMEC 7.2, 2015:

Choosing the correct set of requirements

- The choice of requirements depends on:
  - the **Risk Class** (Class A-B-C-D-E-F).
  - the **Basic Configuration** (Type U, Type P).
  - the **Extensions** to the basic configuration present in the device.



Risk Classes



Usage of WELMEC 7.2, 2015:

Choosing the correct set of requirements

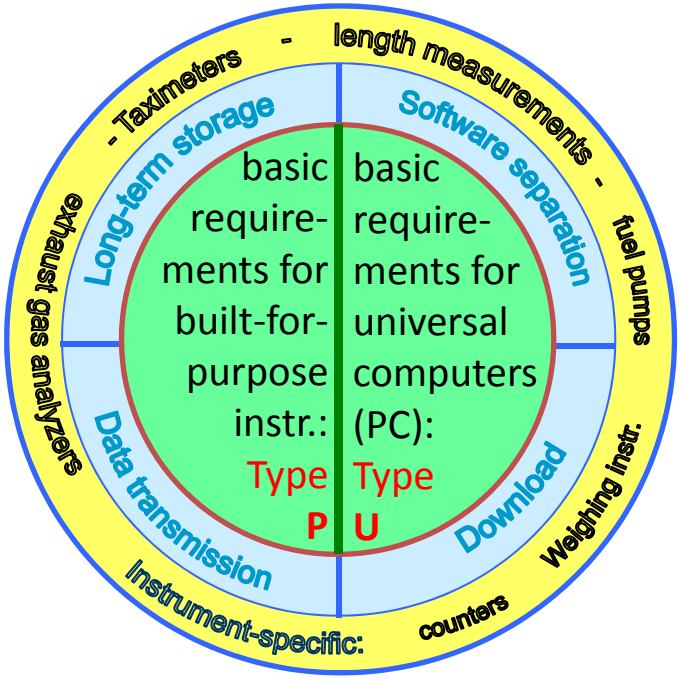
Risk Classes - Summary

Risk class	Software protection	Software examination	Software 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

Usage of WELMEC 7.2, 2015:

Choosing the correct set of requirements

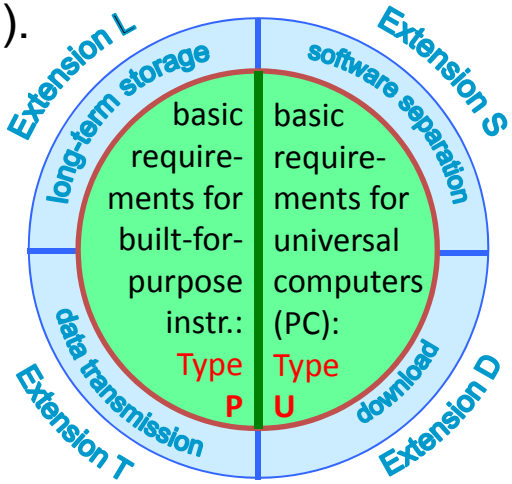
Basic Configuration - Summary



Usage of WELMEC 7.2, 2015:

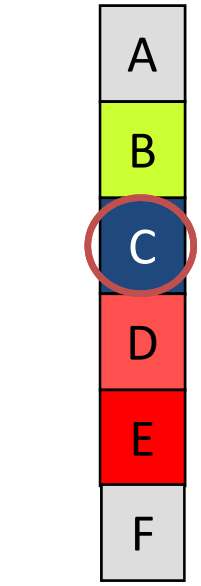
Choosing the correct set of requirements

- Extensions : classified into four categories:
  - Long-term storage (Extension **L**).
  - Transmission of measurement data (Extension **T**).
  - Software separation (Extension **S**).
  - Download of legally relevant software (Extension **D**).

