



TC 5/SC 2/p 4:	Revision of D 31: <i>General requirements for software controlled measuring instruments</i>			TC5_SC2_P4_N031
PG vote/comments on 1WD:	TC5_SC2_P4_N008			
Circulation date:	17 November 2020	Convener: Germany – Marko Esche	Closing date for voting and/or comments: 17 March 2021 at 17:00 CET	
Date comments submitted:		Please type your comments in this form and post it (in Word format) as soon as possible and <u>no later than the closing date</u> in response to document TC5_SC2_P4_N008 on the PG workspace.		
PLEASE INSERT THE COUNTRY CODE AND THE PART AND CLAUSE NUMBER IN EACH ROW. PLEASE DO NOT MODIFY THE NUMBER OF COLUMNS IN THE TABLE.				

Instructions for using this template:

The structure of this table allows for the automatic collation of all the comments posted by the participants. However, this is only possible if the following instructions are followed. Please

- do not add any columns to the table,
- do not merge any of the cells,
- add the Country Code in each row,
- fill in the Part number in each row (if the document to be commented has no parts, leave this column blank),
- enter one reference per row in the Clause/Sub clause column. If your comment applies to more than one clause, please repeat the row or make the reference in the Comments column,
- do not embed other tables in the table,
- enter the date on which you make the comments in the heading.

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 <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
SG1					Implement SG1 results.	Implement SG1 results.	
SG1					Implement changes to SG1 results related to NL comments at the meeting.	Implement changes to SG1 results related to NL comments at the meeting.	
SG2					Implement SG2 results.	Implement SG2 results.	
SG2					Implement changes to SG2 results related to AU comments at the meeting.	Implement changes to SG2 results related to AU comments at the meeting.	
SG3					Implement SG3 results.	Implement SG3 results.	
DE-01		General		ge	According to clause 3.1.1 of B6-2, Recommendations shall exist of specific parts for requirements, test procedures, test report format etc. Although 3.1.1 does not apply to Documents and no other Document has adopted the part separation yet, we should discuss if D31 should be structured following the same principle. This would reduce the number of subdivisions per requirement clause considerably.	Discuss within the whole PG if D31 and its annexes should be split into the five parts described in 3.1.1 of B6-2 to facilitate adoption of software requirements into new or revised recommendations. Feedback from ongoing revisions of Recommendations would be very helpful.	Okay. At the PG meeting, it was agreed to propose this for a potential next revision.
DE-02		General		ge	According to the ToR, this revision shall also deal with existing D31 requirement clauses that do not use normative language.	Requirement clauses that do not use normative language (such as 6.2.8.3, 6.2.8.4.1, 7.2.1) shall be revised and corrected where necessary.	At the PG meeting, it was agreed that the convener shall check all respective clauses and make requirements explicit by using normative language. The language of examples shall be checked as well.
DE-03		General		ed	Certain clauses currently contain more than one requirement (such as 6.1.3.2.5, 6.1.4.1, 6.1.4.2, 6.1.5 6.2.2, 6.2.2.2.2, 6.2.3, 6.2.4.3, 6.2.4.4.1, 6.2.5.3 6.2.5.4, 6.2.8.3) whereas others are split on a very detailed level.	For better legibility and easier reference in test reports, these requirements should be split to separate different requirements into subclauses. The PG should decide on the required level of detailedness per requirement.	Agreed. At the PG meeting, it was concluded to try and provide clauses that can be examined individually. This will be implemented after ICD has been agreed. If too many open issues remain, this will be moved to the next revision.
