MUHAMMAD AZWAN IBRAHIM

OIML D31

An Overview to Software Requirements

OIML Documents

There are 4 main categories of OIML publications: OIML R,D,G and B

Two most commonly used OIML documents

OIML R - which are model regulations that establish the metrological characteristics required of certain measuring instruments and which specify methods and equipment for checking their conformity. OIML Member States shall implement these Recommendations to the greatest possible extent;

OIML D - which are informative in nature and which are intended to harmonise and improve work in the field of legal metrology;

D31 was developed by Project Group 3 in the OIML Technical Subcommittee TC 5/SC 2 Software.

Structure of D31:2019

1. Introduction
2. Scope and field of application
3. Terms and definitions
4. Instructions for use of this Document in drafting OIML Recommendations
5. Risk assessment
6. Requirements for measuring instruments with respect to the application of software

   6.1 General requirements

   6.2 Requirements specific for configurations
7. Type evaluation
8. Verification of measuring instrument

   Annexes

Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

Software examination methods

No	Abbreviation	Description	Application	Preconditions, tools for application	Special skills for performing
1	**AD**	Analysis of the documentation and evaluation of the design	Always	Documentation	-
2	**VFTM**	Verification by functional testing of metrological functions	Correctness of the algorithms, uncertainty, compensating and correcting algorithms, rules for price calculation	Documentation, specimen	-
3	**VFTSw**	Verification by functional testing of software functions	Correct functioning of communication, indication, evidence of intervention, protection against operating errors, protection of parameters, detection of significant defects	Documentation, specimen	-
4	**DFA**	Metrological data flow analysis	Software separation, evaluation of the impact of commands on the instrument's functions	Source code, tools for analysing source code	Programming
5	**CIWT**	Code inspection and walkthrough	All purposes	Source code, tools for analysing source code	Programming
6	**SMT**	Software module testing	All purposes when input and output can clearly be defined	Source code, testing environment	Programming

Software examination methods (example)

	Requirement	Validation procedure A (normal examination level)	Validation procedure B (extended examination level)	Comment
6.1.1	Software identification	AD + VFTSw	AD + VFTSw + CIWT	Select »B« if high conformity is required
6.1.2	Correctness of algorithms and functions	AD + VFTM	AD + VFTM + CIWT/SMT	
6.1.3.1	Prevention of misuse	AD + VFTSw	AD + VFTSw	
6.1.3.2	Evidence of intervention	AD + VFTSw	AD + VFTSw + DFA/CIWT/SMT	Select »B« in case of high risk of fraud
6.1.4.1	Detection of significant defects	AD + VFTSw	AD + VFTSw + CIWT + SMT	Select »B« if high reliability is required
6.1.4.2	Durability protection	AD + VFTSw	AD + VFTSw + CIWT + SMT	Select »B« if high reliability is required

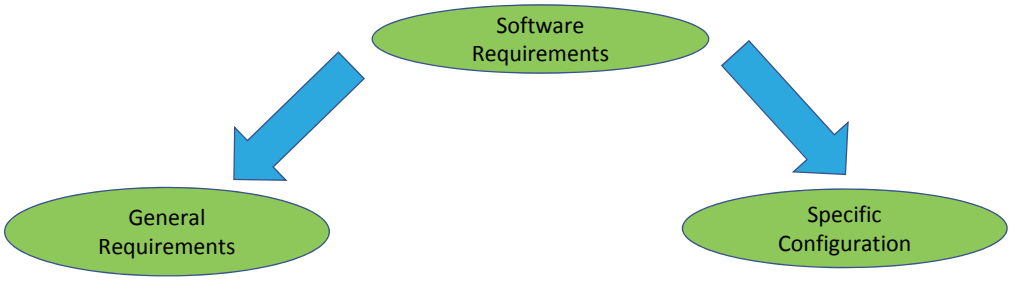
Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

Structure of requirement (Part 6)

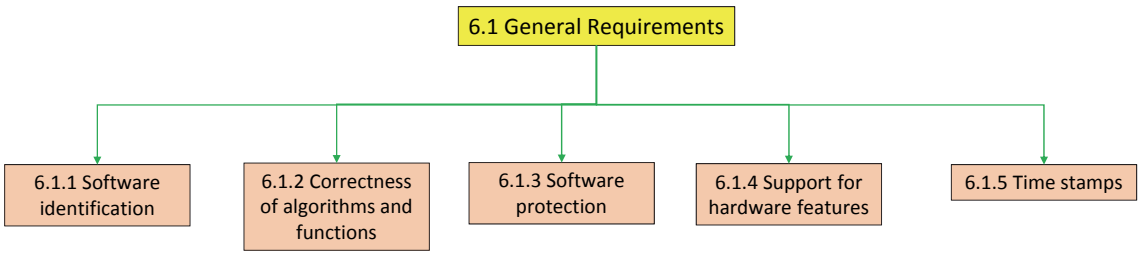
- Set of requirements is variable, depending on the features and complexity of the measuring system:

  6.1 General software requirements (all instruments)

  6.2 Specific software requirements (specific configurations)

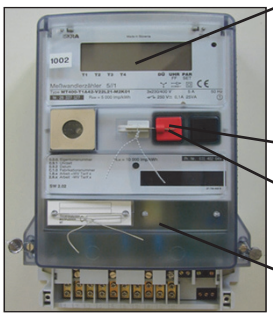


General requirements



Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

- "Simple" instrument (e.g. electricity meter)