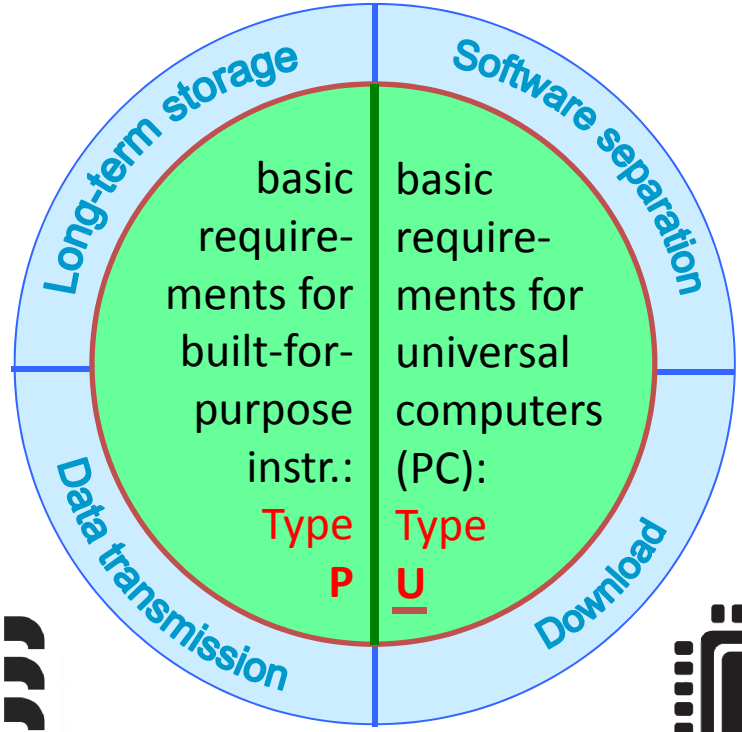


WELMEC 7.2, 2015: Software Guide

Example: Dimensional Instrument



Risk Classes



Basic Requirements for Type U Instruments

- **U1: Documentation**
- **U2: Software identification**
  - The legally relevant software shall be clearly identified. An identification of the software shall be inextricably linked to the software itself. It shall be determined and presented on command or during operation.

  e.g. legally relevant software identifiers; a string added by a version number (class C-D)
- **U3: Influence via user interfaces**
  - Commands entered via the user interface shall not inadmissibly influence legally relevant software, device-specific parameters and measurement data.

  e.g. a module filters all incoming commands, the user has only limited access rights (class B-D)

Basic Requirements for Type U Instruments

- **U4: Influence via communication interfaces**
  - Commands entered via non-sealed communication interfaces of the device shall not inadmissibly influence the legally relevant software and measurement data.

  e.g. a module receives and interprets all data entered via the interface, access to the operating system is limited (class B-D)

- **U5: Protection against accidental or unintentional changes**
  - Legally relevant software and device-specific parameters shall be protected against accidental or unintentional changes.

  e.g. utilization of protection and privacy mechanisms of the operatic system, hashing of relevant parts of the code, limited access rights (class B-D)

Basic Requirements for Type U Instruments

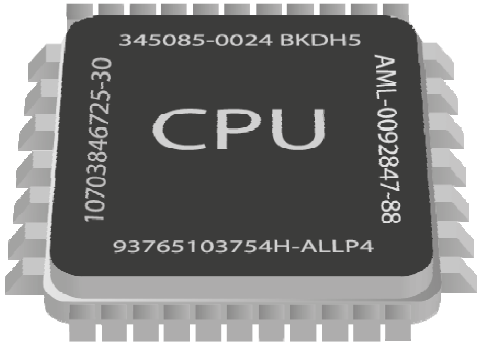
- **U6: Protection against intentional changes**
  - Legally relevant software and measurement data shall be secured against inadmissible modification.

  e.g. protection of programs and data by means of checksums or hashes (class B-C)
- **U7: Parameter protection**
  - Legally relevant parameters shall be secured against unauthorised modification.

  e.g. device-specific parameters are stored on a separate storage unit, which is sealed against removing (class B-D)
- **U8: Presentation of measurement data**
  - Means shall be employed to ensure the authenticity of the legally relevant software. Also the authenticity of the presented results shall be guaranteed.

  e.g. the software periodically checks whether the indication window is correctly displayed, sensor data are encrypted and can only be decrypted by the legally relevant software