NL-001	1	General		Te	It might be necessary to define component because we believe that the requirements of 6.2.2.1 do not apply if all components are in the same housing of the measuring instrument.  The clauses in 6.2.2.1 apply to component that are an identifiable part of an instrument that performs a specific function or functions, and that can be separately evaluated according to specific metrological and technical performance requirements as specified in the relevant Recommendation.  We propose to add this definition in D31.	Add to terminology:  Components  an identifiable part of an instrument that performs a specific function or functions, and that can be separately evaluated according to specific metrological and technical performance requirements as specified in the relevant Recommendation	Agreed.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-002	1	General		Te	<p>The use of components as defined above leads to increase vulnerabilities that needs to be mitigated.</p> <p>We therefore propose several additions to clause 6.2.2.1.</p>	<p>We have identified the following vulnerabilities with regards to use of components and propose to mitigate them as follows:</p> <ul style="list-style-type: none"> <li>• Not the correct component is used. <ul style="list-style-type: none"> <li>◦ Authenticity of the LR-software in the component needs to be checked, see our proposal to 6.2.2.1.4.</li> </ul> </li> <li>• The component is exchanged for another component <ul style="list-style-type: none"> <li>◦ The component is secured and protected against exchanging by means of a software seal, see our proposal to 6.2.2.1.3.</li> </ul> </li> <li>• The component is not available. <ul style="list-style-type: none"> <li>◦ Availability of the LR-software in the component needs to bechecked, see our proposal to 6.2.2.1.4.</li> </ul> </li> <li>• LR software in the component is manipulated. <ul style="list-style-type: none"> <li>◦ LR software shall have protected interfaces, see 6.2.2.1.2</li> <li>◦ LR relevant software shall be secured and protected, see 6.1.3.2</li> <li>◦ Integrity of the LR software in the component is checked by other components, see our proposal to 6.2.2.1.4.</li> </ul> </li> <li>• Non-legally relevant components can access the measurement data. <ul style="list-style-type: none"> <li>◦ Access to measurement data is checked, see our proposal to 6.2.2.1.6</li> </ul> </li> <li>• Non-legally relevant components can manipulate the measurement data. <ul style="list-style-type: none"> <li>◦ Measurement is secured and protected, for example measurement data is encrypted, see our proposal to 6.1.3.2.1 and 6.2.2.1.7.</li> </ul> </li> <li>• Measurement data is deleted before it is further processed. <ul style="list-style-type: none"> <li>◦ Before measurement data is deleted the transmitting component shall check that the receiving component has acknowledge that it has received the measurement data and that it was not</li> </ul> </li> </ul>	<p>Noted. These topics, also raised in the Dutch discussion paper provided separately, were used as the basis for the cloud/smartphone/component discussion with the entire PG. The results of the discussion are noted in the responses to individual comments, see rest of the document.</p>

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
						<p>corrupted, i.e. the integrity checks, see our proposal to 6.2.4.2.</p> <ul style="list-style-type: none"> <li>• In case of a dispute or problem the involved component cannot be identified. <ul style="list-style-type: none"> <li>○ All LR-components shall have a unique ID, see our proposal to 6.2.2.1.5.</li> </ul> </li> <li>• It might not be possible to completely secure and/or protect components, for example in the case of smartphone apps. In that case, the functionality shall be limited in relation to the level of securing and/or protection that can be achieved. <ul style="list-style-type: none"> <li>○ If only limited securing and/or protection can be achieved than the functionality shall be limited accordingly, see our proposal to 6.2.2.1.8.</li> <li>○ In case components with limited functionality and securing/protection are applied, they shall have limited access to the measurement data. The measurement data shall be prepared for transmission or storage for further processing by a component that can be fully secured and protected, that component ensure that the data is complete and protected. That component also ensure that the measurement result is printed or indicated.</li> </ul> </li> <li>• A smartphone is a mobile device which will not always be on side. This possess problems because for some instruments you need a display to verify the measuring instrument, in certain recommendation a display is even mandatory. For others the printer can be used, for example in the case of a weight price labeller or automatic gravimetric filling machines. <ul style="list-style-type: none"> <li>○ In the case a display is required or mandatory, a display shall be attached to the digital data processing unit and the tablet/smartphone shall be available on side.</li> <li>○ In the case that a display is not required or mandatory, a tablet/smartphone shall be available.</li> </ul> </li> </ul> <p>See our proposal 6.2.2.1.9</p>	

