Organisation Internationale de Métrologie Légale

International Organization of Legal Metrology

COLLATED COMMENTS

Template revision date: 2020-01-10

TC 5/SC 2/p 4:	**Revision of D 31:** ***General requirements for software controlled measuring instruments***		**TC5_SC2_P4_N048**
PG vote/comments on 1CD:	TC5_SC2_P4_N029		
Circulation date:	25-07-2022	Convener: Germany – Marko Esche	
Date comments submitted:			

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China)
2 **Type of comment**: ge = general te = technical ed = editorial

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AT-01				ge	Standards and references documents section should be provided for each chapter		This would be in violation of B 6-2 clause 6.4. Therefore, references should remain in Annex A.
AT-02	1			ge	To delete the definition of intrinsic error (DE-04) is not welcomed. Even if it is only used in fault definition, it leaves the reader with an undefined expression.	Alternatively by the fault definition after the words “intrinsic error” the reference “[OIML V 1:2013, 0.06]” can be added.	Agreed, even if the term is defined in V1, we can copy the definition here for better legibility.
AT-03	1			ge	Throughout the document different spellings of “timestamp” are being used. While all three spellings exist (“timestamp”, “time stamp” and “time-stamp”) we are in favour of the term “timestamp”	Change “time stamp” and time-stamp” to “timestamp”	OK. This will be corrected to “timestamp” as used in the Oxford Dictionary.
AT-04	1			Ge	Consider restructuring the document	A Technical Framework (in the Appendix) with use cases, user stories at different stakeholders/(primary/secondary) actors‘ levels with the necessary UML diagrams and functional description would be more beneficial than to list those within the document	OIML D31 is an OIML Document purely intended to be used by OIML PGs when drafting OIML recommendations. Therefore, the envisioned “user stories” and UML diagrams do not really serve a purpose within the document. Moreover, such complete restructuring was rejected during the first PG meeting, see discussion of DE-01 on 1WD. Nevertheless, this could be discussed within the frame of a future revision. At the PG meeting, it was proposed group choices to be made by PGs implementing D31 into a new clause within the frame of the next revision.
AT-05	1	3.2.52		ed	Check grammar	trail of the evolution of dynamic parameters of a module evolution of dynamic parameters of a module	For the evolution of dynamic parameters, a definite article does not seem to be required. The second change will be implemented.
AT-06	1	4.3		te	Reference to relevant documents seems to be missing	When mentioning risk assessment level, a reference to a later chapter (done) or relevant document (recommended security level: ISO/IEC 16085:2021 and DIN EN 62304) should be given here.	As clause 4.3 only serves as a very general overview and details are given immediately in the referenced clause 5, no addition seems to be needed. Moreover, security levels in D31 are only provided on an exemplary basis and separately for each requirement since PGs may decide not to follow one of the two levels at all, but to select their own level per requirement.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AT-07	1	4.4		te	Harmonized standards are missing	there are harmonized standards with respect to software security that should be mentioned here.	There seems to be a misunderstanding here. Clause 4.4 is a general instruction to decide which influence on the software functionality e.g., setting of parameters, modification of log entries, is allowed. If harmonized standards are missing in this aspect, please suggest adequate references.
AT-08	1	4.5		te	too much room for interpretation	Reference to upcoming guidelines with respect to machine readability (e.g. 1448/DCC) would be of benefit in future. PTB is currently evaluating relevant administrative/legal data for this project - first version of administrative part available. Here it doesn't benefit harmonization or intended modularization when too much room for interpretation is given to PGs at a later stage. This would again cause more complex pre-assessments with respect to quality assurance.	D31 as an OIML Document cannot reference guidelines that have not yet been officially published by another standardization body. D31 by definition cannot prescribe which data (or metadata) are to be considered legally relevant by individual PGs since this is outside its scope, see B6-1 clause 3.3. B6-1 clarifies that any OIML Document is intended as an aide to writing normative documents but does not constitute a normative document itself.
AT-09	1	4.6		te	too much room for interpretation	Same issue as in 4.5	See above. Additionally, only instrument-specific PGs can decide on the relevance of instrument-specific parameters.
AT-10	1	5.1		te	A recommendation of harmonized standards would be more preferable here rather than giving an abstract range of "options"	Give a recommendation according to harmonized standards	During the previous revision (see documents of TC5/SC2/p3), it was decided to leave the choice of the risk assessment methodology up to the relevant PG, since many different standards exist in this field. If there is a need to revised this decision (for which TC5/SC2/p4 currently has no mandate), this should be discussed within the frame of another revision. At the PG meeting, it was agreed that additional guidance on risk assessment is not needed since TCs and SCs have already decided on the appropriate risk classes for their instruments.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AT-11	1	6.2.1		te	With transmission of measurement data, the software identification should always be provided		Clause 6.2.1 does not address transmission of measurement data. If such a requirement to transmit the software identification is needed, it should be inserted in clause 6.3.5. As 6.3.5 already requires completeness of transmitted datasets, this should already be implicitly covered. Since software identification may not change at all for some instruments, modification of the existing example in 6.3.5.2 does not appear to be needed.
AT-12	1	6.2.1	4	ed	Check Spelling	measuring instrument	OK, this will be corrected.
AT-13	1	6.2.1 c		te	This cannot be seen as a realistic implementation into a regulation, because firmware update, such as other updates are needed on regularly basis and would hinder improvements/adaptations of post-market surveillance. Redundancy: every update comes with new versioning; hence a new software identification is given.		In fact, the situation described in point c) is the norm for many instruments in legal metrology world-wide e.g., many utility meters. Therefore, the option should be kept.
AT-14	1	6.2.1 c	5	te	Which certificate?	Please insert a reference here.	See clause 3.1, “Unless stated otherwise, the term certificate refers to the OIML type examination certificate.” Therefore, no change is needed.
AT-15	1	6.2.2		te	In this chapter It might be useful to introduce internationally recognized software testing, validation and verification principles such as those given by the ISTQB Foundation		As ISTQB is not an international standardization body but makes reference to ISO standards etc. in its syllabus, D31 cannot reference ISTQB publications. Instead, proposals should be made to explicitly reference international standards where needed. Since these are already given in clause 7.3, no change appears to be needed here.
AT-16	1	6.2.3.1			Reference on how to properly document a software's life cycle development should be mentioned here		Software lifecycle management usually covers aspects including planning, development, maintenance etc. These do not appear to fall under clause 6.2.3.1 which only addresses providing evidence in case of an intervention.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AT-17	1	6.2.4 & 6.2.5			Chapters could be put together; in this chapter related recommendations such as Multi Criteria Decision Analysis could be useful.		During the previous PG meeting, it was decided to establish a separate requirement on demands on the user (see Nl-039 on 1WD). If aspects from MCDA can be applied in this context they should be included in clause 7.3 regarding the actual software examination. 6.2.4 and 6.2.5 only impose relatively simple requirements on the software which should be easy to follow.
AT-18	1	6.2.6.1			Are we talking about testing processes or providing a service manual here?	Clarify at which point of the software development life cycle process these 'detection functions' are acting	D31 only imposes requirements on certified instruments operated in the field. Therefore, no such clarification appears to be needed.
AT-19	1	6.2.6.2		ed	check wording	The relevant Recommendation may require detection functions for durability errors and specify when and/or in which timeframe a check shall be carried out.	Since “at what time” is a valid English expression and also highlights the need to specify a point in time, we can keep it.
AT-20	1	6.2.6.3		ed	Check comma	If support of 6.2.6.1 or 6.2.6.2 is part of the remote verification procedure, it shall be possible to transmit data containing information in this respect to the verification software.	Agreed.
AT-21	1	6.2.7		te	Timestamp format not defined	Define timestamp format (preferably standardized time stamp format; e.g. according to ISO 8601 and RFC 3339)	B6-1 clarifies that D31 as an OIML Document is intended as an aide to writing normative documents but does not constitute a normative document itself. Therefore, D31 cannot prescribe a timestamp format to be used in other recommendations. This is intentionally left up to the relevant PG. In fact, the proposed ISO standard is already mentioned in the example for clause 6.2.7.
AT-22	1	6.2.7		ed	Consider editing both paragraphs	The time stamp shall be in a consistent format, allowing for easy comparison of two records and tracking progress over time. If a measuring instrument uses timestamps, the instrument shall contain an internal clock which shall be used to create the timestamp. 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 (see 6.2.3.4). Automatic setting of the time shall only be possible if legal time is used as a time base in an authenticated manner. If an internal clock is synchronized with legal time, the synchronization method and traceability to legal time shall be described, see 7.1.2.	OK

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AT-23	1	6.3.2.1.2		te	Protective interface - What are the minimum requirements regarding hash functions? MD5-6? SHA2-3?		It is unclear how hash functions pertain to clause 6.3.2.1.2 on protective interfaces.
AT-24	1	7.1.2	bullet point 18	ed	Check spelling	a description of the means to validate the conformity of devices in use even in the presence of dynamic parameter changes; detailed description of the dynamic module's algorithm design as well as a description of the training process and the used training datasets	OK. The spelling will be corrected.
AT-25	1	7.1 – 7.4		te	ISTQB provides state of the art guidelines (functional testing, code inspection, module testing, data flow assessments etc.) which should be considered here or e.g. as minimum requirements to follow		As ISTQB is not an international standardization body but makes reference to ISO standards etc. in its syllabus, D31 cannot reference ISTQB publications. Instead, proposals should be made to explicitly reference international standards where needed. If existing references to international standards in clauses 7.1 to 7.4 need to be updated, please specify them explicitly.
AT-26	1	8.3.3.1 + 8.3.5.1		ed	Check spelling/grammar	The purpose of this remote verification procedure is to check a measuring instrument's operational history. For that purpose, it is necessary to establish first the authenticity of the measuring instrument and its integrity. After the authenticity and integrity have been established, retrieval of the relevant test items is initiated.	Agreed.
AT-27	1	8.3.3.2		ed	Check punctuation	A reference for all legally relevant software (measuring instrument software) shall be made available to the relevant authorities, including approved type, serial number, legally relevant settings and parameters, verification information and status, software version identification, software integrity, audit logs/trails, change logs, event logs, etc. depending on national legislation.	OK
AT-28	1	8.3.6.3		ed	Check wording	Initiate procedure using a build-in diagnostics facility to establish whether the current performance of a flow meter has degraded since the last calibration and whether a recalibration is needed.	OK
AT-29	1	8.3.6.4		ed	Check grammar	Simulating a digital sensor and sending intermediate measuring results to the Digital Data Processing Unit and retrieving the measurement result to evaluate the accuracy of the measurement algorithms in the Digital Data Processing Unit.	OK