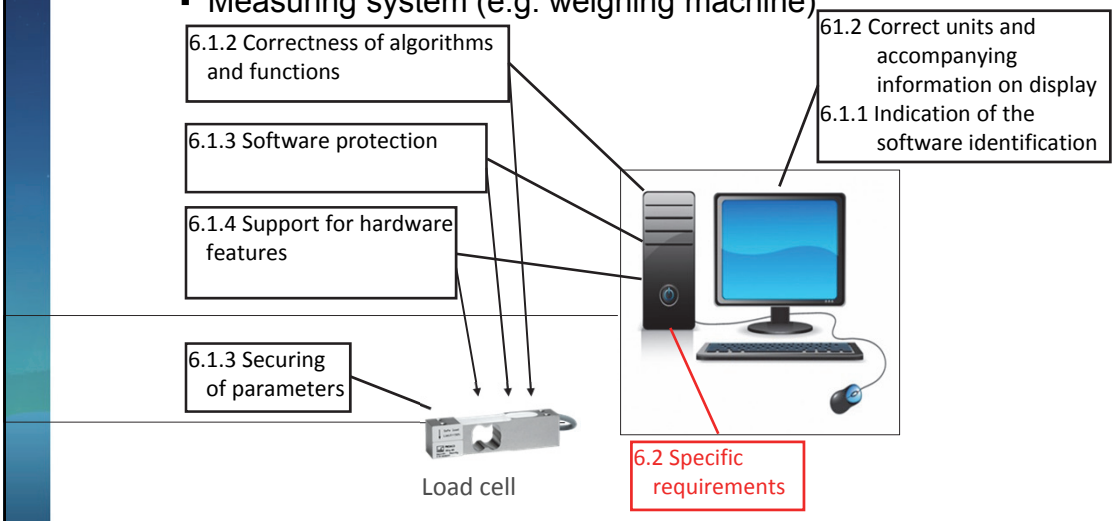
6.1.1 Indication of the software identification
6.1.2 Correctness of algorithms and functions, correct units and accompanying information on display

6.1.3 Software protection

6.1.3 Securing of parameters

6.1.4 Support for hardware features (fault detection, durability protection)

- Measuring system (e.g. weighing machine)



Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC
Asia-Pacific Economic Cooperation

6.1.1 Software identification

- Software of measuring instrument should have version or another token
- The identification shall be inextricably linked to the software itself
- The identification shall be able to be presented or printed on command or displaying
- which is inextricably linked to software itself

Example of software identification
- Version
- Checksum, Hash

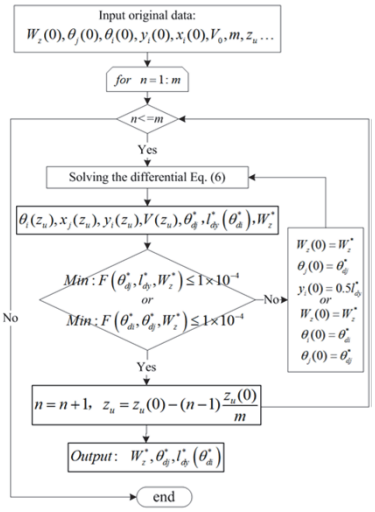
- Software identification shall be clearly stated inside the type approval certificate.

(I) V1.5.12a

V1.5.12a-2D7F (II)

6.1.2 Correctness of algorithms and functions

- Requirement: The measuring algorithms and functions shall be appropriate and functionally correct.
- Take MPE into consideration when constructing or examining an algorithm.
- Examples for obviously essential impact of the software to the MPE:
  - quantization, number of digits, rounds in successive approximation, and abort criterion
  - arithmetic, type of numbers integer, float …)
  - analogue-digital conversion
  - Specific complex applications
  - image processing
  - dynamic weighing



Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

Software protection

Prevention of misuse

Evidence of intervention

6.1.3 Software protection

- Misuse operation is usual in measuring instrument even if with a perfect instruction manual
- warning or dialog box is necessary facing wrong operation
- some important legally parameter is related metrology performance of measuring instrument, if the parameter is modified, metrology performance would be changed, so modifying legal parameter should be authorized and recorded for maintaining performance of measuring instrument

Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

6.1.3.1 Prevention of misuse

- measuring instrument shall be constructed in such a way that possibilities for unintentional, accidental, or intentional misuse are minimal.
- presentation of the measurement results shall be unambiguous for all parties affected
- The user needs good guidance for correct use and for achieving correct measurement results (User-friendly)

- Example: Guided menus for the user for crucial actions
- Keep man-machine-interface simple

6.1.3.2 Evidence of intervention (Fraud protection)

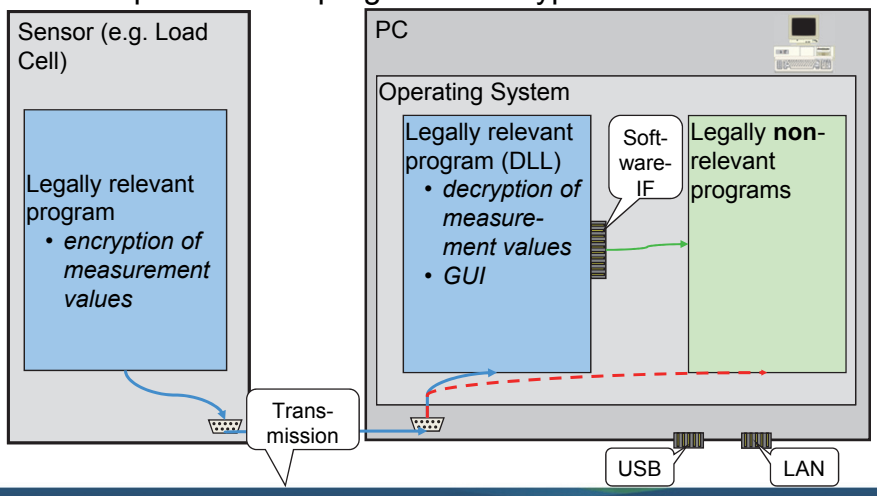
- Software shall be protected in such a way that evidence of any intervention shall be available (e.g. software updates, parameters changes)
- software shall be secured against unauthorised modification, loading, or changes by swapping the memory device
- mechanical sealing or other technical means may be necessary to secure measuring instruments
- audit trails are considered to be part of the legally relevant software and should be protected as such

Examples:
The housing containing the memory device is sealed or the memory device is sealed on the PCB.
Rewritable device: write-enable input inhibited by a switch that can be sealed.