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-003	1	General		Te	<p>Before we implement new clauses for smart meters could we first establish what the use of the smart phone can be:</p> <ol style="list-style-type: none"> <li>1. Can the smartphone be used as an indicator? In the majority of OIML recommendations this means that the measurement data is further processed, i.e. a signal from a sensor, a analog data processing unit or a digital data processing unit is further processed to display the measurement result.</li> <li>2. Can the smartphone be used as a terminal, i.e. a digital device that has one or more keys (or mouse, touch-screen, etc.) to operate the instrument, and a display to provide the measurement results transmitted via the digital interface of an analog or digital data processing device.</li> <li>3. The smartphone is used as display, either the primary display or the secondary display.</li> <li>4. The smartphone is used as a remote storage device. If the protection of the measurement results is handled on the transmitting and receiving components than the smartphone does not contain any legally relevant software.</li> </ol> <p>Depending on the use and functionality of the legally relevant software on the smart phone specific requirements concerning protection and securing are necessary but also regarding availability, integrity, and authenticity of the LR SW in the smartphone and conditions regarding verification and re-verification needs to be specified.</p> <p>We propose to have this discussion first before we put a lot of effort into a use cases which would never be possible or acceptable.</p>	<p>To discuss the requirements of smart phones first.</p> <p>See the separate discussion paper we have send by e-mail.</p> <p>Is it feasible to have an annex for the use of smart phones and cloud storage, cloud computing, comparable to WELMEC guide 7.4, with examples what should be required for these use cases?</p>	<ol style="list-style-type: none"> <li>1. As discussed during the PG meeting, usage of a smartphones as indicator is technically not feasible, at the moment.</li> <li>2. With respect to the usage of a smartphone as a terminal, it was agreed that commands should be triggerable from any device, while restrictions on the display might apply. Any dedicated device should be able to fulfil requirements for a terminal.</li> <li>3. For the time being, the PG has decided to focus on “dedicate devices”. Whether or not communication with a smartphone within a closed network is allowed will be left up to the relevant project groups. With respect to open networks, the question is now obsolete because of the decision to focus on “dedicated devices”. In the meeting, it was clarified that for secondary indication BYOD should be acceptable.</li> <li>3. During the PG meeting it was agreed that protection measures for “dedicated devices” used as a (secondary) display in presence of a printer or primary indication will be left to the relevant PGs.</li> <li>4. As long as only the result is stored on the storage device, the storage device itself can be legally non-relevant. This would depend on protection measures for the result itself.</li> </ol> <p>Requirements proposed in NL-002 and referenced clauses for this use case appear to be useful and will be included in ICD, see other responses. The proposal for an additional annex with illustrative examples for smart phones and cloud computing was withdrawn by the proponent during the meeting.</p>

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-004	1	General		Te	The same for cloud computing. Putting an analogue component in the cloud is challenging and for digital components we must establish criteria regarding availability, integrity and authenticity. And of course the potential functionality, i.e. to further process the measurement data, as data storage device, as Point-of-sale device?	To discuss the requirements of cloud computing.  Is it feasible to have an annex for the use of smart phones and cloud storage and cloud computing, comparable to WELMEC guide 7.4, with examples what should be required for these use cases?	Currently, 1WD only addresses storage of measurement data in the cloud. This also appears to be in line with the use case considered by other member states. During the PG meeting it was agreed to only implement cloud storage examples in D31 for the time being. Nevertheless, new requirements should not prohibit other uses of the cloud. The proposal for an additional annex with illustrative examples for smart phones and cloud computing was withdrawn during the meeting.
NL-005	1	General		Te	D31 requires that the integrity and authenticity is checked and in some cases the availability. We would like to propose that checking facilities are incorporated in the clauses where such a check is required with reference to clause 6.1.4.1. See our proposals below.	For example: 6.1.3.2.1: in case of a software implemented seal, a checking facility shall check the integrity of the software. Or 6.1.3.2.3, a checking facility shall check the integrity of the software. Or 6.1.3.2.5, a checking facility shall check the presence and integrity of the audit trail.	Agreed. However, repeating the same requirement everywhere would probably be error prone. Suggestion to add a new short note in these clauses to reference 6.1.4.1, which already requires checking facilities if software is used for detection of such significant defects:  Proposal: "Note: In case of a software implemented seal, see clause 6.1.4.1 regarding requirements on checking facilities and appropriate reactions."
