Working group 8.51 „Metrological Software“ Last revision: March 12, 2018

Leaflet:
Requirements for the documentation for software testing, according to WELMEC Guide 7.2

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

- Document title or identifier of the document,
- Name of the type of instrument referred to by the relevant document,
- Version number, date of publication or similar,
- Page and section numbering, or other referencing options.

The documents must be easily legible 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 are permitted.

If documents are provided in electronic form, their content should not be updated automatically after the file has been opened (for example disabling the automatic date updating). Therefore, electronic documents are recommended to be submitted as unprotected pdf-files.

The required contents listed below do not have to be included in one single document. They may be distributed over several documents. The operating manual of the measuring instrument must be provided separately.

General content

- Overview of the system hardware (e.g. block diagram with the used hardware components, transmission paths for the measurement values);
- Information about the software structure (e.g. information about which software program is contained in which hardware component);
- Description of all legally relevant software functions, parameters and measurement values;
- If an operating system is used: Designation, 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 legally relevant protection measures;

- For risk classes E and F:
  - Declaration for the generation of the legally relevant executable programs (Manufacturer's declaration);
  - Technical description for the generation of the legally relevant executable programs;
  - Description of the method and details of the technical means by which the bit-to-bit identity between the type and any serial instrument can be checked (If necessary: technical resources for the bit-to-bit identity comparison).

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

Software identification

- Type of identification, description of the realisation (list of the software programs or program parts covered by the identification, calculation methods);
- Values of the software identifiers for which the approval shall be made;
- Instructions for displaying the identifiers.

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 is prevented in the software programs and, if applicable, in the operating system, via the user interfaces.

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;
- Explanation of how an inadmissible influence is prevented in the software programs and, if applicable, in the operating system, via the communication interfaces.

Protection against accidental or unintentional changes

- Description of how legally relevant executable programs and type-specific parameters are protected against accidental or unintentional changes:
  - Which protection measures are used?
  - When are these procedures used?
  - What is the response of the system in case of failure?
  - Which software programs, program parts or parameter sets 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.

Protection against intentional changes

- Description of how legally relevant executable programs, type-specific parameters and, if applicable, important parts of the operating system 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?

  - What is the response of the system in case of failure?
  - Which software programs, program parts or parameter sets or operating system parts are protected?
- Description of how the storage containing software programs or parameters are protected against physical replacement or overwriting.

Parameter protection

- List of all instrument-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?
  - What is the response of the system in case of failure?

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 to ensure that the display of the legally relevant measurement values and other information cannot be confused with those/other indications generated by legally non-relevant applications or software parts (in the case of operating systems, e.g. how to prevent the windows displaying legally relevant information from being covered by other windows).

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

Completeness of stored/transmitted measurement values

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

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

- Indicate the procedure used to protect the values against unintentional changes (e.g. checksum);
- Indicate the software parts that store or *transmit* the measurement values and provide the protection measures, as well as the software parts that read or receive the measurement values and check the measures;
- Indicate which measurement values are protected;
- Behaviour in the event of failure*;*
- Protection against critical user actions (e.g. deleting/modifying the measurement values).

Protection of stored/transmitted measurement values against intentional changes

- Indicate the procedure used to protect the measurement values against intentional changes (in the case of stored values: e.g. protection against storage exchange, usage of checksums or hash values with secret start values; in the case of transmitted values: hash values with secret start values, encryption, as well as hardware measures, such as locking);

- Indicate the software parts that store or *transmit* the measurement values and provide the protection measures, as well as the software parts that read or receive the measurement values and check the measures;
- Indicate which measurement values are protected;
- Behaviour in the event of failure*;*
- Protection against critical user actions (e.g. deleting/modifying the measurement values).

Attribution of stored/transmitted measurement values

- Description of how a measurement is identified;
- Description of how the stored/transmitted values 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).

Confidentiality of keys

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

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.

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.

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?

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 must be documented:

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?

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.

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).

For each **hardware component containing legally relevant and legally non-relevant executable programs,** the following additional documentation is required**:**

Realisation of software separation

- Description of the program structure, indicating the legally relevant and the legally non-relevant parts of the software (e.g. classes/objects, files, libraries);
- Description of how the legally relevant software is protected against modifications or exchanges and against unauthorised interference, in the case the legally non-relevant software can be modified or exchanged during operation.

Mixed indication

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

Interaction between legally non-relevant and legally relevant software

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

For **measuring instruments pursuant to MID, Annex III**, additional documents must be provided, if applicable, as required with Section 10 of WELMEC Guide 7.2.