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AT-30	1	6.2.7 Page 73	(table)	ed	Check wording	The timestamp shall be in a consistent format, allowing for easy comparison of two records and tracking progress over time. If a measuring instrument uses timestamps, the instrument shall contain an internal clock to create the timestamp. Setting the clock may be legally relevant depending on the kind of instrument or the field of application. , Protection according to the risk level shall be applied. Automatic setting of the time shall only be possible if legal time is used as a time base in an authenticated manner.	OK, these seem to be copy&paste errors from the previous revision. The entry will be amended in accordance with changes resulting from AT-22.
AU-01	1	3.1	Note	ed	The reference to OIML certificates should be aligned to the terminology from OIML B 18. An alternative approach could be to directly implement throughout the Document the terms from OIML B 18 “OIML Certificate” and “OIML type evaluation report” as relevant.	Please amend the Note as follows: “Unless stated otherwise, the term certificate refers to the OIML certificate.”	Agreed, we should follow the official OIML terminology.
AU-02	1	3.2.14		ge	It may be useful for new readers to include a Note that explains that this definition covers concepts of machine learning or AI within a legal metrology context.	Suggest the following Note: Such dynamic modules may be considered to incorporate or utilise machine learning or artificial intelligence characteristics and processes.	Agreed, this may help new readers to visualize a possible application of such dynamic modules.
AU-03	1	3.2.35 +		ge	Consideration should be given to the need for the ‘metadata’ terms. None are used on the body of the document. They are only used in the terminology section and Annex C. As such, could we not simply rely upon the conventional meaning of metadata as applied and used in the document? The same is true for some of the ‘data’ terms. Please review their use in the body of the draft.		This should be discussed at the PG meeting. After discussion at the PG meeting, it was agreed to keep the metadata definitions. PGs do not need to copy all of D31 into their respective recommendation. Having the definitions in D31 for clarification is considered helpful.
AU-04	1	3.2.48		ge	The term ‘during use’ could be interpreted as during a measurement process. However I believe we mean during in-service use.	Consider change to “during service” or similar.	V1 appears to use the term “use” in the same sense as 3.2.48 (see V1 clause 6.02). Therefore, we should keep the term.
AU-05	1	3.2.49		te	Suggest that the word “unauthorised” be retained in the definition. There are many examples of sealing devices that allow authorised modification of a measuring instrument. Such as the examples provided in 3.2.58.	Suggest that the definition retain the word “unauthorised”.	3.2.58 does not appear to differentiate between “authorized” and “unauthorized” access. Moreover, sealing should cover both aspects.
AU-06	1	3.2.61		ed	It may be possible to shorten this definition to “device used for storing measurement data” as the definition of measurement data already includes all measurement process data and measurement result data. But this logical may need to be checked.	Possibly amend as follows: “device used for storing measurement data”	This would contradict comment NL-031 to 1WD where it was argued that only data necessary to construct (any part) of the measurement result must be stored.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AU-07	1	4.5		ge	Suggest amending the second sentence to place responsibility on the PG responsible for the development/revision of the relevant Recommendation. OIML D 31 is not intended to place requirements/obligations on manufacturers.	Suggest the second sentence is amended as follows: "PGs shall also decide which metadata is to be documented and recorded as part of the type evaluation."	Indeed, D31 should not impose requirements on the manufacturer directly. Nevertheless, PGs may decide to do so in the relevant Recommendation. Suggestion to rephrase to: "PGs shall also decide which metadata shall be documented by the manufacturer."
AU-08	1	6.3.7	Note	ed	Editorial change to Note 1: "…even in ***the*** presence of dynamic parameter changes…"	Editorial change to Note 1: "…even in the presence of dynamic parameter changes…"	Agreed.
AU-09	1	6.3.8.1		ge	Suggest adding a clarifying Note to remind readers that these requirements apply to dynamic modules of legally relevant software.	E.g. "The requirements of this clause apply generally, including to dynamic modules of legally relevant software."	In fact, SG1 decided to interpret changes of an AI primarily as parameter modifications which would not fall under the mentioned clause. Since the clause applies to all kinds legally relevant software, anyway, the proposed note might only cause confusion.
AU-10	1	6.3.8.1		ge	Include a requirement that clarifies the resource priority of the update compared with measurement processes. Some instruments may be in continuous use (making continuous measurements), as such utility meters. In this case does an update take precedence over an ongoing measurement process?	Suggestion: "It shall either: Not be possible to commence a measurement process once an update process has commenced; or Uninterruptable measurement processes shall take precedence over update processes with respect to system resources." For discussion within the PG?	This would be in line with clause 6.3.9.1.6. Nevertheless, this should be briefly discussed with the entire PG. Revised proposal from the meeting: An update shall not inadmissibly influence the measurement process.
AU-11	1	6.3.9.1	Note	ed	The Note contains requirements and should be moved into the body of the clause.	The Note contains requirements and should be moved into the body of the clause.	Since the requirements in the note do not pertain to the software itself, they should be kept as a note. After discussion, the PG decided to split the note as follows: There shall be a description of the remote verification procedure for accessing/reading of remote verification data and for executing remote verification procedures, see clause 7.1.2. Note: The description shall be made available to the relevant authorities depending on national legislation.
AU-12	1	6.3.9.1.7		ed	The first dot point should say "battery life".	The first dot point should say "battery life".	Agreed.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AU-13	1	6.3.9.1.12	Note 2	ed	The Note contains requirements and should be moved into the body of the clause. Also the requirement should be rephrased to place the obligation on the PGs draft appropriate requirements	Move the Note to the clause and rephrase to place obligation on PGs to draft appropriate requirements.	Agreed. This would be in line with AU-07, too.
BR-01	1	3.2.9		te	The definition of a certificate misses the essential feature of a digital certificate: to bind an identity to a public key.	**cryptographic certificate** A dataset containing the public key belonging to a measuring instrument or a person plus a unique identification of the subject, e.g., serial number of the measuring instrument or name or Personal Identification Number (PIN) of the person, plus date of expiry, plus a trusted party signature, thereby binding the public key to the unique identification of the subject.	Agree. Since definitions should not provide explanations, however, the last proposed subclause should be moved to a note.
BR-02	1	3.2.10		ed	We suggest writing the definition in parallel form, using the security properties by their names and not by definition.	**cryptographic means** means such as encryption and decryption with the purpose of confidentiality, or hashes and signatures (see 3.2.1) to ensure integrity and authenticity	Indeed, the proposed modification aligns integrity, authenticity and confidentiality better. Suggestion to rephrase to "…with the purpose of providing confidentiality" for better legibility. The reference to 3.2.16 will be kept.
BR-03	1	3.2.16		te	Replace the term with a more commonly used: digital signature (sometimes people use electronic signature for other meaning: https://www.linkedin.com/pulse/what-difference-between-digital-signatures-electronic-mutabazi/). Also, add a note about nonrepudiation property provided by digital signature.	**digital signature** software means which is added to software or data with the purpose to verify the origin of software or data, i.e., to prove their authenticity, or to check that the software or data are unchanged, i.e,. to prove their integrity *Note 1:* For digital signing, a public key system is used in general, i.e. a pair of keys where only one needs to be kept private/secret; the other may be public. *Note 2:* The private key is used when software or data are secured. The public key is used when software or data are verified before use. *Note 3:* The verifying instance may require a cryptographic certificate of the securing instance (see 3.2.93.2.93.2.83.1.7) to be sure of the authenticity of the public key. *Note 4:* A digital signature provides nonrepudiation: the signer cannot deny signing the software or data.	Agreed. The reference to 3.2.16 will be kept.
BR-04	1	3.2.22		ge	The term fault has a another meaning for reliability and security community. Maybe a clarification could be useful.	*Note 1: The term fault here is used as in the VIML. Should not be confused with software fault (refs: https://ieeexplore.ieee.org/document/693776; https://link.springer.com/content/pdf/10.1007/978-1-4020-8157-6_13.pdf)*	Since all terms in this OIML Document are used in the sense of V1 and V2, mentioning this explicitly here, would not add any value.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
BR-05	1	3.2.23		te	The current definition does not cover cryptographic hash function properties, and in several places in D31, a cryptographic hash function is necessary.	*Note 2: cryptographic hash function has three additional properties: collision-resistant, preimage resistant, and second preimage resistant.*	Agreed. The proposed note will be added as follows: "A cryptographic hash function has three additional properties: collision-resistance, preimage resistance, and second preimage resistance"
BR-06	1	3.2.39		ge	Which data definition should we use to clearly understand item 3.2.39? Is it measurement data or measurement process data?		The definition refers to measurement result relevant data, see note 1.
BR-07	1	6.2.1		te/ed	Calculating a checksum over its memory (Case II), without any external challenge, does not increase security compared with a textual string (Case I). We suggest removing example II from this item and adding a device/remote attestation example on the Remote Verification item 6.3.9.		Since the concern of 6.2.1 is software identification (which is up to the manufacturer anyway) rather than software integrity, an external challenge does not appear to be needed. Suggestions for a better example for risk level II would be welcome. The PG decided to keep the convener's proposed response. This could be addressed in a future revision.
BR-08	1	6.2.3.1		ed	Example 4 explains how a neural network keeps track of its updates by logging a checksum of its weights in an audit log. This looks like a dynamic identification of the legally controlled neural network. We propose moving this example to item 6.2.1 (software identification) as a minor suggestion.		It was the consensus of SG1 to interpret changes to a neural network as parameter modifications. Therefore, the example should stay in place.
BR-09	1	6.2.3		ed	Item 6.2.3 covers too many topics in one item. We suggest group subitems of 6.2.3 in different items as follows: 6.2.3.2 and 6.2.3.3 grouped in Protection of user interface and Input; 6.2.3.4 and 6.2.3.5 grouped in Protection of software and legally relevant parameters; 6.2.3.6 protection of audit trails and event counters. 6.2.3.1 stay as it is.		Such a restructuring was rejected during the first PG meeting, see discussion of DE-01 on 1WD. Nevertheless, this could be discussed within the frame of a future revision. There was consensus during the PG meeting to address the issue during the next revision.
BR-10	1	6.2.4		ed	The sentence "Legally relevant software shall be secure against accidental or unintentional changes" is hanging and repeating the same idea of the first sentence. We suggest removing it.		The sentence addresses accidental or unintentional changes as opposed to accidental or unintentional misuse addressed in the first sentence. Nevertheless, the sentence will probably be moved to a separate clause in the future, see also response to BR-09.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
BR-11	1	6.2.4		ed	The sentence “The presentation of the measurement results shall be unambiguous for all parties affected” is hanging after the examples. We suggest moving to be after the first paragraph as a one-sentence paragraph.		The sentence will probably be moved to a separate clause in the future, see also response to BR-09. For the time being it should be kept together with the previous sentence on accidental or unintentional changes
BR-12	1	6.3.2.1.3		te	Please, replace RC4 with any other secure symmetric encryption algorithm such as AES (although it is not a stream cipher, it is suitable for the particular example). RC4 has been removed from TLS as stated by RFC 7465 due to several attacks.		Even though attacks on RC4 are known, it might still be sufficient for risk level I. This should be discussed with the entire group. At the meeting, it was decided to implement the solution from UK-07.
BR-13	1	6.3.4.3		ge	Example 2 suggests the public key's presentation on the display of the measuring instrument. A public key could be a colossal hexadecimal number hard for humans to read. We suggest the key fingerprint to be used instead.		OK
BR-14	1	6.3.6.5		ge	The term administration task could be defined in section 3.2 instead be defined in the note.		As the note does not act as a definition of the term, but as an explanation of the requirement, it should be kept in place.
BR-15	1	6.3.8.4.8		Te	Usually, audit trails are circular lists with limited memory space (a few hundreds of events in built-for-purpose instruments). An attacker could easily overload the audit trail of traced updates if all failures attempts are logged. We suggest only logging successful updates on built-for-purpose instruments.		6.3.8.4.9 ensures that such a circular list with an automatic override cannot fulfil the requirement without additional protective measures. Since logging of unsuccessful downloads was already required in D31 :2019, we should not change this here. 6.3.8.4.8 currently contradicts 6.3.8.4.9. Since 6.3.8.4.9 allows for more solutions other than making downloads impossible (which should be defined by the respective PGs) we propose to delete the sentence from 6.3.8.4.8 entirely. To clarify this, we will add a note : “Note: PGs need to define an appropriate reaction”