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

Fraud protection

- Ex.: encapsulated PC program + encrypted transmission



6.1.3.2 Evidence of intervention (Fraud protection)

Only clearly documented functions are allowed to be activated by the user interface.

- Example: Data entered through the user interface are redirected to a program that filters incoming commands. It only allows documented ones and discards all others.

Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

6.1.3.2 Evidence of intervention (Fraud protection)

Parameters that fix the legally relevant characteristics of the measuring instrument shall be protected against modification. If necessary for the purpose of verification of a measuring instrument, displaying or printing of the current parameter settings shall be possible

- Example: Device specific parameters to be secured are stored in a non-volatile memory. The write-enable input of the memory is inhibited by a switch that can be sealed.

6.1.3.2 Evidence of intervention (Fraud protection)

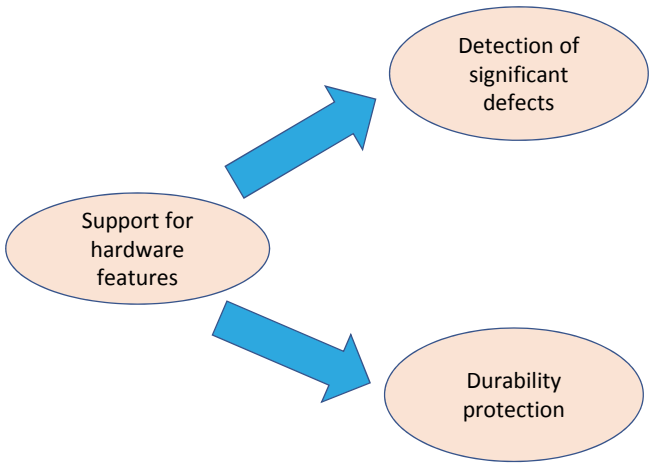
Software protection shall comprise appropriate sealing by mechanical, electronic and/or cryptographic means, making an intervention impossible or evident.

- Example, electronic sealing:
  - The metrological parameters of an instrument can be input and adjusted by a menu item.
  - The software recognizes each change and increments an event counter.
  - The event counter value can be indicated.
  - The initial value is registered (e.g. on the plate).
  - If the indicated value differs from the registered one, the instrument is in an unverified state (equivalent to a broken seal).

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

6.1.4 Support for hardware features

- If the hardware or software part have certain faults, software should support to check, and make response.
- A good measuring instrument could be used for years, and for a period time it need to be calibrated or adjusted
- software should satisfy the check of prescribed time in order to guarantee the durability of measuring instrument.



6.1.4.1 Detection of significant defects

- Example:
  - On each start-up the legally relevant program calculates a checksum of the program code and legally relevant parameters.
  - The nominal value of these checksums has been calculated in advance and stored in the instrument.
  - If the calculated and stored values do not match, the program is stopped.

Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

6.1.4.2 Durability protection

Example of durability protection

- Some kinds of measuring instruments require an adjustment after a prescribed time interval, in order to guarantee the durability of the measurement.
- The software gives a warning when the maintenance interval has elapsed and even stops measuring, if it has been exceeded for a certain time interval.

6.1.5 Time stamp

- The time stamp shall be in a consistent format, allowing for easy comparison of two different records and tracking progress over time
- The time stamp shall be read from the clock of the instrument.
- Depending on the kind of instrument or on the field of application, setting the clock may be legally relevant and appropriate protection means shall be taken according to the risk level to be applied

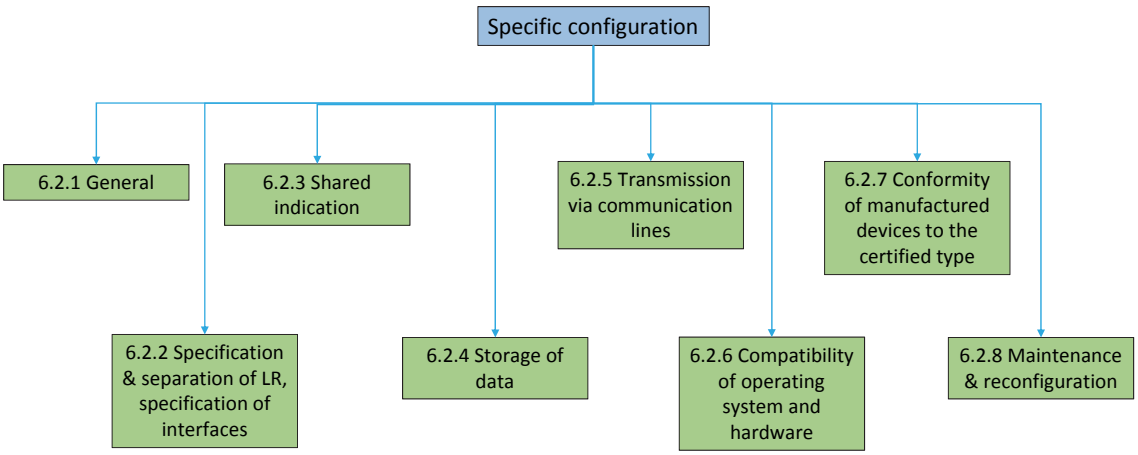
- Where the specific field of application requires high accuracy information concerning the exact time of the measurement, it may be necessary to improve the reliability of the internal clock using specific means. (e.g. redundancy of internal quartz-controlled clock, regular self- calibration)

Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

6.2 Specific Configuration

- deal with technical features that are not common for some kinds of instruments or in some areas of application.
- shall be considered in addition to 6.1

