Physikalisch-Technische Bundesanstalt
National Metrology Institute

Working group 8.51 “Metrological Software“ Last revision: April 07, 2022

Leaflet:
Configuration of legally relevant software for measuring instruments [special case]

1 General

In general, legally relevant software on measuring instruments is examined based on its functions concerning certain security properties[1], according to the WELMEC 7.2 Software Guide [1]. The validation of these properties can, however, be reduced to the examination of the configuration if the legally relevant software:

1. was developed for a general purpose,
2. is classified as proven in use,
3. complies with the state of the art,
4. does not stem from the manufacturer of the measuring instrument.

The purpose of this leaflet is to support the manufacturer of the measuring instrument in configuring the legally relevant software under the above conditions and according to the WELMEC 7.2 Software Guide [1].

The following cases can be considered as configurable legally relevant software:

- operating systems,
- database management systems,
- run-time environments,
- software for inter-process communication,
- software for hardware virtualization.

For a more detailed distinction of the liability of requirements, see RFC 2119 [2].

2 General requirements

The following requirements for the configuration of legally relevant software in measuring instruments generally apply to all software listed in section 1:

1. The software shall provide all necessary resources to permanently ensure the measuring operation.
2. Legally relevant configuration: The configuration of those parts of the software addressing protection of the legally relevant software on the measuring instrument or implementing the legally relevant function must be identifiable.
3. All changes to the legally relevant parts of the configurable software shall be traceable.

The documentation shall include a description of the configuration of the legally relevant software, the implemented protection measures and the legally relevant function. Furthermore, a description of the

[1] For instance, identification of software and traceability of changes.

method of identification and for tracing changes of the configuration of the legally relevant software as well as of the respective parts of the software is needed.

The implemented protective measures shall comply with the state of the art. Additionally, for examination according to the WELMEC 7.2 Software Guide [1] in higher risk classes, files for the legally relevant configuration of the software shall be provided.

3 Operating systems

Operating systems can be divided into general-purpose and those for special purposes.

General-purpose operating systems have mostly multi-user capabilities and possess various tools for administration and control of the measuring instrument.

Special-purpose operating systems are mostly designed for a dedicated task and are usually employed in a specific part of measurement data processing on the measuring instrument, e.g., pre-processing of sensor data under real-time conditions.

If legally relevant software is executed on a component with an operating system, the following requirement applies:

1. If the general-purpose operating system can only run in an administrable mode, the component shall not provide any open interfaces.
2. The measuring instrument shall not be administrable by the special purpose operating system.

Remark: The second requirement is solely used for determining the measuring instrument characteristic. According to the WELMEC 7.2 Software Guide [1], a measuring instrument can be categorized as an instrument of type P, if further criteria from [1] are met.

If legally relevant software runs on a general-purpose operating system, that operating system shall be configured according to the requirements of leaflet “Configuration of general-purpose operating systems for measuring instruments” [3].

4 Database management systems

If legally relevant data is stored in an administrable database management system (DBMS) on a general-purpose operating system, the following requirements apply:

1. The protection measures of the DBMS shall be matched to the protection measures of the underlying operating system.
2. The programmable interfaces of the DBMS shall be configured so that legally relevant datasets cannot be inadmissibly modified.

Remark: Additional requirements for long-term storage of measurement data can be found in extension L (Long-term Storage of Measurement Data) of the WELMEC 7.2 Software Guide [1].

5 Run time environments

If legally relevant software runs in one or more run-time environments (RTE) on a general-purpose operating system, the following requirements apply:

1. The run-time environment that runs the legally relevant software shall be installed under the legally relevant account of the operating system.
2. *In case of software separation:* Legally relevant objects must be protected against inadmissible influence during transfer from one RTE to another RTE.

Remark: Further requirements on the transmission of legally relevant data can be found in section 6 “Software for inter-process communication” of this leaflet and in extension T (Transmission of Measurement Data via Communication Networks) of the WELMEC 7.2 Software Guide [1].

6 Software for inter process communication

If legally relevant software communicates via an inter-process communication (IPC) framework on a general-purpose operating system, the following requirements apply:

1. The protection measures of the IPC framework shall be matched to the protection measures of the underlying operating system.
2. *In case of software separation:* If there is data exchange via the IPC software to legally non-relevant software, the legally relevant data exchange shall be secured according to extension T for *open* networks.

Remark: Only IPC frameworks are considered that are not part of the software equipment of a general-purpose operating system. For the configuration of an IPC framework that is part of a general-purpose operating system, see leaflet “Configuration of general-purpose operating systems for measuring instruments” [3].

7 Software for hardware virtualization

If legally relevant software is operated as a guest instance on a hypervisor, in a *localized environment* with virtualized hardware, the following requirements apply for the hypervisor:

1. The component on which the hypervisor runs, shall be physically protected against inadmissible access.
2. The hypervisor shall be integrated into the chain of trust of the system boot process.
3. The hypervisor should be configured in a way that hypervisor modules or virtualized components not needed for the legally relevant purpose are deactivated.
4. The hypervisor shall be configured in a way that prevents the execution of guest instances that can inadmissibly influence the legally relevant software.
5. The hypervisor shall be configured in a way that its interfaces are protected against inadmissible influence of the legally relevant guest instance.
6. Unnecessary hypervisor interfaces should be deactivated.

8 References

[1] WELMEC, *WELMEC 7.2, Software Guide (Measuring Instruments Directive 2014/32/EU),* 2015.

[2] S. Bradner, “Key words for use in RFCs to Indicate Requirement Levels - RFC 2199,” 21. January 2020. [Online]. Available: https://datatracker.ietf.org/doc/rfc2119/. [Accessed 22. March 2022].

[3] Physikalisch-Technische Bundesanstalt, Working group 8.51 "Metrological Software", *Leaflet: Configuration of general-purpose operating systems for measuring instruments [special case],* in the current version.

PTB-8.51-MB11-KOonfigSW-EN-V03