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
BR-16	1	6.3.9		Te	An example of software integrity verification via software remote attestation (see comment on item 6.2.1).	(I) The instrument engages with a verifier in software remote attestation protocol. The instrument receives a random challenge from the verifier, calculates a checksum of the executable code concatenated with the challenge, and presents the result. The verifier, which has access to the code, can perform the same computation and check if the response is valid or not.	Such an example should be placed in clause 8.3, unless there are additional requirements on the instrument itself that need to be fulfilled to enable this verification procedure. This should be briefly discussed with the entire PG. The PG decided to include this in 6.3.9.1.2. as a level II solution. It will be modified to use a rainbow table instead of access to the code.
BR-17	1	7.3.2.3		ge	The complementary procedures state that it is not possible to detect unauthorized commands. First, it is unclear if unauthorized is used as a synonym for undocumented. For extended examination, software analysis should be combined with the functional test to detect unauthorized/undocumented commands.	For the extended examination level, a software analysis such as 7.3.2.4 or 7.3.2.5 is necessary and should be combined with 7.3.2.2 in search of unauthorized commands (e.g., debug interface accidentally enabled).	Agreed. The term “unauthorized” does indeed seem to mean “undocumented”. Before adding the proposed sentence, we should briefly consult with the entire PG. This was agreed upon at the meeting.
BR-18	1	Annex B		te	We suggest that the test report brings the cryptographic hash of each file analyzed (source files, documentation files, and binaries) or the cryptographic hash function of a compressed file that includes all analyzed files.		OK
CA-01		3.2		Remark	A definition for ‘operating system” should be provided		Agreed.
CA-02		3.2.4.7			The term ‘Protective interface’ is defined but another term “protective software interface” is used in clause 6.3.2.2.3,	Remove ‘software” from “protective software interface”	Since a protective interface is defined as a software module, the term “protective software interface” is indeed redundant.
CA-03		3.2.45			The term “mobile app” is defined however only the term “app” is used in the document.	Remove “mobile” from “mobile app"	The term will be discussed with the entire PG, see also response to CZ-05. The PG decided that we will use “mobile app” consistently to avoid confusion with apps on other platforms.
CA-04		6.2		Ed	This paragraph below does not add any new information as compared with clause 6.1 At the time of publishing this Document, the general requirements represent the state of the art in information technology (IT). They are in principle applicable to all kinds of software-controlled measuring instruments and components of measuring instruments. They should be considered in all Recommendations. In contrast to these general requirements, the requirements specific for configurations (6.36.36.36.2) deal with technical features that are not common for some kinds of instruments or in some areas of application.	Suggest to delete test in 6.2: At the time of publishing this Document, the general requirements represent the state of the art in information technology (IT). They are in principle applicable to all kinds of software-controlled measuring instruments and components of measuring instruments. They should be considered in all Recommendations. In contrast to these general requirements, the requirements specific for configurations (6.36.36.36.2) deal with technical features that are not common for some kinds of instruments or in some areas of application.	A general housekeeping update of D31 was rejected for this revision, see discussion of DE-01 on 1WD. Nevertheless, this could be discussed within the frame of a future revision.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
CA-05		6.2.1		Ed	Software modules of a measuring instrument/ or component shall be unambiguously identified. Suggest to add uniquely to this clause.	Software modules of a measuring instrument/ or component shall be unambiguously and uniquely identified.	Agreed.
CA-06		6.2.7			The term 'legal time" is not defined. Is it up to national jurisdictions to determine what is legal? If so, perhaps it should be stated.		Agreed, we can add a note to specify what "legal time" refers to.
CA-07		6.3.8		Ed	The term "Verified update" seems peculiar for the application. The two words together suggest an update has been verified but actually for the described condition a verification/examination is still required after the update has occurred. It seems that if a an update necessitates verification the more appropriate term would be "unverified update"	Change "Verified update" to "Update requiring verification"	Agreed. Nevertheless, this should be briefly discussed with the entire PG. At the meeting, there was consensus to keep the current title.
CECIP-01				ed	No chapter numbers available	Add chapter numbers	The comment seems to be referring to the first version of 1CD uploaded in error to the OIML website by BIML on 2021-10-08. It was immediately afterwards replaced by a pdf-Version that contains all clause numbers etc. The version is still available from the OIML website.
CECIP-02		3.2.6 Page 7		te	Definition cloud: Please note that a cloud may be accessible over the internet. But it may be also a company internal network not connected to the internet.	Add company network to the definition	OK, we should use the term "Internet or another network" here to allow for such a situation.
CECIP-03		3.2.55 Page 14		te	Definition of "software identification": In times of digitalization and virtual instruments a software -ID may also be a codes information that cannot be read by a human. Therefore "readable" shall mean "by human or by machine".	Add clarification on readable. Working group should discuss.	Ultimately, such information should still be readable for humans, even if they are rendered as lengthy codes. Therefore, no change is needed.
CECIP-04		3.2.61 Page 15		te	Definition of "storage device": This definition is not too easy to understand. (measurement data construct the measurement result?)	Could this be clarified? Working group should discuss	The term is well aligned both with the rest of the terminology clause and Annex C. Nevertheless, if there is still time at the PG meeting, this could be discussed. The PG decided to add a note to clarify that an explanation may be found in Annex C.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
CECIP-05		5 Page 18 Risk assess-ment	e)	ge	When selecting risk levels for a particular category of instruments and area of application (trade, direct selling to the public, health, law enforcement, etc.), the following aspects can be taken into account: a) … b) … c) … d) … e) the possibility to repeat a measurement or to interrupt it. Add item f) because, the weight of a product can be determined at later point of time with another scale again. This is not possible e.g. in case of a water or gas meter. Therefore a scale has a lower risk level compared to a water or gas meter.	When selecting risk levels for a particular category of instruments and area of application (trade, direct selling to the public, health, law enforcement, etc.), the following aspects can be taken into account: a) b) c) d) e) the possibility to repeat a measurement or to interrupt it. f) The possibility of verifying the measurement at a later point in time.	Agreed, but we should use the phrase "checking the measurement at a later point", instead.
CECIP-06		6.2.1 Page 19 Software identific-ation		ge	If a measuring instrument or component has neither display nor printer or if the instrument facilitates remote verification, the identification shall be sent via a communication interface, in order to be displayed/printed on another component or by the **verification software.** The term „verification software" is not defined in the document.	Please define the term „verification software" in the chapter "terms and definitions". Working group should discuss.	This should be solved by the solution proposed in response to JP-16. Nevertheless, we should rephrase the clause to make sure that the verification software is not the only way of visualizing the software identification. Proposal to replace the part "or by the verification software" with "If the instrument facilitates remote verification, the software identification shall also be sent to the verification software."
CECIP-07		6.2.3.2 Page 22 Evidence and prevention of intervention		te	All inputs from the user interface shall be handled by a protective interface. Any function that can be activated by the user interface shall: - be clearly documented (see 7.1.2) Problem, caused by the sentence above: This would make a software separation pointless, since every extension in the non-legally relevant software would require an extension in the legally relevant software.	All legally relevant inputs from the user interface shall be handled by a protective interface and shall be clearly documented (see 7.1.2). Any function that can be activated by the user interface shall not be able to influence the legally relevant characteristics of the instrument.	The respective phrase has been part of D31 since its original 2008 edition. As all clauses only ever impose restrictions on legally relevant software/parameters/data, there is no need to modify the proposed clause. If there is sufficient time at the PG meeting, we can discuss if this needs to be highlighted here. At the meeting, it was decided that the current phrasing is clear enough.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
CECIP-08		6.2.3.3 Page 23 Evidence and prevention of intervention		te	All inputs from communication interfaces shall be handled by a protective interface. Any function that can be activated through a communication interface shall: - be clearly documented (see 7.1.2) Problem, caused by sentence above: This would make a software separation pointless, since every extension in the non-legally relevant software would require an extension in the legally relevant software.	All legally relevant inputs from the communication interface shall be handled by a protective interface and shall be clearly documented (see 7.1.2) Any function that can be activated by the communication interface shall not be able to influence the legally relevant characteristics of the instrument.	The respective phrase has been part of D31 since its original 2008 edition. As all clauses only ever impose restrictions on legally relevant software/parameters/data, there is no need to modify the proposed clause. If there is sufficient time at the PG meeting, we can discuss if this needs to be highlighted here. At the meeting, it was decided that the current phrasing is clear enough.
CECIP-09		6.3.6.3.4 Page 41 Boot Process		te	The boot configuration shall be secured and protected. Examples: The sealed housing of the measuring instrument together with the protection of all open interfaces ensures that the boot configuration can only be modified after a seal has been broken, Problem, caused by the sentence above: A sealing of the boot-configuration is not possible by using standard hardware. Bios-configuration is secured by password. The following sentence must remain. The boot loader is protected by security means, e.g. a secure password.	The boot configuration shall be secured and protected. Examples: The boot loader is protected by security means, e.g. a secure password or sealed housing.	The secure password has the issue that it must be kept secret unless a seal is broken. Sealing a random password inside the housing appears to be a valid implementation of the current clause. We should briefly discuss this with the entire PG before adding it as another example. Modified proposal from the PG meeting: The boot loader is protected by a password which is sealed inside the housing of the instrument. The sealed housing together with the protection of all open interfaces ensures that the boot configuration can only be modified after a seal has been broken.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
CECIP-10		6.3.6.7.2 Page 43 Identifica-tion and traceability		te	Example: (I)/(II) All changes to the operating system configuration are logged in an audit trail. Each entry of the audit trail contains a time stamp of the modification as well as the identifier of the new configuration. **The module in charge of maintaining the audit trail and protecting it against modification serves as a trust anchor and is not updated itself, see** 6.3.8.4.4. Problem, caused by the sentence above: This conflicts with the requirement that certificates used to verify integrity and authenticity must have a limited lifetime from an IT-security point of view. It must therefore be possible for the existing anchor point software to verify the new anchor point software.	Example: (I)/(II) All changes to the operating system configuration are logged in an audit trail. Each entry of the audit trail contains a time stamp of the modification as well as the identifier of the new configuration. The module responsible for maintaining the audit trail and protecting against changes serves as an anchor of trust. If this module is to be changed, the existing module must make a separate entry in the audit trail before the new module is installed.	The given argument is technically incorrect. If limited lifetime of certificates is an issue, updated certificates can simply be downloaded to the instrument. Since the addressed sentence is part of an informative example, there is no need to modify the download manager for this.
CECIP-11		7.3.2.2 Page 63		te	Preconditions: In addition, the services of the programmer should be made available to the examiner for the purposes of answering questions. It is not possible to make the programmer available for questions of the examiner.	Proposal to delete the requirement	This procedure is commonly used in code inspection worldwide. Since this is a “should” requirement which only serves as a backup solution, we can keep it in place.
CECIP-12		8.1 Page 67		te	Verification of a measuring instrument General: an examination of the inputs/outputs of the measuring instrument to verify that they are free of unwanted side effects inadmissible influence Checking the functionality of all present I/O ports is very time consuming and may not be a subject of a verification. This is subject to type examination only.	Remove from the chapter on verification	Even if the procedure is time consuming, it should still be an option for verification bodies.
CECIP-13				ge	Possibly not for this group, but it would be helpful to generate a list of differences between D31 and WELMEC Guide 7.2 There are several additions in comparison to guide 7.2.		Such a difference analysis is no task for TC5/SC2/p4 and should be made by the responsible RMO i.e., WELMEC.
CH-01	1	Annex C	1	Ed	Wrong quote for Measurement Result, according to current terminology section (3.2.39).	Change to correct quote: "set of quantity values being attributed to a measurand together with any other available relevant data"	This is a copy&paste error from 1WD and will be corrected.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
CH-02	1	Annex C	1	Ed	Rephrasing of the first paragraph, including suggested correction in CH-1.	Rephrase to: "In this Document, the definition of Measurement Result (3.2.39) is “a set of quantity values being attributed to a measurand together with any other relevant data”, (i.e., Measurement Result Relevant Data). This is illustrated in Figure A.1, as the Measured Quantity Value (MQV) and the Measurement Result Relevant Data (MRRD), both being part of the Measurement Result (MR)."	The rephrased version appears to be much clearer and will be implemented.
CH-03	1	Annex C	2	Ed	Rephrasing of the second paragraph.	Rephrase to: "Together with the Measurement Process Data (MPD), these form the Measurement Data."	OK
CH-04	1	Annex C	6	Ed	Related to the description of Figure A.2: Removal of unnecessary "-".	Change from "Figure A.2. – Also indicates" to "Figure A.2 also indicates	The formatting error will be corrected. This looks like a copy&paste error from the figure caption.
CZ-01	1	Contents		Ed	The content of sections 6.2 and 6.3, which contain importants points and are written in a lot of pages, is not described in more details.	Itemize the sections 6.2 and 6.3 in details in the table of contents, i.e. place the headings of subsections 6.2.1, 6.2.2, ... 6.2.7 and 6.3.1, ... 6.3.9). It will help to better orientation in the document.	Since all other OIML Documents also restrict the table of contents to one/two levels of clauses, we should not deviate here. Moreover, adding 16 new items to the table will not improve legibility. The issue should be solved when the entire document is restructured in the frame of the next revision.
CZ-02	1	All document		Ed	Different level headings are written in the same type and font size, see eg. heading 6.2, 6.2.2 and 6.2.2.1. So the document is quite confusing. It's hard to find in it.	Distinguish the font for each level of headings.	Agreed. This problem stems from the Word template provided by BIML, which has embedded styles for all headings. This will be solved prior to publication of 2CD.
CZ-03	1	3.2.6		Ge	The definition of “cloud” says: cloud=”servers that are accessed over the Internet, and the software and databases that run on those servers” But we have to distiguish between servers and cloud. Cloud is not just a server(s). Cloud providers offer not just space for your data/application, but they offer also services. And everything is mirrored in other clouds so a net of clouds must be made. It is not possible to put a physical sealing into it. And it should be clear that “cloud” is server which is not commonly physically accessible (it is a field of servers in closed area offered by 3rd party).	Amend the definition.	Since the individual configurations of cloud servers differ widely in the field (especially regarding mirroring of data, provision of services etc.) we cannot narrow down the definition to a specific use case. However, we should combine this proposal with the ones made in FR-02 and NL-02 and add a note stating that, “Cloud servers may not be physically accessible to all parties and may be located in a different country. Their physical location may not be not known and not fixed.”