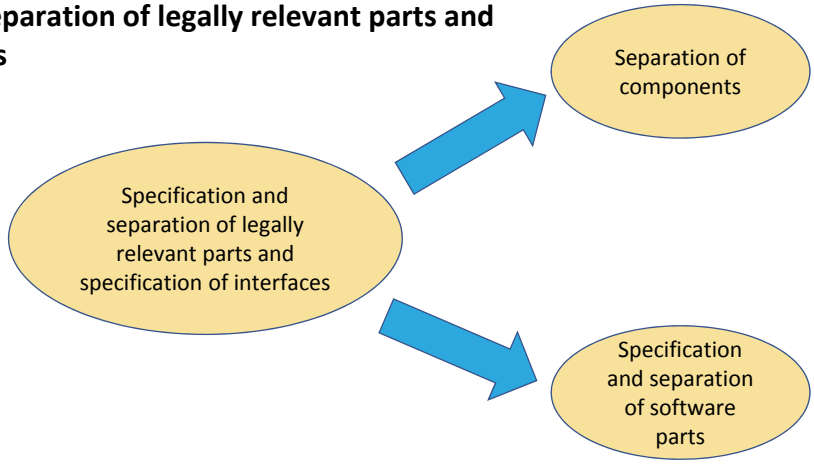
6.2 Specific configuration



Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

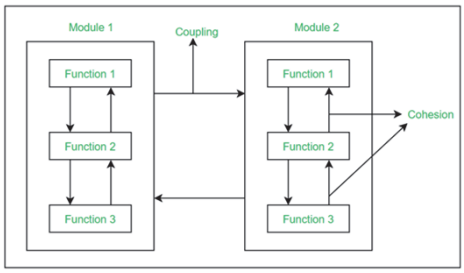
6.2.2 Specification and separation of legally relevant parts and specification of interfaces

- applies if the measuring instrument/component has interfaces for communicating with other instruments/ components, with the user, or with other software parts besides the legally relevant parts within a measuring instrument/component.
- Legally relevant parts of a measuring instrument – whether software or hardware parts – shall not be inadmissibly influenced by other parts of the measuring instrument.



6.2.2.1 Specification and separation of software parts

- All software modules (programs, subroutines, objects, etc.), that perform legally relevant functions or that process legally relevant measurement data, form the legally relevant software part of a measuring instrument/component shall be made identifiable as described in 6.1.1
- If the separation of the software is not possible or needed, the software is legally relevant as a whole
- If the legally relevant software part communicates with other software parts, a software interface shall be defined.
  - All communications shall be performed exclusively via this interface
  - The legally relevant software part and the interface shall be clearly documented
  - All legally relevant functions and data domains of the software shall be described
  - The software interface consists of program code and dedicated data domains

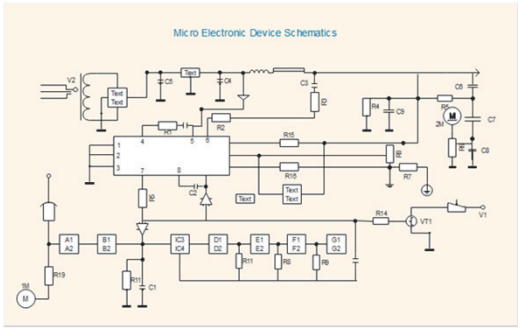


Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

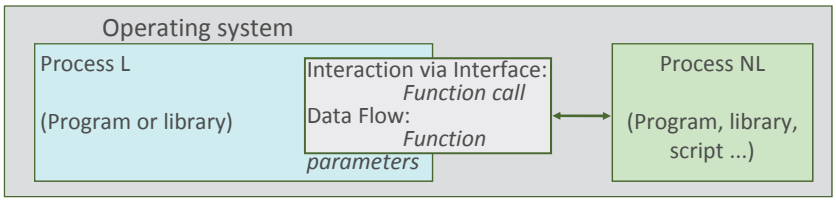
6.2.2.1 Separation of components

- Components of a measuring instrument that perform legally relevant functions shall be identified, clearly defined and documented. They form the legally relevant part of the measuring instrument.

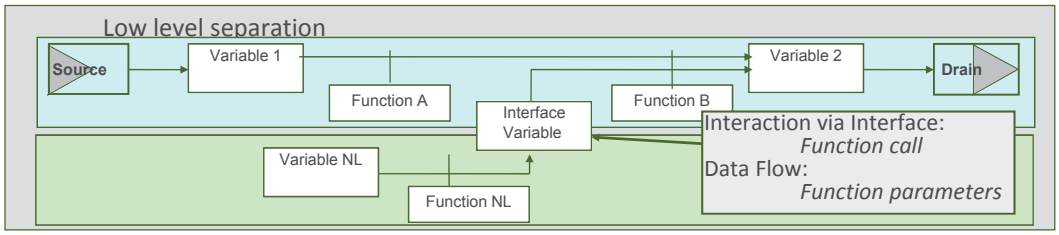
- It shall be demonstrated that the functions and data of components that are legally relevant cannot be inadmissibly influenced by commands received via the interface from the other, legally non-relevant parts.
  - This implies that there is an unambiguous assignment of each command to all initiated functions or data changes in the component.



Example: High level separation, operating system



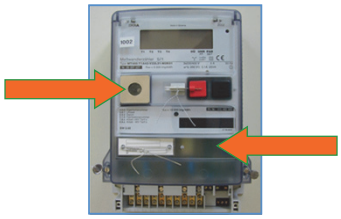
Example: Low level separation, using the features of programming language



Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC
Asia-Pacific Economic Cooperation

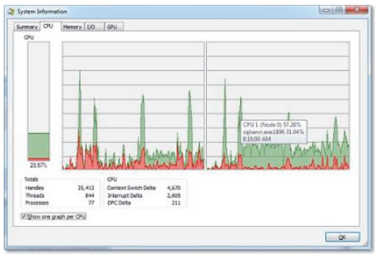
6.2.2.2 Specification and separation of software parts (continue)

- There shall be an unambiguous assignment of each command to all initiated functions or data changes in the legally relevant software part.
  - Functions that are triggered through the software interface shall be declared and documented.
  - Only documented functions shall be activated through the software interface.