Basic Requirements for Type U Instruments

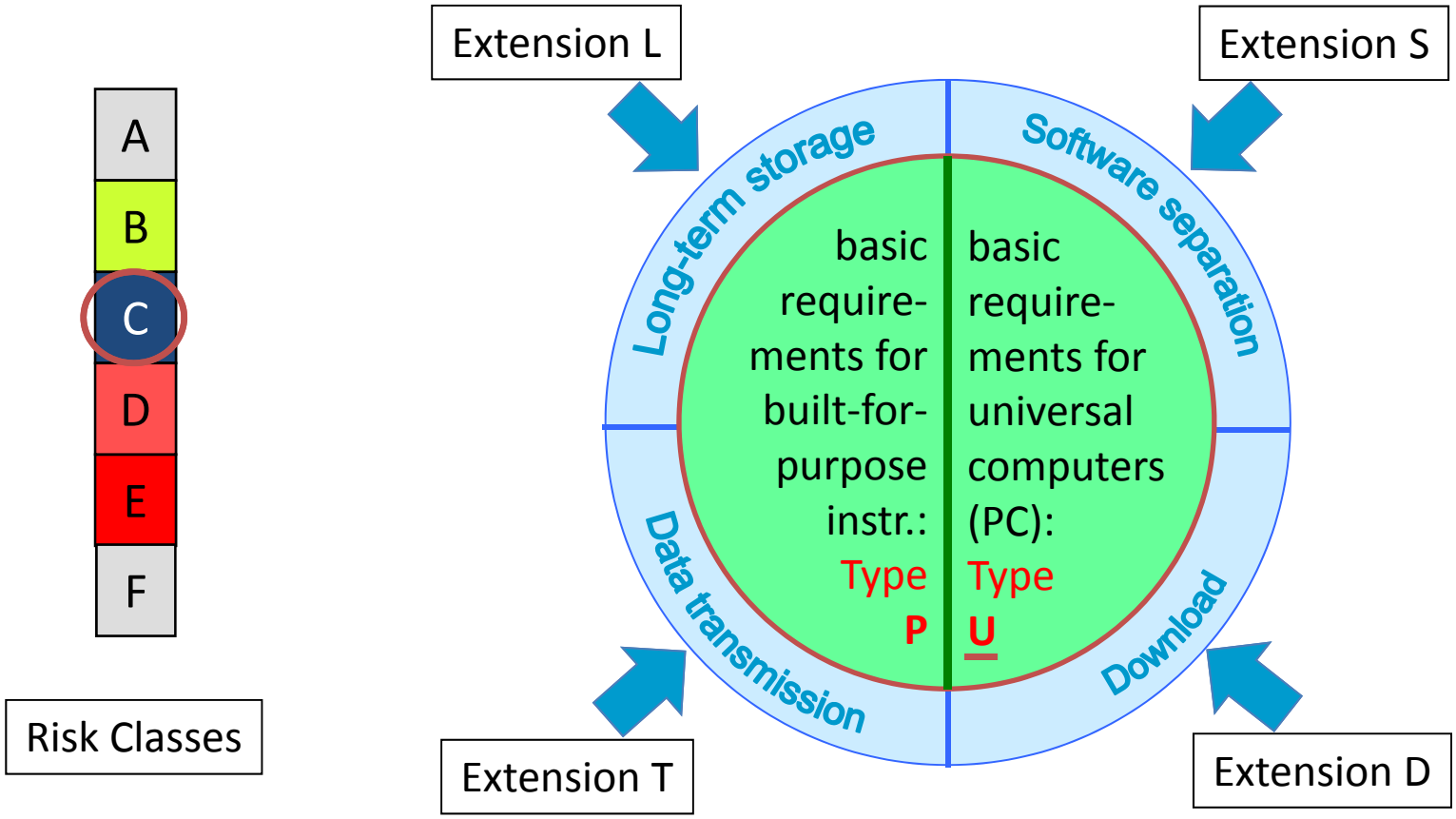


- **U1: Documentation**
- **U2: Software identification**
- **U3: Influence via user interfaces**
- **U4: Influence via communication interfaces**
- **U5: Protection against accidental or unintentional changes**
- **U6: Protection against intentional changes**
- **U7: Parameter protection**
- **U8: Presentation of measurement data**
- **U9: Influence of other software (Extension S)**

(WELMEC 7.2, 2015: p. 24-33)

WELMEC 7.2, 2015: Software Guide

Example: Dimensional Instrument



Extension L: Long-Term Storage

- Special requirements for the storage of data after measurement has been completed.
- Extension L should specifically be used when long-term storage is required by regulations.
- For three types of storage units:
  - Integrated storage unit.
  - Universal Computer storage unit.
  - Removable or remote (external) storage unit.

Extension L: Long-Term Storage

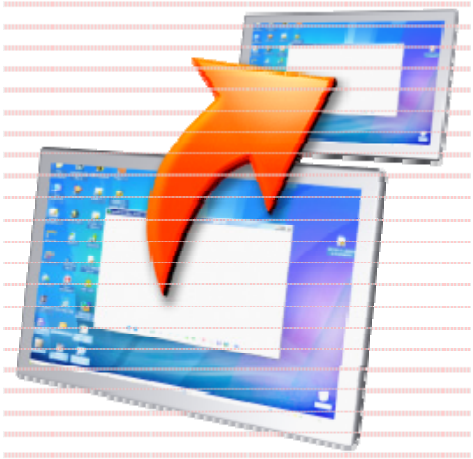
- **L1: Completeness of measurement data stored**
- **L2: Protection against accidental or unintentional changes**
- **L3: Integrity of data**
- **L4: Authenticity of measurement data stored**
- **L5: Confidentiality of keys**
- **L6: Retrieval, verification, and indication of stored data**
- **L7: Automatic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

(WELMEC 7.2, 2015: p. 34-42)

Extension T: Data Transmission

- Special requirements for Transmission of Measurement Data via Communication Networks

- Only applied if measurement data is transmitted via communication networks to a distant device, where it is further processed and/or used for legally relevant purposes.