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
CZ-04	1	3.2.8		Ed	See the comment NL-009: “It was proposed to use the term component for a hardware part and module for a software part.” But from the definition of the “component” is not obvious that it is always a hardware part.	Add the word “hardware”: component = identifiable hardware part of an instrument that performs a specific function or...	Agreed.
CZ-05	1	3.2.45		Ge	The definitionf for “mobile app” was given: “computer program or software application designed to run on a mobile device such as a phone, tablet, or watch” We were surprise about watch. Do we really want to deal with them? They are so many types of them – some very simple, others very smart. In general they are much more vulnerable than mobile/tablet.	Leave out watch from the definition.	The current wording was proposed by France after the first PG meeting. Before changing the definition, we should consult the entire PG. The PG decided to keep the current definition.
CZ-06	1	6.2.1	paragraph 3	Ed	There is written: “If a measuring instrument or component has neither display nor printer or if the instrument facilitates remote verification, the identification shall be sent via a communication interface, in order to be displayed/printed on another component or by the verification software.” The identification shall be always shown via legally relevant software. It must be clear. So we propose to amend the sentence in thay way.	Add the words “legally relevant”. “If a measuring instrument or component has neither display nor printer or if the instrument facilitates remote verification, the identification shall be sent via a communication interface, in order to be displayed/printed on another legally relevant component or by the verification software.” Further we propose to go though the whole document and check whether the words “legally relevant” should be added there or not – for a clarity.	Agreed, the addition clarifies the meaning of the word “another”, implying that the other component is also legally relevant. The rest of the document will be checked accordingly.
CZ-07	1	6.2.3.6	Paragraph	Ge	What happens when audit trails have no more capacity? We should specify what is appropriate to happen. Therefore it is said that it shall not be possible to delete the data of audit trails, in case the memory is full other change must be banned.	Add into the sections: If the audit trail has no more capacity an appropriate response is required, i.e. no other change of a parametr should be done without breaking the seal. Maybe we can add also a note: Note: PG may specified exceptions or other behavior.	Agreed, generalizing the existing condition for logging of software updates (6.3.8.4.9) for all audit trails makes sense. Before implementing this we should discuss it with the entire PG to avoid contradictions between 6.2.3.6 and 6.3.8.4. The following phrasing was agreed upon at the meeting: “If the audit trail has no more capacity an appropriate response is required i.e., either the oldest entry may be deleted, or no other change of a parameter shall be possible without breaking the seal. Note: PGs may specify what the appropriate responses are.”