6.2.2.2 Specification and separation of software parts (continue)

- The legally relevant software part shall have priority using the resources over nonrelevant software.
  - The legally relevant process shall not be inadmissibly interrupted by legally non-relevant software
  - The measurement process (realised by the legally relevant software part) shall not be delayed or blocked by other processes



Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

6.2.3 Shared indication

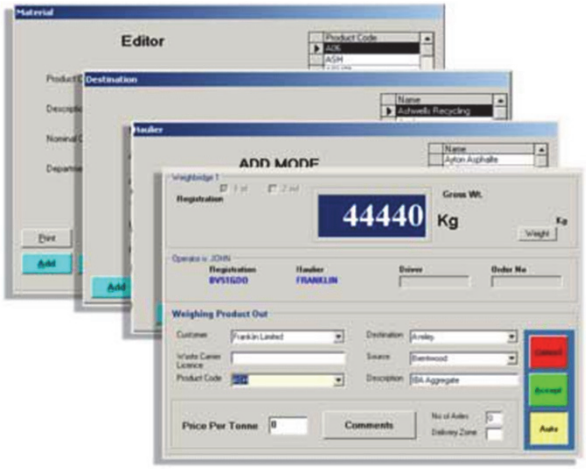
- A display or printout may be employed to present both information from the legally relevant software part and other information.
- If a display or printout is used both for legally relevant and legally nonrelevant outputs, the legally relevant information should always be readable, and clearly distinguishable from other information.

- The window containing the legally relevant data shall have highest priority i.e.
  - it shall not be deleted by other software
  - or overlapped by windows generated by other software
  - or minimized
  - or made invisible

as long as the measurement is running and the presented results are needed for the legally relevant purpose.

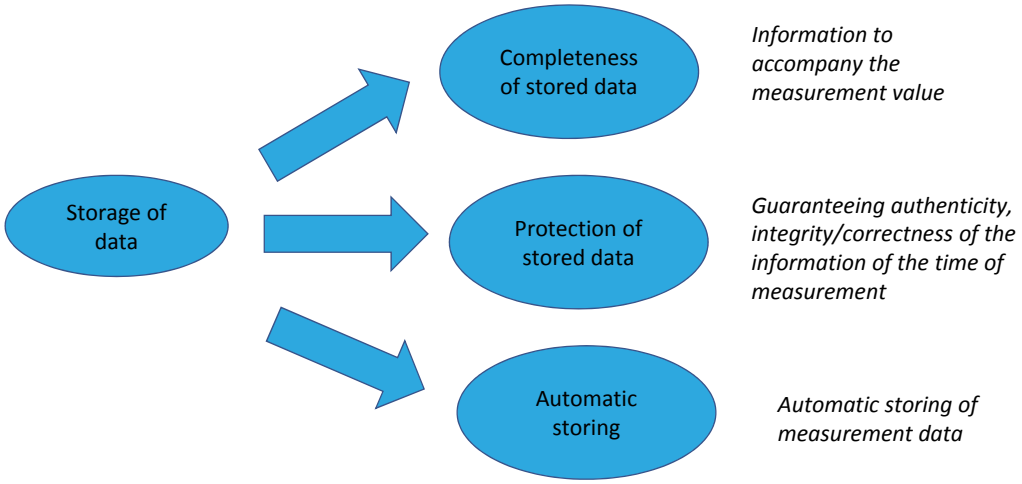
Example of shared indication

- The instrument has an operating system with a multiple windows user interface.
- The window displaying the legally relevant data is generated and controlled by procedures in the legally relevant dynamically linkable library
- During measurement, these procedures check cyclically that the relevant window is still on top of all the other open windows; if not, the procedures place it on top.



Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

6.2.4 Storage of data



6.2.4.2 Completeness of stored data

- The measurement data stored shall be accompanied by all relevant information necessary for future legally relevant use.

Examples:
A stored dataset of the measurement result includes the following entries:

- measured value including unit;
- time stamp of measurement (see 6.1.5);
- place of measurement or identification of the measuring instrument that was
- used for the measurement;
- unambiguous identification of the measurement, e.g. consecutive numbers enabling assignment to values printed on an invoice.

Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

6.2.4.3 Protection of stored data

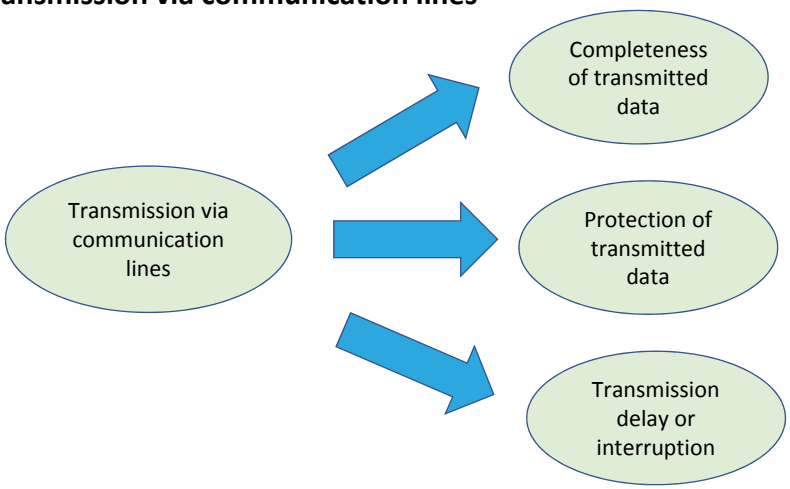
- The stored measurement data shall be protected by software means to guarantee the authenticity, integrity and, if necessary, correctness of the information concerning the time of measurement.
- The software that displays or further processes the measurement data and accompanying data or the measurement result shall check the time of measurement, authenticity, and integrity of the data after having read them from the storage.
- If an irregularity is detected, the data shall be discarded or marked unusable.
- Software modules that prepare data for storing, or that check data after reading are considered part of the legally relevant software.

