Physikalisch-Technische Bundesanstalt
National Metrology Institute

Working group 8.51 „Metrological Software“ Last revision: July 16, 2020

Leaflet:
Software documentation requirements for conformity assessments

1 General

For each measuring instrument submitted for conformity assessment, in case the instrument contains software, a software documentation must be submitted. This documentation must include the following general characteristics:

- Meaningful document title and/or identifier of the document,
- Name of the type of measuring instrument to which the document relates,
- Version number/issue date of the document or similar and
- Page and section numbering, or other referencing options.

The documents must be easy to read and consistent. They must be written in German, provided they are intended for users, operators, and market supervision or verification authorities. In all other cases, either German or English documents are permitted.

If the documents are provided in electronic form, their content shall not be updated automatically after the file has been opened (for example disabling the automatic date updating) and they shall be viewable und searchable with widely used, freely available programs. Therefore, electronic documents are recommended to be submitted as unprotected pdf-files.

The following required content may be included in one single document, but it can also be distributed among several documents. The operation manual of the measuring instrument must be provided separately.

The checklist “Software documentation” in the annex can be used to check the completeness of the created documents. It is recommended to submit the list with the created documents within the frame of the type examination, since the test effort is reduced if the list is completed and correct.

2 General content

A basic understanding of the entire measuring instrument is necessary in order to be able to determine the scope and detailed requirements of the software examination, the following must be documented:

2.1 System hardware

- Overview of the system hardware (e.g. block diagram with the used hardware components, transmission paths for the measurement values and parameters)

2.2 Software structure

- Pertinent information about the software structure (e.g. pertinent information about which software modules[1] are contained in which hardware component)

2.3 Measuring process, parameter and measuring values

- Description of the legally relevant measuring process including all involved software modules, parameters and measurement values

2.4 Operating system

- In the case of an operating system being used: type, version, and further characteristics (e.g. service packs installed for MS Windows, name of the Linux distribution), description of the configuration of the operating system, with regards to all legally relevant protection measures (Details can be found in [1])

2.5 Legally relevant executable software modules

For risk classes E and F:

- Declaration for the generation of the legally relevant executable software modules (Manufacturer's declaration) [2]
- Technical description for the generation of the legally relevant executable software modules [3]
- Description of the method and details of the technical means by which the bit-to-bit identity between the type pattern and any serial instrument can be checked (If necessary: technical means for the bit-to-bit identity comparison)

3 Basic requirements for legally relevant software

For each **legally relevant executable software module**, the following must be documented:

3.1 Software identification

- Type of identification, description of the realisation (list of the software modules and type-specific parameters covered by the identification as well as the formation rules of the identifiers)
- Values of the identifiers for which the approval shall be made
- Instructions for displaying the identifiers

3.2 Influence via user interface

- List of all user interfaces (e.g. graphical user interface, push-buttons, switches, controllers, dongles, jumpers, keys)
- List of all user actions (e.g. inputs, commands, menu items, buttons) for all existing user interfaces and, if applicable, their possible combinations as well as their effect
- Explanation of how an inadmissible influence the legally relevant properties of the measuring instruments via the user interfaces is prevented

3.3 Influence via communication interface

- List of all communication interfaces (e.g. interfaces for wired connections, optical/infrared and acoustic connections, radio connections, analogue connections)
- List of all receivable commands of all communication interfaces and their effect

[1] The term „software module“ includes programs, libraries, drivers, data sets, operating system components and more.

- Explanation of how an inadmissible influence the legally relevant properties of the measuring instruments via the communication interfaces is prevented

3.4 Protection against accidental or unintentional changes

- Description of how legally relevant executable software modules, type-specific parameters and device-specific parameters are protected against accidental or unintentional changes:
  - Which protection measures are used?
  - When are these procedures used?
  - When are the protection measures checked?
  - What is the response of the system in case of failure?
  - Which software modules or parameters are protected?
- Description of how critical user actions (e.g. deleting or modifying data) are prevented (e.g. by deactivation or request for confirmation)
- Description of plausibility checks for user input

3.5 Protection against intentional changes

- Description of how legally relevant executable software modules and type-specific parameters are protected against manipulations:
  - Which protection measures are used? (Hardware solutions can also be used here, such as security seals, seals, dongles)
  - When are these procedures used?
  - When are the protective measures checked?
  - What is the response of the system in case of failure?
  - Which software modules or parameters are protected?
- Description of how the storage containing software modules or parameters are protected against physical replacement or overwriting

3.6 Parameter protection

- List of all device-specific parameters with name, short description, range of values, normal value, storage location, and display and modification options
- Description of the protection measures for the instrument-specific parameters:
  - Which protection measures are used for which instrument-specific parameters?
  - When are these procedures used?
  - When are the protective measures checked?
  - What is the response of the system in case of failure?