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
CZ-08	1	6.2.4	Example 2	Ge	There is written: „Once the measurement is completed the result is indicated on a display attached to the instrument. The result is also sent back to the smartphone for secondary indication.“ We should define what is the „secondary indication“ – is it always legally relevant indication or not?	Define/specify what „the secondary indication” is.	Since secondary indications may indeed not be legally relevant for all instruments while they are legally relevant for others, we cannot specify this here. However, we can provide a proper definition together with a note on the potential relevance in clause 3.2. This should be discussed. After discussion at the PG meeting, it was agreed to delete “secondary” in the example. This should solve the issue.
CZ-09	1	6.3.2.2.2		Ge	There is written: “Measurement data shall not be made available to legally non-relevant modules prior to primary indication. Furthermore, PGs may decide that no secondary indication is allowed for certain scenarios.” Again we should define what is the „secondary indication“ – is it always legally relevant indication or not?	Define/specify what „the secondary indication” is.	See response to CZ-08. As a result of the discussion at the PG meeting, it was agreed to delete the sentence mentioning the secondary indication altogether and to add the following note to the clause: “This does not preclude legally relevant modules to show intermediate measurement data.”
CZ-10	1	6.2.4 6.3.2.1.7 6.3.3	example 2 example example 3	Ge	During last PG meeting held in May 2021 was decided that the smartphone has to be “dedicated device”, not “bring-your-own-device”. But it is not meantioned anywhere in the document. Nevertheless the term “mobile app” was defined (see the Terminology section) and the term “app” is meantioned several times in the document (in sense “mobile app”). So we shoud add what “smartphone app” means and state what dedicated device means. In case it is missing the user can easily think the smartphone app is an application that can be downloaded and installed into his own smartphone.	Add information that the “smartphone app” means the application in dedicated device and state what dedicated device means.	There was consensus during the PG meeting to focus on dedicated devices but to leave the technical implementation of the requirements up to the manufacturer (see discussion on NL-042). This implies that BYOD might be possible in certain cases as long as all requirements (including full protection and securing) can be met. In the example in 6.3.2.1.7 this is explicitly mentioned.
CZ-11	1	6.2.4 6.3.2.1.7 6.3.3	example 2 example example 3	Ge	The “Mobile app” is defined, but it is not used in the text of document. But a term “Smartphone app” is used several times. So it will be useful to add/replace the definition or add that smartphone app is mobile app.	Add/replace the definition or add that smartphone app is mobile app: “Smartphone (mobile) app….”	Agreed. The term “smartphone app” should be changed to “mobile app” throughout the document.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
CZ-12	1	6.3.4.3 and 6.3.5.3	example 2 example 2	Ed	See the comment NL-009: "It was proposed to use the term component for a hardware part and module for a software part." There is written: „The private and public keys used for signing are generated in a hardware security module which protects the private key against manipulation or reading and exports the public key." The word "module" is used there, but "module" should be used just for SW part and this is a HW part. So we should find another word – e.g. key or facility.	Replace „hardware security module" by „hardware security key" or „hardware security facility".	The term "hardware security module (HSM)" – just like the term "trusted platform module (TPM)" is well-known and established in the IT security community. Therefore, we should not change the term in D31.
CZ-13	1	6.3.4.4.2		Te	The point says: "Measurement data stored in a component to construct the measurement result can be deleted if the next module or component state a proper completion of expected actions engaged." The bold part of the sentence is not clear. The completion should be evaluated by the module or component – what kind of module/component? (And was also taken into account that was agreed that the "module" always means SW module and the "component" is HW part of a device?) And what actions shoud be completed? Settlement of a transaction or its printing?	Refrase the article and make it clearer.	During writing of 1CD it was indeed taken into account that "module" would only refer to software and "component" to hardware. The phrasing of the sentence was intentional in this regard. If the next module states completion of the expected actions, this implies that the respective checking has been performed. Nevertheless, we can rephrase the sentence as follows to avoid confusion: "Measurement data stored in a component to construct the measurement result can be deleted if the next module or component has checked and stated a proper completion of all expected actions engaged." Since the actions to be performed by the next module or component, depend upon the specific use case, the requirement cannot be made more specific in this regard.
CZ-14	1	6.3.6.1		Ge		Add a sentence: PG may decide whether to use operating system at all or constrain it.	Usually, it is up to the manufacturer to use or not to use an operating system. However, if an operating system is used, PGs are at least obliged to consider the proposed operating system requirements in clause 6.3.6. The proposed sentence does not fit into this context.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
CZ-15	1	6.3.6.7.2		Ge	When reading the article and its notes we derived that the manufacture have to ensure that the legally relevant operating system part may not be updated without his knowledge – in case he do not want to do verified or traced update. And we have a question for clarification: The legally relevant operating system part may not be updated without its approval by NB? If "YES" add it as a note 3 into the article.	Potentially add a sentence: The legally relevant operating system part may not be updated without its approval by NB.	6.3.6.7.2 already points to clauses 6.3.8.3 and 6.3.8.4 regarding requirements on software updates. If we need to add a note on approval of new software versions, it should be placed in 6.3.8.1. This should be discussed with the entire PG. At the meeting, everyone was of the opinion that this is already covered by the first sentence of 6.3.8.2.
CZ-16	1	6.3.8.4.9		Te	The requirement was reworded related to the comment NL-112. But the note about sufficient capacity of the audit trail vanished. The capacity could vary a lot. We should point out that the capacity should be sufficient and that also depends on national regulations. And the same with the appropriate reaction.	Add the note: Note: PGs need to define the sufficient capacity for the audit trail and need to define the appropriate reaction. Both also depend on national regulations.	The originally proposed note from NL-112 was accidentally not implemented in 1CD. This will be amended.
CZ-17	1	7.2.2		Ge	Traced update procedure has/could have a big influence to the measuring instrument. So it is important for the involved subjects to know that the instrument has that possibility. So we suggest to add into certificate also information about that functionality.	Include also a traced update procedure into the section "software modules under legal control": software modules under legal control, including whether or not the instrument is equipped with a remote verification procedure or a traced update procedure;	Agreed. Nevertheless, this should be briefly discussed with the entire PG as it will affect all certificates. Everyone agreed at the meeting.
CZ-18	1	8.3.6.4		Ed	Digital Data Processing Unit In Terminology section there is mentioned just the term CPU – "Central Processing Unit", but not "the Digital Data Processing Unit". It should be define.	Put in a Terminology part what the "the Digital Data Processing Unit"(DPU) is and its difference to CPU.	Agreed. A definition will be added.
DE-01	1	General		Ge	D34 clarifies that the term "type examination certificate" only pertains to MID. Within OIML CS the term should be "type approval certificate".	Change the term throughout the document.	We should follow the proposal made it AU-01 and use the term "OIML certificate" as specified in B18 and D34. All instances of the term should be checked.
DE-02	1	3.2.27	Note 2	Ed	Please check the wording of the note, something appears to be incorrect.	Rephrase the note.	Agreed, the wording of the note could be clearer. Proposal: "The relevant Recommendations define what is legally relevant and formulate requirements to those items (e.g., data, functions, securing and protection features and information for the completion of the transaction)."
DE-03	1	6.2.1	Paragraph 6	Ed	For consistency, we should stick to the expression "in use" if an instrument is used in the field. Therefore, we propose to reword the paragraph.	Regardless of the form of the software identification it shall be accessible, to allow for it to be checked, at any time the instrument is in use.	As suggested in AU-04, the term "in service" should be better fitting to describe the state of the measuring instrument. All instances of "in use" will be replaced accordingly.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
DE-04	1	6.2.3.1	Example 4	Te	The example should be amended to allow inspectors to check the actual configuration of the neural network's parameters for each measurement result.	Either include all parameter settings in the audit trails (as opposed to the hash) or export signed parameter sets after every change.	Agreed. The actual modification of the example should be discussed with the entire PG. At the meeting, the example was rewritten as follows: "The software contains a neural network of fixed topology, but with flexible weights that change from time to time, to affect the measuring algorithm's behaviour. A ~~**checksum**~~ **hash** over all weights in predefined order is used to identify the neural network weights, while a version number is used for the neural network overall structure and the rest of the software. The ~~**checksum**~~ **hash** is updated and logged in an audit trail, everytime that the parameters change. **The file containing neural weights, that matches the hash, is stored within the instrument for the time period required by national legislation or stored externally in case of limited storage. The file matching a certain hash is accessible upon request.**"
DE-05	1	6.2.6.2		Ed	The sentence "The relevant Recommendation may suggest…" is no longer needed.	Delete the sentence.	Agreed.
DE-06	1	6.2.7	Paragraph 2	Te	Sentence 2 addresses protection measures for setting the clock of an instrument while sentence 3 allows automatic setting of the clock. It should be clarified how both sentences interact.	Add a note to clarify if and how automatic setting of the clock needs to be logged.	Agreed, proposal for the note: "In case an internal clock is automatically synchronized with legal time, protection of the clock implies logging of the synchronization. PGs should consider audit trail capacity when deciding on the level of detailedness of the synchronization records." This should be discussed with the entire PG. Revised proposal from the PG meeting: "PGs shall specify under which circumstances a setting of the clock shall be logged."