6.2.4.4 Automatic storing

- measurement data shall be stored automatically when the measurement is concluded, i.e. when the final measurement result used for the legal purpose has been generated.
- The storage device shall have sufficient permanency to ensure that the measurement data are not corrupted under normal storage conditions.
  - There shall be sufficient memory storage for the intended application.
- When the data necessary for the calculation of the measurement result are relevant for legal purposes, all measurement result relevant data included in the calculation shall be automatically stored with the final value.
- Stored data may be deleted if either:
  - the transaction is settled, or
  - these data are printed by a printing device subject to legal control

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

6.2.5 Transmission via communication lines



6.2.5.1 Completeness of transmitted data

- The measurement data stored shall be accompanied by all relevant information necessary for future legally relevant use.

Examples:
A transmitted dataset of the measurement result includes the following entries:

- measured value including unit;
- time stamp of measurement (see 6.1.5);
- place of measurement or identification of the measuring instrument that was
- used for the measurement;
- unambiguous identification of the measurement, e.g. consecutive numbers enabling assignment to values printed on an invoice.

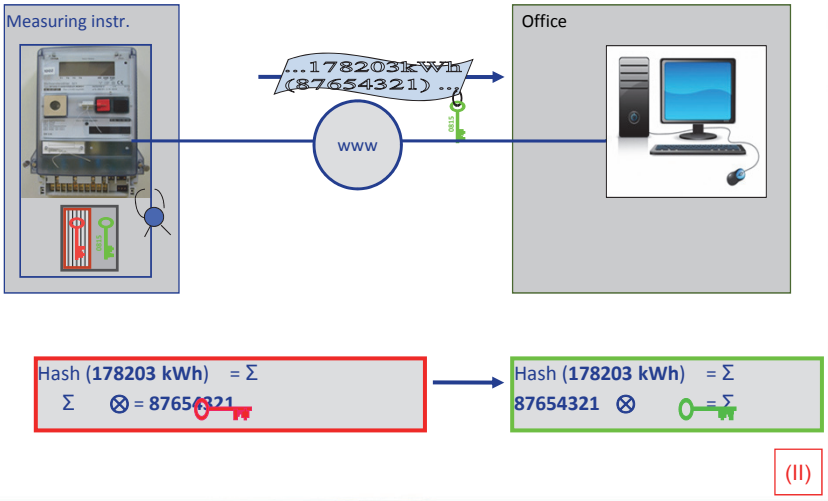
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

6.2.5.2 Protection of transmitted data

- The transmitted data shall be protected by software means to guarantee the authenticity, integrity and, if necessary correctness of the information concerning the time of measurement.
- The software that displays or further processes the measurement data and accompanying data shall check the time of measurement, authenticity, and integrity of the data received from a transmission channel.
- If an irregularity is detected, the data shall be discarded or marked unusable.
- Software modules that prepare measurement data for sending, or that check measurement data after receiving, are considered part of the legally relevant software.

Example

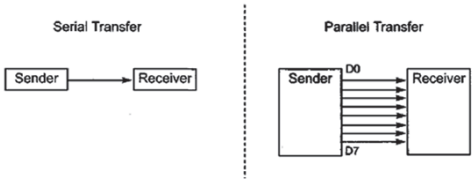
- Public Key System: Secret Key hidden in the measuring instrument
- Approved algorithms for high security: RSA or Elliptic Curves
- Relevant data + signature + public key sent: Integrity verifiable



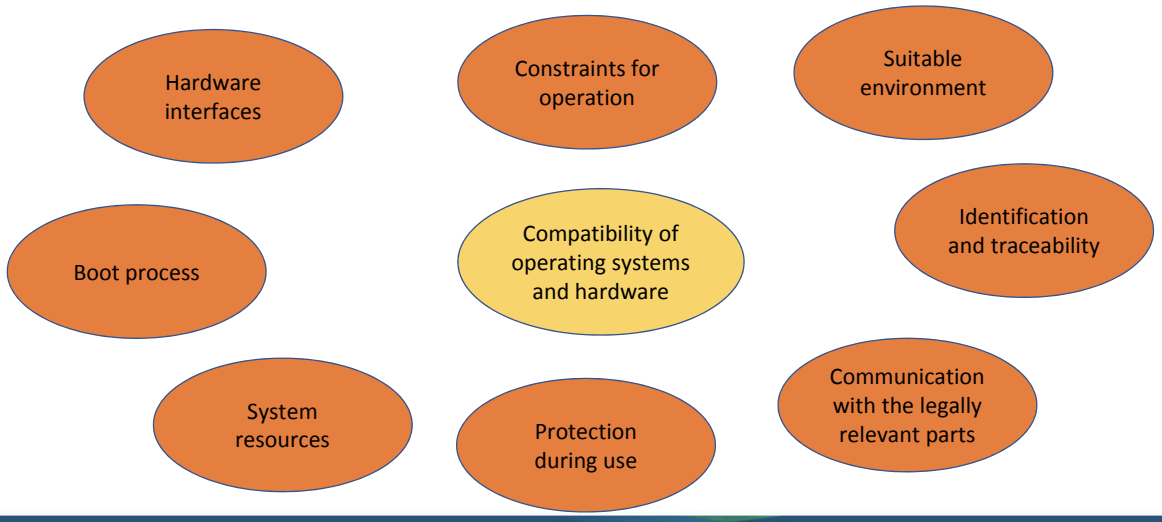
(II)

6.2.5.3 Transmission delay or interruption

- The measurement shall not be inadmissibly influenced by a transmission delay or interruption.
- If network services become unavailable or very slow, no measurement data shall be lost.
- It may be necessary to stop the measurement process to avoid the loss of measurement data.



