Working group 8.51 „Metrological Software“ Last revision: March 19, 2019

Leaflet: Configuration of general purpose operating systems for measuring instruments

This document is intended to assist the manufacturer to configure relevant parts of a general purpose operating system[1], installed on a measuring instrument[2], in cases where the operating system fulfills the essential requirements of Appendix 2 of the Measures and Verification Act (MessEV) [1] or in cases where the operating system can inadmissibly influence the legally relevant software on the measuring instrument.

Prerequisite for this are the proven-in-use and technical state-of-the-art properties of the operating system and its suitability for the general purpose. If the operating system is not equipped with the feature of user administration or runs in an administrable mode, the component[3] shall not provide any open interfaces.

Each of the following requirements must be met by technical measures at the hardware, operating system or software application level. The implemented protective measures must be documented by the manufacturer and must comply with the state-of-the-art. Additionally, for conformity assessment in higher risk classes (E-F), relevant configuration files and scripts of the operating system must be provided by the manufacturer.

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

Hardware properties

Without protected hardware, the protection of an operating system is not possible.

1. The component on which the operating system runs must be physically protected against unauthorized access.
2. There shall not be any open interfaces with given direct memory access.

The documentation must list the used components and describe the physical measures protecting them.

[1] Hereinafter referred to as the "operating system".
[2] Instrument components and auxiliary equipment included.
[3] Part of a measuring instrument, equipped with the legally relevant software.

Boot process and loading of the legally relevant software

While booting the operating system, a chain of trust is implemented, from the protected hardware to the loaded legally relevant software. Thereby, the integrity and authenticity of the legally relevant software is ensured.

1. At the end of the boot process, a chain of trust must be established over the individual components of the boot process.
2. The processing of the chain of trust may be interrupted, if its integrity is preserved.
3. The boot configuration must be protected against unauthorized modifications.
4. Booting via open interfaces must be prevented.

The documentation must contain the description of the chain of trust, the trusted anchor, and the boot configuration. Furthermore, the technical measures to prevent booting via open interfaces as well as to maintain the authenticity and integrity of the entire loaded legally relevant software must be documented.

Admissible components

When the operating system is started, device drivers and libraries are loaded, and services are activated.

1. The smallest number of operating system components[4] required to ensure the measuring operation should be selected.

The documentation must describe the loaded and loadable kernel modules, the device drivers and software libraries, the description of the kernel configuration as well as the services with their execution state.

Special mention should be made of the components that the manufacturer herself (or on her behalf) has implemented, referring to the measurement purpose or its support. It is also necessary to describe how it is ensured that the required system resources are available for operational use.

Protection during use

After placing on the market, operating systems have on-board features to prevent the influence of other programs during the operation of the legally relevant software.

1. The execution of software that may influence the legally relevant software inadmissibly must be prevented.
2. The operating system should ensure the uniqueness of the display of the legally relevant software.
3. The access control must be configured in such way that the intended use may not be inadmissibly influenced.
4. The administration shall only be allowed after a violation of protective measures.

[4] Kernel modules, services, drivers, libraries, etc. (including third-party providers).

The documentation must describe the display mode of the legally relevant software, the configuration of the user administration, as well as the control of the program execution. Furthermore, the technical measures to protect the administrator account must be documented.

Protective interfaces

The control of the data flow by the protection of interfaces is one of the central tasks in the configuration of the operating system.

1. Open hardware interfaces must be protected against inadmissible influence of the legally relevant software.
2. Software interfaces between operating system components and legally non-relevant software must be protected against inadmissible influence of the legally relevant software.
3. Unnecessary interfaces should be deactivated.

The documentation must list the open hardware interfaces. If legally non-relevant software exists, the software interfaces from the operating system to this software must also be listed. For all mentioned interfaces, the configuration and measures for controlling the data traffic must be documented.

Testability and traceability

The measure and verification act requires the identifiability of legally relevant software, as well as the traceability of changes, after placing it on the market. The legally relevant software includes the configuration of the operating system, as well as those operating system components that have been changed or added for the legally relevant task.

1. The configuration of the legally relevant parts of the operating system must be identifiable.
2. All changes to the configuration must be traceable.

The documentation must include an identifier, as well as a description of the measures for the identification. The traceability of changes in the legally relevant parts of the operating system must be documented.

References

[1] „Verordnung über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt sowie über ihre Verwendung und Eichung (Mess- und Eichverordnung - MessEV)“, Bundesgesetzblatt Jahrgang 2014 Teil 1, Nr. 58, Dezember 2014, zuletzt geändert am 11.08.2017.

[2] S. Bradner, Key words for use in RFCs to Indicate Requirements Levels, March 1997, URL: https://tools.ietf.org/html/rfc2119 (last accessed on February 05, 2019).