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
DE-07	1	6.3.2	Paragraph 3	Ed	To increase legibility and for consistency, we propose to reword the paragraph.	Recommendations may specify the software modules, hardware components and data that are legally relevant.	Agreed. Since modules and components are now exclusively used for software and hardware, respectively, proposal to phrase the sentence as follows: "Recommendations may specify the modules, components and data that are legally relevant."
DE-08	1	6.3.2.1.2	Paragraph 1	Ed	The paragraph now contains two almost identical sentences on the influence on data etc. via the protective interface.	We should discuss if we can delete the last sentence.	Agreed. We should at least be able to combine and simplify both sentences. This will be discussed with the entire PG. At the PG meeting, it was decided to delete the second sentence.
DE-09	1	6.3.2.2		Ed	Since the term "modules" is now exclusively used for software, we should align the title of 6.3.2.2 with 6.3.2.1.	Change the title of 6.3.2.2 to "Separation of modules".	Agreed.
DE-10	1	6.3.2.2.1	Paragraph 3	Ed	The last paragraph contains no requirement and should, therefore, be a note.	Note: Software separation takes either place in the complete measuring instrument or in a specified component. • For separation of components, see 6.3.2.1. For communication between components, see 6.3.5.	Agreed.
DE-11	1	6.3.5.3	Example 1	Ed	Both sentence 2 and 3 start with the pronoun "it" although they refer to different objects.	Modify the sentences to avoid confusion.	Agreed. Proposal to rewrite the example as follows: "The legally relevant software of the sending device calculates a CRC32 [11] of the dataset, which is appended to the dataset. A secret initial value is used for the calculation of the CRC32 instead of the value given in the standard [11]. This initial value …"
DE-12	1	6.3.7		Ed	The term "certified type" does not exist in D34, where certification is seen as a product of type evaluation and type approval. Should we use the same terms here?	Discuss the term "certified type" and change to "approved type" if deemed necessary.	This should be discussed with the entire PG. At the meeting, it was agreed to use the term "approved type" throughout the document.
DE-13	1	6.3.9.1.5	Paragraph 1	Ed	Please check the wording of the paragraph, something appears to be incorrect.	Rephrase the paragraph.	Agreed. The paragraph will be amended, see response to JP-12.
DE-14	1	Annex B	Checklist	Ed	The checklist in Annex B currently makes it difficult to give "pass" and "fail" marks for individual subclauses.	Reformat the checklist to follow the established structure of checklists in other test report formats more closely, e.g. R76-2: Insert additional horizontal separation lines for sub clauses and clearly separate clause titles from requirement texts.	This should be discussed with the entire PG. At the meeting, everyone agreed.
FR-01	1	3.2.14		Ge	The concept of "dynamic module of legally relevant software" and what could be as a dynamic module is not very clear, especially without a participation in SG 1.	Please clarify (example, note…) or give an explanation.	This should be solved by changes resulting from AU-02.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
FR-02	1	3.2.6		Ge	If clouds are introduced in this document, we must collectively assume that the location of the servers is not always known and fixed and can be in another country. This statement can have consequences because national regulation may not apply to the country where servers are located. Moreover, the owner and the manufacturer of the instrument have no control on it. The users of this Document have to be clearly warned.	Add a note to indicate that: - the location of the servers is not always known and fixed and can be in another country - the manufacturer of the instrument and the owner of the instrument have not control on it.	This should be solved by the combined proposal laid down in the response to CZ-03.
FR-03	1	6.2.3.1	Example 4	te	The example should be amended to clarify how inspectors check the actual configuration of the neural network's parameters for each measurement result.	Please clarify.	This should be solved by the outcome of the discussion of DE-04. See response to DE-04.
FR-04	1	6.3.6.8		te	What is exactly the "configuration management" of dynamic modules of legally relevant software ?	Please clarify.	Clause 3.2.53 already specifies the scope of configuration management. Nevertheless, we can discuss its application to dynamic modules of legally relevant software. At the meeting, it was decided to amend the term to "software configuration management" in clause 6.3.6.8. It was also agreed to respond to the comment as follows: "Clause 3.2.53 already specifies the scope of configuration management. Suggestions for a different example/note would be welcome."
FR-05	1	6.3.7		te	It is stated in the case of dynamic modules of legally relevant software, the documentation submitted by the manufacturer describes a means to validate the conformity to type. Inspectors have not the documentation. It is not clear how it is possible for inspectors to evaluate the conformity of these dynamic modules on instruments in use. Are information available in the configuration management of dynamic modules of legally relevant software (6.3.6.8) ?	Please clarify.	Obviously, such information also needs to be included in the certificate to make it available to inspectors, verification officers etc. This should be briefly discussed with the entire PG. At the meeting it was concluded that inspectors should have access to the documentation. The argument given in the comment also applies to other issues regarding conformity to type, for which the certificate is sufficient. Therefore, no change is needed.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
FR-06	1	8.1	note	te	The note states national authorities may develop data set types to control devices in use. It shall be possible to check instruments in use without data set types developed by national authorities.	Add an information (in this subclause or in other subclause) to clarify instruments in use can be checked without data set types developed by national authorities.	Agreed. The following sentence will be added to the note: "This does not affect the requirement, that instrument software shall be verifiable."
FR-07	1	8.3		te	National regulation can totally forbid remote verification, especially for instruments used for legal proceedings.	Add a note.	Agree. The following note will be added to 8.3.1: "National legislation may allow or disallow remote verification depending on the instrument."
FR-08	1	8.3.6.2 to 8.3.6.5		ge	Procedures in 8.3.6.2 to 8.3.6.5 are solutions for measuring instruments. These solutions could be mandatory, forbidden or optional according to measuring instruments. The actual instrument specific requirements shall be left up to the project groups.	Change the first sentence of 8.3.6.1 to state subclauses 8.3.6.2 to 8.3.6.5 gives examples for specific types of measuring instruments and add a sentence to state instrument specific requirements shall be left up to the project groups.	Agreed. See also response to NL-15
IR-01	1				No comment at this stage		Noted.
JP-01	1	3.2.45 mobile app		ed	In the end of 3.2.45, the text reads "[Cambridge Dictionary]". It seems better to provide more detailed information of the reference since the content/description may vary depending on the edition.	Provide details of the reference, i.e., year of publication and the number of editions.	OK. Depending on the outcome of the discussion of CZ-05, no reference to the Dictionary may be needed anymore.
JP-02	1	3.2.62 test item	Note 1	ed	The second "and" seems to be redundant.	Remove the second "and".	Agreed. This appears to be a copy&paste error.
JP-03	1	6.2.1 Software identification	Secon-to-last paragraph	te	The expression "at any time" seems too demanding. Some measuring instruments indicate software identification only when they start, and they do not show the identification while they are in-service. Otherwise, it might be better to employ an expression that we can leave its concrete interpretation up to individual PG.	We propose two options for correction. Option 1: Replace "at any time" with "when". Option 2: Delete "at any time the instrument is in-service."	Agreed. For specific instruments the interruption of the measurement process to indicate the identification may indeed be extremely difficult. Option 1 was selected at the PG meeting.
JP-04	1	6.2.1 Software identification	Note.3 Note.4	ed	Note 2 is omitted.	Correct "Note 3" to "Note 2", and "Note 4" to "Note 3" respectively.	OK. The numbering of the notes will be corrected.
JP-05	1	6.2.5 Demand on the user	All	Ed.	The title is "Demand on the user" while the text reads "… from the user". This difference may be confusing to the readers.	Change the text as shown below. *The software of a measuring instrument shall be designed ~~in such a way~~ that there should be no unreasonable demands on ~~are required from~~ the user to obtain a correct measurement result.*	Since both appear to be grammatically correct expressions, we should retain the current clause.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
JP-06	1	6.2.6.2 Durability protection	3rd para.	ed	For the relevant part, the word "significant" is used only in this part. However, the word seems unnecessary.	Delete "significant" from the text as shown below. *The documentation to be submitted for type evaluation shall contain a list of the ~~significant~~ durability errors that will be detected by the software*	Agreed. Since "significant durability error" is not defined anywhere, we should omit the adjective here.
JP-07	1	6.3.2.1.3	2nd para.		The term "pairing parameters" needs to be defined in Chapter 3, "Terms and definitions".	Add the definition of "paring parameters". We propose the following definition: In general, paring parameter means any parameter that is necessary to connect and run the separated components that form the measuring instrument, such as IP address, Bluetooth pairing key, and encryption key. Depending on the individual design of the measuring instrument, this includes parameters that are used with intent as part of software seal to prevent exchanging or spoofing the components.	During discussion of 1WD comments, it was agreed to explain the term by means of an example (see responses to JP-04 and KR-04 to 1WD). Therefore, no change is needed. At the meeting, it was decided to combine the proposed text with the current note in 6.3.2.1.3.
JP-08	1	6.3.2.1.7	2nd sentence of 2nd item	ge	In the 2nd sentence, the component ensures that the measurement result is printed or indicated in case of a dispute. However, it is not sufficient.	Modify the 2nd sentence as follows: *The component also ensures that the measurement result is printed or indicated together with message or warning in case of a dispute.*	This seems to be a misunderstanding. The indication in case of a dispute does not address data integrity but a dispute between user and customer. Such warnings are required anyway by 6.3.5.3. Proposal to solve this by changing "in case of a dispute" to "in case of doubt".
JP-09	1	6.3.2.2.3	Examples 2)	te	It is difficult to understand the meaning of "sealed administrator password". It is not clear how to seal the password.	Add a definition for "sealed administrator password".	The word "sealed" is explained in the terminology "means intended to protect the measuring instrument against any modification, readjustment, removal of parts or software, etc.". We could explain in the example the manner of sealing, to make it more concise.
JP-10	1	6.3.3 Shared indications	the last paragraph	ge	"6.3.3 Shared indications" might not be suitable for the requirements of marking of AI.	Split the clause 6.3.3 into two clauses: (1) Shared indications and (2) Information of dynamic modules of legally relevant software.	Such a restructuring was rejected during the first PG meeting, see discussion of DE-01 on 1WD. Nevertheless, this could be discussed within the frame of a future revision. At the PG meeting, it was decided to solve the issue now by moving the respective sentences to a new clause 6.2.8 in 2CD.
JP-11	1	6.3.9.1.7		ed	"Batty" in the sentence of "Requirements on batty life," is a typo.	Correct to "battery life".	Agreed.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
JP-12	1	6.3.9.1.5		ed	The phrase "significant defect for the purpose of remote verification" does not sound correct.	Replace "significant defect <u>for</u> the purpose of remote verification" with either (1) "significant defect <u>in</u> the remote verification" or (2) "significant defect <u>in the process of</u> remote verification".	The sentence appears to be correct, The clause lists all the requirements that are necessary for the purpose of remote verification, which include "a facility for detection of significant defects". We could rephrase the clause as a list to make the meaning clearer: "For the purpose of remote verification, the instrument shall • use time stamps (reference); • provide evidence of intervention (reference) • use audit trails (reference) have a facility for detection of significant defects."
JP-13	1	6.3.9.1.11		ed/te	The word "data" in "(A)ccess rights to the instrument for remote verification data" seems unnecessary. This does not conform to the description of 7.1.2: *.... description <u>of the access rights to the instrument for remote verification</u> and a description how test items can ...* (20th line of p.50). In addition, it seems necessary to have a requirement that access rights are appropriately set, such as that only relevant personnel can access remote verification.	Delete the word "data" from the text as shown below. *Access rights to the instrument for remote verification ~~data~~ shall be described ...* In addition, add a requirement for the appropriateness of access rights.	Agreed, the word data appears to be misplaced here. Since requirements on remote verification depend on national legislation (see 8.3.2 in 1CD), we cannot impose any restrictions on the access rights here. Nevertheless, a potential note to that effect should be discussed with the entire PG. At the PG meeting, it was agreed to delete "data". Also, the reference to "access to diagnostics, build in weights etc." was deleted in 8.3.6.1 (now 8.3.3.3.1).