6.2.6 Compatibility of operating systems and hardware



Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

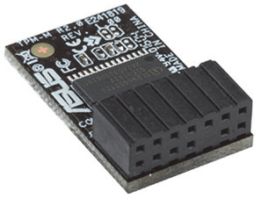
6.2.6.2 Hardware interfaces

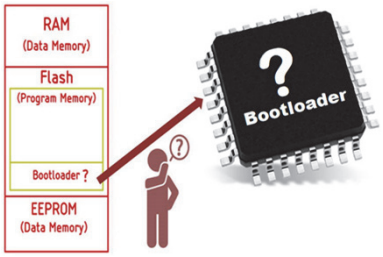
- Hardware interfaces not equipped with a protective software interface shall not be able to inadmissibly influence the legally relevant software part (e.g. by preventing usage of the interface by means of a physical seal).

6.2.6.3 Boot process

- If a secure boot process is needed:
  - To ensure integrity and authenticity of the legally relevant software part, a chain of trust shall be established over the individual components of the boot process.
  - The boot configuration shall be protected against modifications.
  - Booting via open interfaces shall be prohibited.

Examples:
- The boot loader is protected by security means, e.g. a secure password.
- A TPM (trusted platform module)





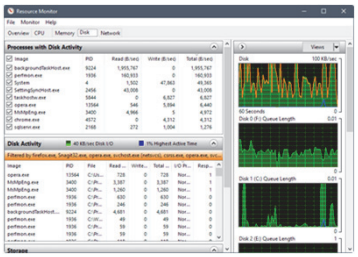
Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

6.2.6.4 System resources

- there are enough resources for the operation of the legally relevant application in combination of both OS and legally relevant software part.

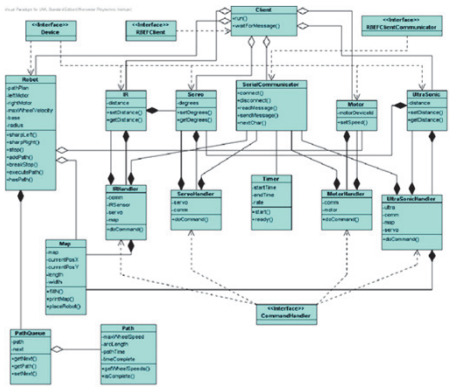
6.2.6.5 Protection during use

- The operation of software that is not legally relevant shall not inadmissibly influence the legally relevant application.
- The combination of the legally relevant software part and the operating system shall ensure that the legally relevant display is distinguishable.
- The access control shall be configured in such way that the intended use cannot be inadmissibly influenced.
- The administration tasks of the legally relevant software part shall be protected



6.2.6.6 Communication with legally relevant software part

- Communication with the legally relevant software part shall be made via protective interfaces.



Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

6.2.6.7 Identification and traceability

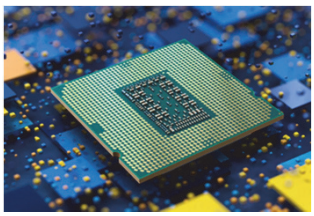
- The configuration of the operating system shall be identifiable. The identifier shall be displayed by the measuring instrument:
  - on command; or
  - during operation.

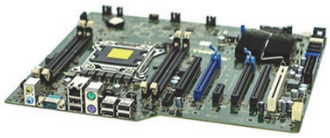
  Examples:
  - On a Windows operating system, the configuration consists of legally relevant:
    - kernel modules
    - list of installed packages
    - libraries
    - accounts and user privileges
    - passwords
    - configuration files
    - file read/write permissions
    - registry keys

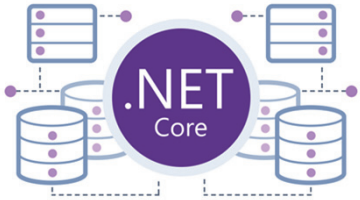
  - Each of the above is identified by means of a checksum

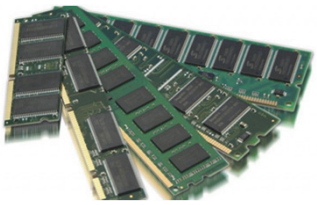
6.2.6.8 Suitable environment

- The manufacturer shall identify the hardware and software environment that is suitable.
- Minimum resources and a suitable configuration (e.g. processor, memory, specific communication, version of operating system, etc.) necessary for correct functioning shall be declared by the manufacturer and stated in the certificate.



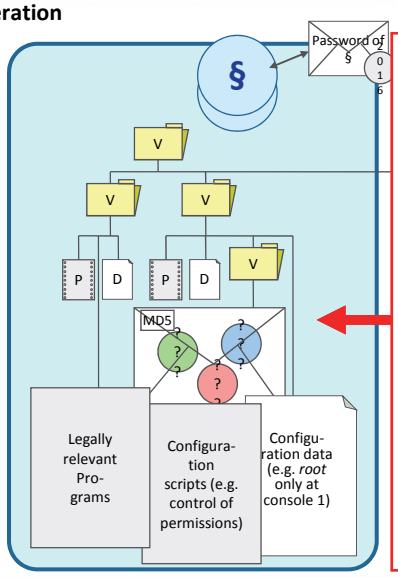






6.2.6.9 Constraints for operation

- Prevent the operation if minimum resources or suitable configuration are not met.
- Fixing hardware, operating system, or system configuration shall be considered in the following cases:
  - High conformity is required
  - Cryptographic algorithms or keys need to be implemented