3.7 Software authenticity and presentation of measurement values (only if legally non-relevant software is present)

- Indicate the displayable legally relevant measurement values
- Description of how to ensure that the legally relevant software exclusively displays and/or issues the legally relevant measurement values and that the displayed legally relevant measurement values have been measured by the legally relevant sensor or by other legally relevant hardware components
- Description of how it is ensured that the display of the legally relevant measurement values and other information cannot be confused with those/other indications generated by legally non-relevant software modules

4 Long-term storage and transmission

For each **hardware component permanently storing legally relevant measurement values and parameters** and for each **transmission of legally relevant measurement values and parameters between two legally relevant hardware components,** the following must be documented:

4.1 Completeness of stored/transmitted measurement values and parameters

- List of all measurement values and parameters, including name, short description, format, and unit
- Specify the storage location and/or the transmission path

4.2 Protection of stored/transmitted measurement values and parameters against accidental or unintentional changes

- Indicate the measures taken to protect the values against unintentional changes (e.g. checksum)
- Indicate the software modules that store or *transmit* the measurement values and parameters and provide the protection measures, as well as the software modules that read or receive the measurement values and parameters and check the protection measures
- Indicate which measurement values and parameters are protected
- Behaviour in the event of failure

4.3 Protection of stored/transmitted measurement values and parameters against intentional changes

- Indicate the measures taken to protect against intentional changes (in the case of stored values/parameters: e.g. protection against storage exchange, usage of checksums or hash values with secret start values; in the case of transmitted values/parameters: hash values with secret start values, encryption, as well as hardware measures, such as locking)
- Indicate the software modules that store or *transmit* the measurement values and parameters and provide the protection measures, as well as the software modules that read or receive the measurement values and parameters and check the protection measures
- Indicate which measurement values and parameters are protected
- Behaviour in the event of failure

4.4 Attribution of stored/transmitted measurement values and parameters

- Description of how a measurement is identified
- Description of how the stored/transmitted values and parameters are attributed to a measurement
- Description of how the attribution is protected against changes
- In case of stored measurement values: Description of whether and how the attribution to the measurement is clearly recognizable on each legally relevant output (e.g. displays, print out, invoices, receipts)
- In case of transmitted measurement values: Description of how the receiving component or the receiving software can determine the origin of the received values (e.g. serial number of the sender)

4.5 Confidentiality of keys

- If secret keys, start values, polynomials or similar are used: Description of how these are protected against reading, deleting and modifying

4.6 Automatic storing

- Description of how and to what extent the measurement values are automatically saved
- If the user can discard measurements or delay the data storage: Description of the conditions or rules applicable to these cases

4.7 Storage capacity and continuity

- Indicate the range of the stored measurement values with their exact lengths specifications
- Indicate the capacity of the storage medium used and, if applicable, the description of how it can be physically exchanged
- Specify the number of storable measurements (absolute specification or computation formula)
- Measures invoked when the storage capacity is exceeded or in the absence of the storage medium
- Protection measures against premature deleting stored measurement values

4.8 Transmission delay and availability of transmission services

- Description of how the receiving component reacts in the event of delays in the transmission of measurement values
- If measurement values should not get lost during transmission, the following must be described:
  - How is the user prevented from interrupting the transmission?
  - How is feedback given, regarding the successful/unsuccessful transmission?
  - How are the transmitted measurement values buffered for a possible re-transmission?
  - What happens if the buffer capacity is exceeded?
  - How is a connection failure detected and, if applicable, how is it re-established?

5 Software update of legally relevant software

If the **legally relevant software** of a serial device **is planned to be updated during operation without breaking a seal** (and thus without subsequent verification), the following additional documentation according to [4] is required:

5.1 Download mechanism

- Description of the download mechanism:
  - To what extent does the mechanism run automatically?
  - Which parts of the software are exchanged, which parts are not?
  - How is the new software put into operation after the download?
  - Which existing protection measures are deactivated for the download? When and how are they re-activated (after the successful/unsuccessful download)?
  - What checks or monitoring mechanisms are available during the download process?
  - What are the consequences of an error or of an interruption of the download?
  - How is it ensured that legally relevant functions and data cannot be influenced or changed during the download process?
  - Are there country-specific possibilities to block the download?
  - How many downloads, download attempts or failed downloads are allowed?