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
JP-14	1	6.3.9.1.12		te	From this requirement, it is expected that there will be a procedure to notify the remote verification results and have them stored in the measuring instrument.	Specify a new clause after 8.3.5 that describe a procedure how the data of remote verification results shall be notified to the measuring instrument, protected, and secured in it.	Since data transmission to the instrument from a legally non-relevant source is outside the scope of D31, we cannot impose any restrictions on it. Regarding protection and securing of remote verification results, this is already covered by the last paragraph of 6.3.9.1.12. Nevertheless, this should be briefly discussed with the entire PG. At the PG meeting, there was consensus that the current clause already covers the results of remote verification. The second paragraph was rephrased to clarify this: "The result of the remote verification shall contain, at least, a unique ID (at least identifying the verification authority) and…"
JP-15	1	8.3.2 General requirements	1st paragraph	te	The second sentence is not clear, although the sentence can be understood as covering the communication between the device and the remote unit outside of it (8.3.1 Figure 2).	Clarify that the second sentence covers communication between a device and a remote unit outside of it (8.3.1 Figure 2).	Agreed, the sentence should be more concise.
JP-16	1	8.3.2 General requirements	Note 5	te	Specify "verification software" concretely in order to avoid confusion between "verification software" and "verification algorithm" in 8.3.1.	Specify "verification software" concretely. As a concrete example, we propose to add the precondition that the verification software runs on the Remote Unit.	Agreed, the expression should be more concise. Proposal to rephrase the note to: "D31 only imposes requirements on the measuring instrument's software. Verification software running on the remote unit is covered by national legislation."
JP-17	1	8.3.3 Extraction of audit trails or other logging mechanisms	title	ed	It seems difficult to extract mechanisms for logging.	It might be better to change the title to "Extraction of audit trails or other logs".	OK, we could phrase it as "Extraction of data from audit trails or other logging mechanisms"
JP-18	1	8.3.3.1 General	3rd paragraph	te/ed	We consider that audit trails or other logs are extracted in 8.3.3. However, the 3rd sentence uses a term "test item" accompanied with two items "software integrity" and "identity of software" without specifications of the applicable test procedures. We consider that this clause refers operational history to be extracted for testing, and therefore, inapplicable items should be deleted.	We propose to delete the phrase "software integrity, identity of software" from the sentence which is not considered as operational history as shown below. *Applicable test items for this remote verification procedure are ~~software integrity, identity of software,~~ evidence of interventions, audit trails, detection of significant defects.*	The argument is sound. Software integrity and software identity would belong in the category "Direct extraction of test items".

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
JP-19	1	8.3.4.1 General	2nd paragraph	te	The test item “software integrity” seems to belong to the next procedure “Live integrity verification methods” in 8.3.5.	Delete “software integrity” from the paragraph.	Agreed. We do not need to cover the same test item with two different procedures.
JP-20	1	8.3.5 Live integrity verification methods 8.3.5.1 General	2nd paragraph	te	In the second sentence of 8.3.5.1, the distinction between the integrity of “authenticity and integrity” and the “live integrity” of title 8.3.5 is unclear.	The distinction between the integrity of “authenticity and integrity” and “live integrity” needs to be clearly stated. If necessary, add requirements to 8.3.5.1 for checking of connection requirements (stated in 6.3.9.4.1).	Indeed, 8.3.5.1 as proposed by SG2 seems to be unclear in its entirety. We should discuss the clause with the entire PG. At the PG meeting the following was agreed: - A general requirement for checking integrity and authenticity of the measuring instrument will be added to 8.3.2. Respective sentences in 8.3.3.1 and 8.3.5.1 will be deleted. - The clause 8.3.4 will be separated into the following three distinct subclauses under 8.3.3.2: software integrity (previously “live integrity verification”), check of parameters and software dentification. See also response to JP-19. - The test item for 8.3.4 will be changed from “software integrity” to “integrity measure”. Thus, 8.3.5.1 will become a subclause of 8.3.4, which should solve the issue.
JP-21	1	8.3.6.5	All	te	The description of the simulation setting is unclear. Specifically, they are as follows: (1) The category of measuring instrument described is unclear. (2) It is unclear that the object of the simulation is supposed to be the start and end signals to the sensor, not the output from the sensor. (3) It is unclear whether “mother unit” can be understood to mean “motherboard”. (4) It is unclear what "P2P" refers to and what the relationship is.	Propose the following correction. (1) Specify the category of measuring instrument being described. (2) Specify that the target of the simulation is not the output from the sensor, but the starting and ending signals to the sensor. (3) Add a sentence stating that “mother unit” means “motherboard”. (4) Specify what two “P(pair)”s of “P2P” refer.	This will be discussed with the original proponent. A proposed modification will be presented at the meeting. The proposed modification, to explain that the clause specifically addresses an example for point-to-point speed meters, was agreed upon at the meeting.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
JP-22	1	Annex C		ed	Especially for non-English-speaking countries, descriptions of abbreviation help understanding. After translating from English, it is often difficult to assume what an abbreviation stands for.	Add the abbreviations (MQV, MQVM, MRRD, MRRM MPD, MPM and MRRI) in Annex C to their original terms in Chapter 3, "Terms and definitions" and/or 3.3, "Abbreviations".	Agreed.
JP-23	1	Figure A.1		ed	Better to use abbreviations instead of the symbols (spade, club, heart, diamond and square) in the figure.	The symbols should be replaced with abbreviations.	This was already rejected during the previous revision. At the meeting, it was decided that the symbols will be replaced with the abbreviations.
JP-24	1	Figure A.2	4th para.	ed	"Measured Quantity Metadata (MQMD)" seems incorrect. "During processing, the Measured Quantity Value (MQV) with "integer value" as the Measured Quantity Metadata (MQMD) is assigned 'kWh'	Correct "Measured Quantity Metadata (MQMD)" to "Measured Quantity Value Metadata (MQVM)". *During processing, the Measured Quantity Value (MQV) with "integer value" as the ~~Measured Quantity Metadata (MQMD)~~ Measured Quantity Value Metadata (MQVM) is assigned 'kWh' as Measurement Result Relevant Data (MRRD) …as customer ID (MRRM).*	Agreed.
KR-01	1	3.2.7		ge	The description of 'communication interface' and the meaning of Note 1 are not appropriate. Note 1 describes an example of communication means, but in the description of the communication interface, it is explained that it is a part of the instrument.	(1) Delete or modify Note1. (2) Changed the description of the communication interface to the communication method Choose (1) or (2)	Suggestion to rephrase note 1 as follows: "Communication interfaces can support wired, optical, radio, etc. communication and they are usually designed to use a specific protocol."
KR-02	1	6.2.3.1		ge	We suggest that the definition and examples of 'neural network' and 'weights of a neural network" are needed.	To clarify the terms and usage, add the definition of "Neural network" and "weights of a neural network"	Since this wording only appears within examples, a separate definition appears unnecessary. A proposal for a more extensive example on the other hand, would be welcome.
KR-03	1	6.3.3		ge	Shared indications description means that the sub-indicator that outputs measurement data should be managed as a legal weighing part.	The description of the current version is not about the auxiliary indicator handling measurement data.	The statement made in the proposed change column is correct. It is unclear if any change is needed.
KR-04	1	6.3.9.1		ge	In D31, Remote Verification Capability means software verification.	Since it can be misunderstood as verification of the instrument's measuring performance, it should be described as software verification.	Since D31 only concerns the software of measuring instruments, the fact that remote verification is in relation to the software of the measuring instrument should be clear. Revised response after the meeting: Depending on the type of instrument, the remote verification procedures may indeed also cover the metrological characteristics.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
KR-05	1	6.3.9.4.1		ge	The details of the connection requirements are unclear.	It would be better to indicate a clause for connection requirements.	Agreed, a better explanation for what is meant with "connection requirements" is needed. This should be discussed with the entire group. After discussion at the PG meeting, it was decided to change the title of 3.9.4 to "Connection requirements" and 3.9.4.1 to "The connection to the remote verification software shall comply with 6.3.5."
NL-01	1	3.3	note	Ed	Terminology used in PD-05 is OIML certificate.	Change OIML type examination certificate into OIML certificate.	Agreed, we should follow the official OIML terminology.
NL-02	1	3.2.6		Ge	This definition does not match the definition used by cloud service providers (e.g. Microsoft, Amazon, Google). An important feature of these services is that the physical location of the server is not known and not fixed. This is relevant for legal metrology as the national laws may not apply when servers are not located in the country. Also, cloud servers are not maintained by the manufacturer, the user, or the owner of measuring instruments. It means they have no control over the OS and basis servers (webserver, database server) and their versions, security and updates.	If a match with the cloud server providers is necessary, change the definition to: Servers that are accessed over the Internet, and the software and databases that run on those servers, for which the physical location is not known and not fixed.	Agreed. See CZ-03 for a combined proposal based on NL-02, FR-02 and CZ-03.
NL-03	1	3.2.24		Ge	The definition of software is now limited to executable software (= programs). This makes legally relevant software (3.2.29) limited to executables. This is inconsistent with: 3.2.66: Type-specific parameters are part of the legally relevant software. 6.2.3.1 where software includes parameters and data.	Change 3.2.66 and 6.2.3.1 according to the definition stated in 3.2.24 or adjust 3.2.24	This is true. To solve the issue it is proposed to add the following note: "Software may include parameters and data, see 3.2.66."
NL-04	1	6.2.4	Example 2	Ed	Consequent use of "mobile app", for which we have a definition.	Replace smartphone app with mobile app.	Agreed.
NL-05	1	6.3.2.1.7	Example	Ed	Consequent use of "mobile app", for which we have a definition.	Replace smartphone app with mobile app.	Agreed.
NL-06	1	6.3.3	Example 3	Ed	Consequent use of "mobile app", for which we have a definition.	Replace smartphone app with mobile app. Replace app with mobile app (2x).	Agreed.
NL-07	1	6.3.4.1	Note 2	Ed	Note 2 seems to be out of place and does not relate to the text. Neither "total stored count" and "audit trail" are mentioned in the text.	Delete the note or move it to the appropriate place.	Agreed. The note should be moved to the clause on audit trails (6.2.3.6).