NL-006	1	General (6.2.2.1)		Te	With respect to separation of components we would like to propose to extend the requirements not only to the pairing parameters but also that a software-controlled component shall check the authenticity, integrity, and availability of another software-controlled instrument.  And add the requirement that through the (hardware) interfaces the LR software, data and parameters shall not be inadmissibly influenced, because that is not only applicable to OS but also to components.	See our proposals for 6.2.2.1.2, 6.2.2.1.3, 6.2.2.1.4 below	Noted.
NL-007	1	General (3.1.4 and 3.1.59)		Te	The difference between a built-for-purpose device and universal device becomes very thin if both are equipped with an Operating System. We therefore propose that an evaluation shall take place to ensure that if an operating system is present, it cannot be accessed directly.	See our proposal for 6.2.6.9 constraint for operation and 7.3.1, table 2.	Noted.
NL-008	1	General		Ed	For readability, we propose to change instrument/component to instrument or component.	See our proposals in our comments to remote verification.	Agreed.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-009	1	General		Ed	It was proposed to use the term component for a hardware part and module for a software part.	Change were appropriate part into module or component.	Since this is already proposed in SG3 results, this will be implemented.
NL-010	1	General		Ed	D31 now use the term “in the field” for instruments in use. We propose to use instead instruments in use.	Change “instrument in the field” to “instruments in use”.	It was agreed during the previous revision to use the term “in the field” when verification is addressed, and we should stick to that decision. There are only two other occurrences of “instrument in the field (6.2.8.1, 8.1). These will be changed to “in use” as suggested.
NL-011	1	General		Ed	D31 states now that influence on the “ <i>legally relevant characteristics of the measurement instrument should not occur</i> ”. In our opinion characteristics are usually maximum measuring range, temperature range, etcetera. But we are not sure if this cover the measurement result relevant data or the LR-software Typically, the type- and device specific parameters fix the legally relevant characteristics. In our opinion the legally relevant software and measurement data shall also be protected. We therefore propose to use “have an influence on the legally relevant software, parameters and measurement data”.	Change were appropriate “metrological characteristics” to “legally relevant software, parameters and measurement data”.	The term “characteristics” appears to be a little more general since it may also cover effects on the hardware of the instrument. Some definitions (see 3.1.1, 3.1.11) from V1 also use the term. Suggestion to add a new clause to chapter 4 to D31 “PGs shall decide which metrological characteristics (at least legally relevant software, parameters and measurement data) shall comply with the requirements laid out in the following clauses.” This way, we ensure that software assets are covered while PGs may extend the scope of the term for their needs.
NL-012	1	General		Te	We have introduced general requirements of audit trails but we believe that the same applies for event counters.	Add event counters to 6.1.3.2.5, see our proposal there.	Noted.
NL-013	1	General		Te	We propose to check and collect all documentation requirements in the document to include them in 7.1.2, to ensure that 7.1.2 covers everything.	To be executed if the document is in its more final stages.	Agreed. This is also related to DE-19.
NL-014	1	General		Te	We propose to check all examples ones all proposed changes from the different subgroups have been implemented. We have for the moment focused on the requirements.	To be executed if the document is in its more final stages.	Agreed. All examples will be checked again. once the requirements have been revised.
NL-015	1	General		Te	Many examples seem to contain requirements for which there exist be no relevant clause. Examples need to clarify a requirement. For all relevant requirements in an example, we propose to add a clause with that requirement.	Check examples for requirements. See for example our proposal for 6.1.3.2.1	At the moment, no example should include normative language. Nonetheless, all examples will be checked again for implicit requirements.