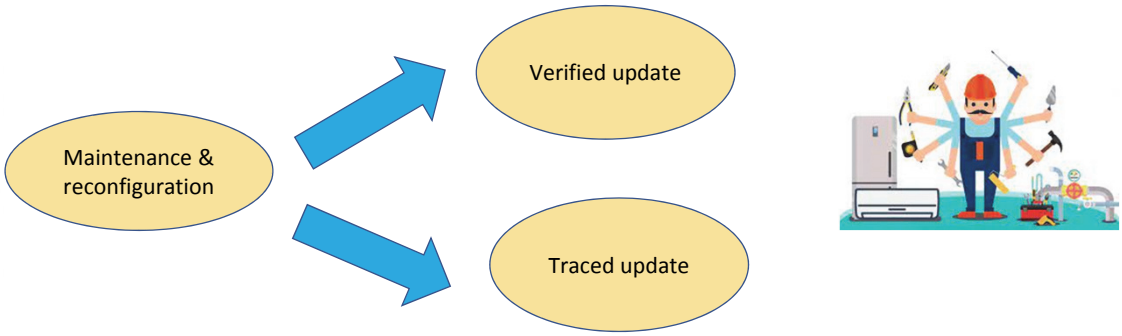


Means to keep environment fixed:

- Separate software
- Make use of the multi-tasking protection means of the operating system: lock the role “admin” or “root”.
- Adjust read-write-execute permissions
- Reduce functionalities of the OS by enabling “Security Policies”
- Reduce functionality: no plug&play interfaces allowed (USB, Firewire, PCMCIA, …)
- Highest protection of LAN interface (Firewall)

6.2.8 Maintenance & reconfiguration

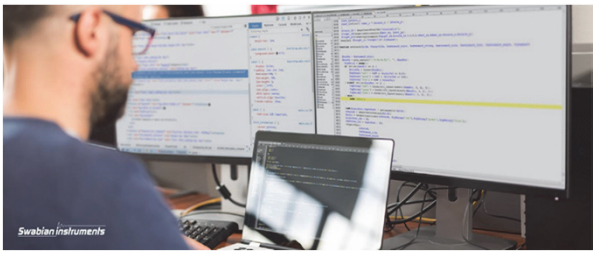
- Updating the legally relevant software part of a measuring instrument in the field should be considered as
  - a modification of the measuring instrument, when exchanging the software with another certified version, or
  - a repair of the measuring instrument, when re-installing the same version.



Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

6.2.8.3 Verified update

- The software to be updated can be loaded locally, i.e. directly on the measuring instrument, or remotely via a network. A seal needs to be broken for the update to take effect.
- A person should be on the installation site of the measuring instrument to check that the updated software has been installed successfully.
- After the update of the legally relevant software part of a measuring instrument (exchange with another certified version or re-installation) the measuring instrument should not be employed for legal purposes before a verification of the measuring instrument has been performed and the securing means have been renewed and the protection means have been reactivated



6.2.8.4 Traced update

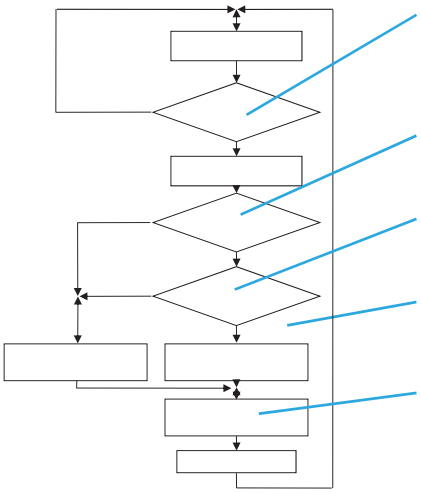
- Traced update is the procedure of changing software in a verified instrument or component after which a subsequent verification is not necessary.
- This means the traced update shall not affect existing parameters.
- The software to be updated can be loaded locally, i.e. directly on the measuring instrument, or remotely via a network.
- The software update is recorded in an audit trail.
- The procedure of a traced update comprises several steps: loading, integrity checking, checking of the origin (authentication), installation, logging and activation.

Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

6.2.8.4 Traced update (continue)

- Traced update of software shall be automatic. If some of the securing or protection measures of the instrument are turned off to enable updating, they shall be turned on again immediately after update, independent of the result of the update process.
- Software shall be protected in such a way that evidence of any intervention shall be available. During an update, any existing audit trail information and event counter value shall be retained.
- Technical means shall be employed to guarantee the authenticity of the loaded software, i.e. that it originates from the owner of the certificate.
- Technical means shall be employed to ensure the integrity of the loaded software, i.e. that it has not been inadmissibly changed before loading. This can be accomplished by adding a checksum or hash code of the loaded software and verifying it during the loading procedure.
- An audit trail shall be employed to ensure that traced updates of the legally relevant software part are adequately traceable within the instrument for subsequent verification and surveillance or inspection.
- If the loaded software fails the integrity test or the authenticity test, the instrument shall discard the new version and use the previous version of the software or switch to an inoperable mode. In this mode, the measuring functions shall be inhibited.

6.2.8.4 Traced update (continue)



- Traced update automatic.
- Control of traced update by fixed software
- Start only with consent of the user

- Guarantee that integrity is OK

- Guarantee that authenticity is OK (origin known and correct)

- Automatic installation. Fall back to old version if installation fails.

- Audit trail of all update activities
- All relevant steps traceable

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

Information to be included in the certificate

- software identification of all certified versions;
- method to display the current software identification on the certified instrument in use;
- securing means as well as means to provide evidence of an intervention and the method to check them (e.g. hardware seals, event counters, audit trails.);
- software modules under legal control;
- if applicable:
  - means of integrity protection checking;
  - Software operating environment

National Metrology Institute of Malaysia
Lot PT 4803, Bandar Baru Salak Tinggi
43900 Sepang, Selangor Malaysia

Dr. Muhammad Azwan Ibrahim
Telephone: 603 8778 1658
E-Mail: mdazwan@sirim.my
www.nmim.gov.my