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-08	1	6.3.4.4.1	First paragraph and third paragraph .	Ed	The first sentence “When, considering the application, data storage is required, measurement data shall be stored automatically”, excludes manual storage. This may not be appropriate for all kinds of measuring instruments. Think about non-automatic weighing instruments were an intelligent action of the operator is required to accept the measurement. After that data storage is automatically carried out. (Relates to former comment NL-087)	Change to: Depending on the application, automatic storage might be required.	Agreed.
NL-09	1	6.3.4.4.1	First and third paragraph	Ed	The first sentence “When, considering the application, data storage is required, measurement data shall be stored automatically”, excludes manual storage. That makes the use of the term “automatic storage” a duplicate.	Change the third paragraph to: ” If data storage is required, manual or automatic, no measurement shall be possible if the storage device is not available.”	Agreed.
NL-10	1	6.3.8.2	First paragraph	ed	The last sentence uses the word should. But we feel that this is a requirement and therefore must be changed to shall.	Change the last sentence to: “In the case that device-specific parameters (especially calibration parameters) are concerned, only a verified update *shall* be done.”	Since this is not a requirement on the software but on the person responsible for the update, we cannot impose any restrictions. Therefore, “should” should stay in place.
NL-11	1	6.3.8.4.10		ed	This is a requirement therefore should must be changed to shall.	Change to: “When the software is updated, the audit trail *shall* not be erased or overwritten.”	Agreed.
NL-12	1	6.3.9.1		ed	The text must refer to exact requirements, like in 6.3.6.1 (and other places).	Change to: “In case the instrument facilitates remote verification, the requirements in 6.3.9.1.1 to 6.3.9.1.12 shall be met.” or change to: “In case the instrument facilitates remote verification, the requirements in 6.3.9 shall be met.”	Indeed, we should align this general clause with the other ones. Therefore option 1 is preferred.
NL-13	1	7.3.2.3		ed	Reference to WELMEC 2.3, but this document is recently withdrawn.	Remove the reference to WELMEC 2.3	In fact, WELMEC 2.3 has now been replaced with WELMEC 7.5. However, as this is simply an application of WELMEC 7.2, we should simply delete the reference.
NL-14	1	Annex A	Ref [8]	ed	Reference to WELMEC 2.3, but this document is recently withdrawn.	Remove the reference to WELMEC 2.3	Agreed, see also response to NL-13.
NL-15	1	8.3.6.1		ge	It is not clear if the procedures in 8.3.6.2 to 8.3.6.5 are mandatory, voluntary or examples for these specific types of measuring instruments. Only the specific PG’s shall prescribe procedures for specific instruments.	Change the first sentence of 8.3.6.1 to: The following subclauses 8.3.6.2 to 8.3.6.5 gives *an example of* a specific realization of this remote verification procedure for certain specific types of measuring instruments.	This should be combined with the proposal from FR-08 to also include a note on a PG’s obligation to come up with specific requirements if needed.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
UK-01	1	Introduction		ge	In the Introduction, we have the following statement: "Furthermore, this International Document can provide guidance to OIML Member States in the implementation of OIML Recommendations in their national laws".	Since OIML consists of Member States and Corresponding Members, I suggest adding Corresponding Members to the introduction since they also benefit from OIML Publications: "Furthermore, this International Document can provide guidance to OIML Member States and Corresponding Members in the implementation of OIML Recommendations in their national laws".	Agreed.
UK-02	1			ge	"certified type" is mentioned several times in the document, however a definition will be useful to readers of different languages	I propose that we add a definition or terminology for "certified type"	Unfortunately, B18 also uses the term without giving a proper definition. We should consult BIML on this. Depending on the outcome of the discussion on DE-12 (#D3 Terminology), this might already be resolved. The PG decided to use "approved type", see discussion on DE-12.
UK-03	1			ge	"dynamic modules" is mentioned several times in the document, however a definition will be useful to readers	Proposal, add a definition or terminology for "dynamic modules"	This should be solved by changes resulting from AU-02.
UK-04	1	3.1		ed	In OIML B 18 *Framework for the OIML Certification System (OIML-CS),* OIML Certificate is mentioned in 3.25, not OIML type examination certificate which pertains to EU-type examination Certificate in OIML D34 *Conformity to Type (CTT) – Pre-market conformity assessment of measuring instruments*	Please align with B 18, 3.25 terminology: *3.25* *OIML Certificate* *Type Examination Certificate, issued by an OIML Issuing Authority, attesting the conformity of a type of a measuring instrument or module with the relevant requirements of an OIML Recommendation at the time of testing and evaluation*	Agreed. This is in line with the proposals from DE-01, AU-01, NL-01. The definition will be added to the terminology.
UK-05	1	3.2.6			Cloud servers can be based anywhere in the world and subject to national regulations. Suggest clarifying this in the terminology	Add a note that the location of the servers can be anywhere in the world without accurate location data and subject to national regulations.	This should be solved by the proposal detailed in response to CZ-03.
UK-06	1	6.2.1	3rd	ed	If a measuring instrumen or…	Correct to If a measuring instrument or..	Agreed.
UK-07	1	6.3.2.1.3	te	te	There is consensus across the industry that the Rivest Cipher 4 (RC4) is no longer cryptographically secure and also as indicated in RFC 7465: Prohibiting RC4 Cipher Suites	Proposal is to replace RC4 with any other secure encryption algorithm such as AES-128 which is considered more secure than RC4.	Even though attacks on RC4 are known, it might still be sufficient for risk level I. This should be discussed with the entire group. The group decided to implement the solution from UK-07.
US-01	1	3.2.35-3.2.44		Ed	These concepts are not obvious to the uninitiated. Annex C was developed to lend some clarity to these definitions.	Suggest referring to Annex C somewhere in the definition.	Agreed. Such references will be added as notes to the individual terms.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
US-02	1	3.2.68		Ed	The phrase, "or its (hardware) components or (software) modules" is redundant.	Suggest truncating the definition to end at "measuring instrument".	If the definition were truncated as suggested, it would always imply communication with an entire measuring instrument even if separate user interfaces are available on different components.
US-03	1	6.1		Ed	The first paragraph is a little difficult to read as written.	Suggest writing as bullets. For example: The general requirements are separated into: - general requirements (6.2), applicable to…; and requirements for specific configurations (6.3).	OK
US-04	1	6.2.2		Ed	The note "The requirement regarding hidden functions only applies to legal metrology," is actually a requirement.	Make this obvious in the text of 6.2.2 and do not include it as a note.	Since anything stated in D31 only ever applies to legal metrology, we should not explicitly mention this in one requirement and thus cause confusion.
US-05	1	6.2.3.2		Ed	Are influences assumed to be inadmissible, or does this cover other influences as well?	Alter the text of the second bullet to read, "not be able to <u>inadmissibly</u> influence the legally relevant characteristics of the instrument."	Agreed. Otherwise, we would make any interaction with the software through the interface impossible.
US-06	1	6.2.3.1	7th paragraph	Te (minor)	"In case of dynamic modules of legally relevant software with predefined parameters, these shall be considered as a part of the software and treated as such. This entails **logging of all parameter changes** in an audit trail (see 3.2.1)." If adaptation of parameters is a continuous process, then the audit trail is filling up rapidly.	Improve the language to exclude continuous adapting parameters. OR Exclude the possibility of continuous adapting parameters.	If we were not to log changes to continuously adapting parameters, we would end up with measurement results that can no longer be traced back to a specific configuration. Maybe, we simply need to point out that continuous adaptation poses a risk. This should be discussed with the entire PG. At the meeting, there was consensus that modifications resulting from DE-04 and FR-03 solved the issue.
US-07	1	6.2.3.1	Note 1	Te (minor)	"… additional external protection means (e.g. cryptographic signatures for transmitted or indicated measurement data) may be used to **check correct behaviour** of the software." With a signature you can check integrity and authenticity but not the correctness of the behaviour.	"… additional external protection means (e.g. cryptographic signatures for transmitted or indicated measurement data) may be used to check ~~**correct behaviour**~~ **the integrity** of the software."	As the signature is not applied to the software, but to data sent by the software, a correct signature implies integrity of data and thus correct behaviour of the software.
US-08	1	6.3.2.1.6		Ed.	"…are not physically connected **and therefore present in the same location**, …" This is incorrect and the next sentence actually implies that the components are <u>not</u> in the same location. We assume that this is a typo.	"…are not physically connected and **<u>not</u>** therefore present in the same location, …"	Agreed.

Country Code[1]	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment[2]	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
US-09	1	6.3.2.2.2		Te/Ed	The restriction limiting availability of measurement data only to legally-relevant modules prior to primary indication is limiting and has the potential to be impractical (the 3rd paragraph). There are cases where a user may need to see imperfect data during a process, e.g. aircraft refueling.	Can the first sentence of the third paragraph be eliminated without altering the requirements? Or could some other condition be used to accommodate cases where in-process data may be visible to a user? The point is that data cannot be altered by the user, but is it relevant that it can/cannot be visible? Perhaps deem acceptable for example only if secondary device indicates result is not legally relevant?	The original intention of the sentence was indeed to ensure that measurement data is not visible to external entities prior to primary indication. If this is deemed too limiting, it should be discussed with the entire PG This has been solved as a result of the discussion of CZ-09.
US-10	1	6.3.9.1.7		Ed	In bullet item 1, 'battery' misspelled	Replace 'batty' with 'battery'	OK
US-11	1	8.3.6.2 – 8.3.6.5		Te.	These are very solution for specific instruments and not related to software (which is the focus of D31). Although this is very useful, the actual instrument specific requirements should be left up to the project groups.	Change 8.3.6.2 - 8.3.6.5 into examples.	Agreed. We should implement the combined solution proposed in NL-15 and FR-08.
US-12	1	8.3.6.2		Ed	"Initiate an internal weighing procedure using a build-in weight in …".	Use "built-in" instead.	OK
US-13	1	8.3.6.3		Ed	"Initiate procedure using a build-in diagnostics facility…"	Use "built-in" instead.	OK