IR-01					<b>No comment</b>		Noted.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENOR/PG on each comment submitted
KR-06				Ge	Is smartphone app the only receiving device that is concerned? If smartphone app is allowed, other computing devices such as wallpad, tablet PC, PC, etc should be allowed as well		Indeed, in the provided examples the smartphone is the only indication device. Currently, there are no restrictions on the used hardware, so tablets etc. would also be acceptable. Nevertheless, the examples will be revised, anyway, once the use of smartphones has been discussed.
NL-016	1	2.1	Note 2	Ed	This document addresses security of data, parameters, and software. We propose to reflect that in note 2	Change to: This Document addresses some aspects concerning data, parameter and software security. In addition, national regulations for this area need to be considered	Agreed.
NL-017	1	3		Ed	We wonder if terms and definitions from D11 are used in this document.		Indeed, there is one definition from D11 currently in use in D31, see 3.1.12. Other references to D11 may be found in 6.1.4.2
NL-018	1	3.1.1		Te	We would like to propose to bring this definition more in line with the definition in 3.1.6 for an Event, see also our proposal there.	Change to: continuous data file containing a time stamped information record of events, e.g. changes in the value of the legally relevant parameters or a modification or update of the legally relevant software, or other activities that are legally relevant and which may influence the legally relevant software, parameters and measurement data. Adapted from [OIML V 1:2013, 6.05]	Since this is a V1 definition that stems from D31 we should be able to modify it. TC1 should be informed once the change has been agreed upon.  However, as we should refrain from repeating the definition of “event” here, we should simply implement the proposed note to 3.1.16 (see NL-020).  In 3.1.1, we can then simply add the following: “3.1.1 Note: Regarding examples for events logged in an audit trail, see 3.1.16.”
NL-019	1	3.1.15		Te	Characteristics are usually maximum measuring range, temperature range, etcetera. Typically type- and device specific parameters fix the legally relevant characteristics. In our opinion the legally relevant software, parameters and measurement data should also be protected.	Change to: continuous data file containing an information record of failures or significant defects that have an influence on the legally relevant metrological software, parameters and measurement data of the measuring instrument.	Agreed. However, we should follow the proposal given in response to NL-011 and keep the term “metrological characteristics” here to allow also for HW effects. With the introduction of the new clause 4.6 on metrological characteristics, we can then leave 3.1.15 as it is.
NL-020	1	3.1.16		Te	We propose to add a note to make in line with 3.1.1 Audit trail. Also, this definition is not very accurate in line what we are trying to achieve in D31. We therefore propose to add a note to clarify what an event is.	Add: Note: For the purpose of this Document, events are considered changes in the value of the legally relevant parameters, or a modification or update of the legally relevant software, or other activities that are legally relevant and which may influence the metrological data and/or characteristics .	Agreed, the suggested note would help new readers of D31.



Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-021	1	3.1.21		Te	The term unauthorized leaves the door open for interpretations. We propose to change this, this will also bring this definition in line with other changes proposed by the subgroup Terminology and with the requirement in clause 6.1.3.1 prevention of misuse. See also our proposal there.	Change to: 3.1.21 Integrity (of software, measurement data or parameters) Assurance that the legally relevant software, measurement data or parameters have not been subjected to any unintentional or accidental changes or intentional misuse while in use, transfer, storage, repair of maintenance.	Since integrity can also address legally non-relevant assets, we should not add that adjective. Also, as “intentional misuse” has no connection to asset integrity, that addition would be misleading. We should use “inadmissible changes” instead. The other proposed changes will be implemented. The new definition would read, “assurance that the software, measurement data or parameters have not been subjected to any unintentional or accidental changes or <u>inadmissible changes</u> while in use, transfer, storage, repair <u>or</u> maintenance”
DE-04		3.1.24		te	The term “intrinsic error” is only used in “fault” definition.	The definition for “intrinsic error” should be deleted.	Agreed.
NL-022	1	3.1.27		Ed	We would propose to delete the term part in the title of the definition	Change to: 3.1.27 Legally relevant software	This will be implemented as it is part of the SG3 results.