5.2 Authentication and integrity of downloaded software

- Description of how it is checked, whether the newly downloaded software is the correct one for the measuring instrument in question

- Description of the integrity check of the downloaded software
- Description of the reaction of the system in the event of a failure

5.3 Traceability of legally relevant software download

- Type of logging of the download
- Description of the log storage (size, as well as protection against changes, deleting or remove)

6 Software separation

For each **hardware component containing legally relevant and legally non-relevant executable software modules,** the following additional documentation to [5]is required**:**

6.1 Realisation of software separation

- Description of the software structure, indicating which modules form the legally relevant and the legally non-relevant parts of the software
- Description of how the legally relevant software modules are protected against modifications or exchanges and against unauthorised interference, in the case the legally non-relevant software modules can be modified or exchanged

6.2 Mixed indication

- If legally relevant and legally non-relevant software modules use the same output medium: how can the outputs be differentiated

6.3 Interaction between legally non-relevant and legally relevant software

- Description of all interactions (e.g. commands, data flows) between the legally non-relevant software modules and the legally relevant software modules

7 Additional documents

For **measuring instruments pursuant to MID, Annex III** [6], additional documents must be provided, if applicable, as required with Section 10 of WELMEC 7.2, 2015: Software Guide [7].

8 References

[1] Leaflet: Configuration of general purpose operating systems for measuring instruments, Physikalisch-Technische Bundesanstalt, Working group 8.51 „Metrological Software“, in the current version
[2] Leaflet: Generation of the legally relevant executable software modules, Physikalisch-Technische Bundesanstalt, Working group 8.51 „Metrological Software“, in the current version
[3] Leaflet: Technical description for the generation of the legally relevant executable software modules, Physikalisch-Technische Bundesanstalt, Working group 8.51 „Metrological Software“, in the current version
[4] Leaflet: Requirements for software updates in measuring instruments and ancillary equipment in legal metrology, Physikalisch-Technische Bundesanstalt, Working group 8.51 „Metrological Software“, in the current version
[5] Leaflet: Requirements for software separation in measuring instruments and ancillary equipment in legal metrology, Physikalisch-Technische Bundesanstalt, Working group 8.51 „Metrological Software“, in the current version

[6] 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), Offical Journal of the European Union, L 96/149, March 29, 2014
[7] WELMEC 7.2, 2015: Software Guide (Measuring Instruments Directive 2014/32/EU), WELMEC, 2015

Annex: checklist "Software documentation"

(Tables may have to be duplicated)

Topic	Reference in the documentation	Remark
1 General	----------	----------
7 Additional documents		

2 General content		
Topic	**Reference in the documentation**	**Remark**
2.1 System hardware		
2.2 Software structure		
2.3 Measuring process, parameter and measuring values		
2.4 Operating system		
For risk class E and F: 2.5 Legally relevant executable software modules		

3 Basic requirements for legally relevant software		
Topic	**Reference in the documentation**	**Remark**
3.1 Software identification		
3.2 Influence via user interface		
3.3 Influence via communication interface		
3.4 Protection against accidental or unintentional changes		
3.5 Protection against intentional changes		
3.6 Parameter protection		
3.7 Software authenticity and presentation of measurement values (only if legally non-relevant software is present)		

4 Long-term storage and transmission		
Topic	**Reference in the documentation**	**Remark**
4.1 Completeness of stored/transmitted measurement values and parameters		
4.2 Protection of stored/transmitted measurement values and parameters against accidental or unintentional changes		
4.3 Protection of stored/transmitted measurement values and parameters against intentional changes		
4.4 Attribution of stored/transmitted measurement values and parameters		
4.5 Confidentiality of keys		
4.6 Automatic storing		
4.7 Storage capacity and continuity		
4.8 Transmission delay and availability of transmission services		

5 Software update of legally relevant software		
Topic	**Reference in the documentation**	**Remark**
5.1 Download mechanism		
5.2 Authentication and integrity of downloaded software		
5.3 Traceability of legally relevant software download		

6 Software separation		
Topic	**Reference in the documentation**	**Remark**
6.1 Realisation of software separation		
6.2 Mixed indication		
6.3 Interaction between legally non-relevant and legally relevant software		