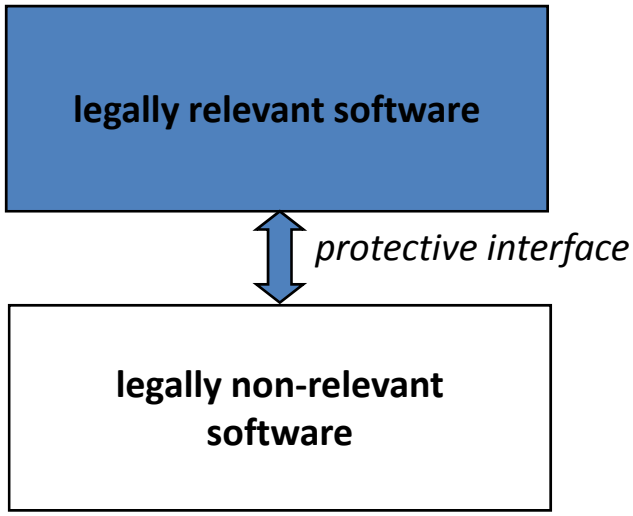
Extension T: Data Transmission

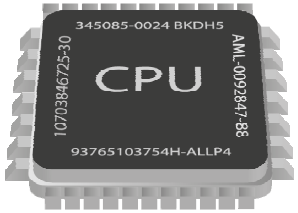
- **T1: Completeness of transmitted data**
- **T2: Protection against accidental or unintentional changes**
- **T3: Integrity of data**
- **T4: Authenticity of transmitted data**
- **T5: Confidentiality of keys**
- **T6: Handling of corrupted data**
- **T7: Transmission delay**
- **T8: Availability of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

(WELMEC 7.2, 2015: p. 43-50)

Extension S: Software Separation

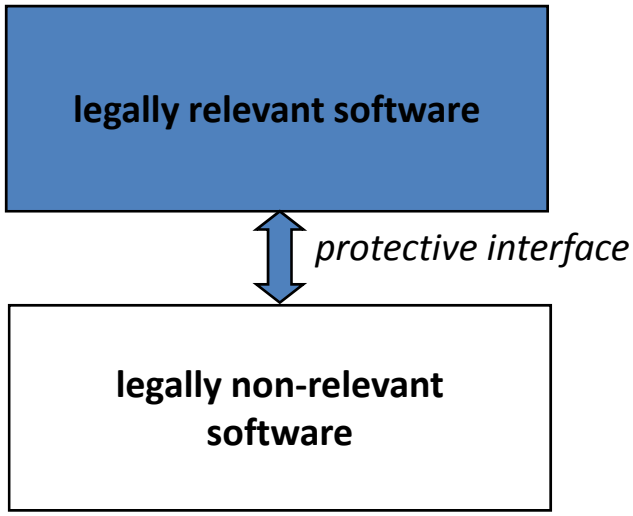
- Optional design methodology.
- Allows the manufacturer to easily modify legally non-relevant software.
- Protective Software Interface Idea.





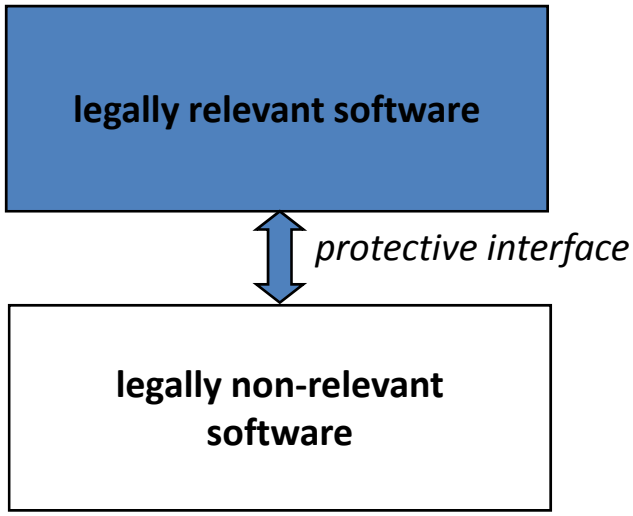
Extension S: Software Separation

- Protective Software Interface:
  - All interactions and data flow shall not inadmissibly influence the legally relevant software including the dynamic behaviour of a measuring process.
  - There shall be an unambiguous assignment of each command sent via the software interface to the initiated function or data change in the legally relevant software.
  - The interface shall be documented completely.



Extension S: Software Separation

- **S1: Realisation of software separation**
- **S2: Mixed indication**
- **S3: Protective software interface**



(WELMEC 7.2, 2015: p. 51-54)

Extension D: Download of Legally Relevant Software

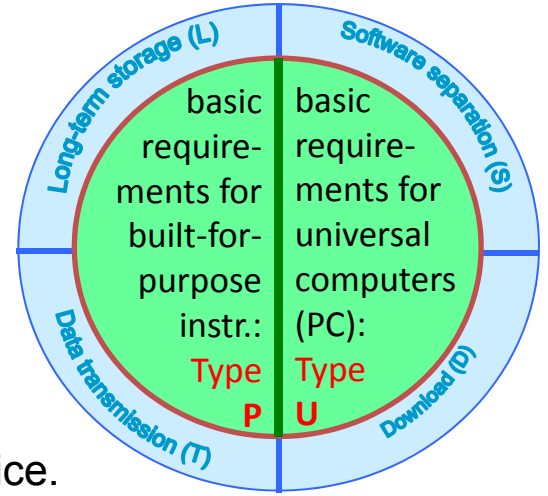
- Important remarks:
  - MID does not cover download of legally relevant software
  - Added to WELMEC (it should always exist the download-disable option)
  - In Germany Extension D is legally accepted since 2015 (only national)

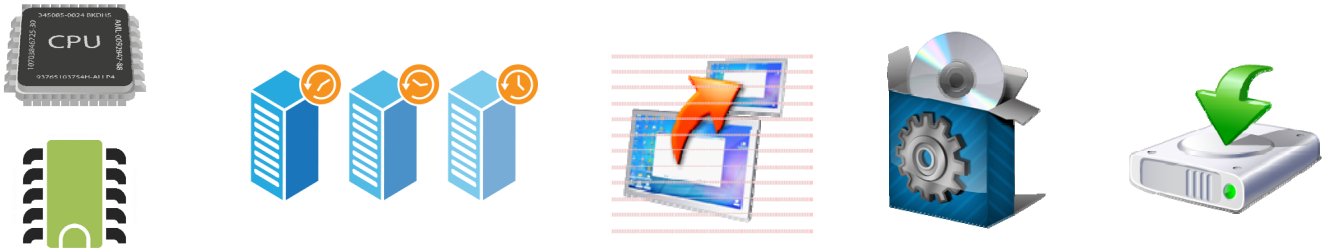
- **D1: Download mechanism**
- **D2: Authentication of transmitted software**
- **D3: Integrity of downloaded software**
- **D4: Traceability of legally relevant software download**

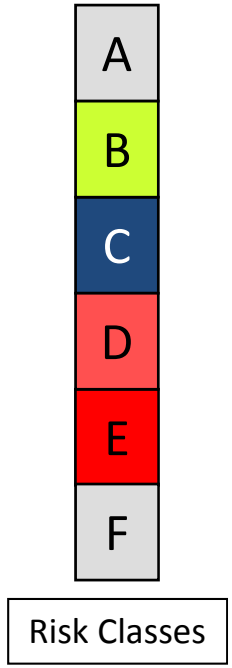
(WELMEC Guide 7.2: p. 55-59)

Summary

- Choosing the correct set of requirements:
  - **Risk Class** (Class A-B-C-D-E-F).
  - **Basic Configuration** (Type U, Type P).
  - **Extensions** to the basic configuration present in the device.
    - Long-term storage (Extension **L**)
    - Transmission of measurement data (Extension **T**)
    - Software separation (Extension **S**)
    - Download of legally relevant software (Extension **D**)







Thank you for your attention!

Questions?

Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Abbestraße 2-12
10587 Berlin

Dr.-Ing. Federico Grasso Toro
Telephone: 030 3481-7022
E-Mail: federico.grassotoro@ptb.de

www.ptb.de

Basic Requirements for Type P Instruments

- **P1: Documentation**
- **P2: Software identification**
- **P3: Influence via user interfaces**
- **P4: Influence via communication interfaces**
- **P5: Protection against accidental or unintentional changes**
- **P6: Protection against intentional changes**
- **P7: Parameter protection**

(WELMEC 7.2, 2015: p. 17-23)