AU-02		3.1.31		Ge	Measurement data is defined as data used during the measurement process – which appears to be different to the measurement result (i.e. the outcome of the measurement process). But the term measurement data is used to refer to measurement results. For example, clauses 6.2.5.2 and 6.2.5.2 refer to measurement data and provide example which refer to the measurement result. The measurement data described in 3.1.54 and 6.2.4.4.1 also suggests that the measurement result should be part of measurement data.	Clarify the terms and usage.	This should be solved by SG3 results (including the revised Annex C).
NL-023	1	3.1.31		Ed	For the purpose of clarification, could we add a reference here to Annex C in the note?	Change to: Note: Measurement data includes measurement result relevant data and measurement process data. See Annex C.	Agreed. The reference would help readers in understanding measurement terminology.
NL-024	1	3.1.38		Ed	For the purpose of clarification, could we add a reference here to Annex C in the note?	Change to Note: Examples of measurement result relevant data include digital number or analogue value originating from a sensor or measuring instrument ID, in cases where it is part of the measurement result, see Annex C.	Agreed.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AU-01		3.1.4		ed	The new and old wording of the note are phrased as requirements.	Suggest amended as: “Includes devices that may not incorporate an operating system.”	Agreed, the current note uses normative language and should be rephrased. Since the new proposal does not address accessibility of the operating system at all, we should include both as follows: “Note 1: Built-for-purpose devices include devices that may not incorporate an operating system. Note 2: If an operating system is present, it is not directly accessible.”
AU-03		3.1.43		ge	The interface may include data flows from the legally relevant software, e.g. the interface between the processor and the indicating device.	Suggest the term is amended to: “legally relevant software interface that handles all data flow to <b>and from</b> the legally relevant software part <b>in order</b> to prevent inadmissible influences”	Since we are only trying to protect the legally relevant software from external influence and not vice versa, addressing data leaving the legally relevant software is not necessary.
NL-025	1	3.1.43		Te	We wonder if the second paragraph of clause 6.2.2.2.2 should not be stated in the definition as a note, because it seems to explain what is expected from the protective interface.  And considering that we use the term protective interface in more clauses, we would propose to either	Change to: Legally relevant software interface that handles all data flow to the legally relevant software module to prevent inadmissible influences  Note: The protective interface consists of program code and dedicated data domains. Defined coded commands or data are exchanged between components or modules. In case of communication between software modules by storing to the dedicated data domain by one part of the protective interface and reading from it by another part of the protective interface. So, the program code that deals with this writing and reading is part of the protective interface.	Moving the second paragraph from 6.2.2.2.2 here would likely decrease visibility of the text as a clause would be turned into a note in a definition. Exchanging “part” for module has already been proposed by SG3 and will be implemented.
NL-026	1	3.1.46		Te	We propose to add checking facilities to detect the deletion of the audit trail, integrity breach in the parameters, unauthorized updates and accidental software changes due to physical effect to reflect this note. See our <a href="#">proposal</a> at the relevant clauses below		Noted.
NL-027	1	3.1.46	Note	Te	We propose to reword this note and delete the term unauthorised in relation to parameters because that can lead to misinterpretations.	Change to: Note: Example of a significant defect include: a) deletion of the audit trail, b) misuse of the parameters by manipulation, c) unauthorised updates, d) accidental software changes due to physical effects	Since “misuse of parameters” is an action that can be performed without classifying as a significant defect, we should not mention it here. Suggestion to use “inadmissible parameter changes” instead.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AU-04		3.1.48		ed	The note appears to be expressed as a requirement.	Suggest moving the note to be an additional requirement of 6.1.1. (see AU comment below)	Since one important aspect of software identification is the possibility to check it when needed, we should rephrase the note as a statement and add a reference to the requirement instead: “Note: Software identification may be checked on an instrument whilst in use, see 6.1.1.”
AU-05		3.1.51		Ed	The note appears to be expressed as a requirement.	Suggest moving the note to be an additional requirement of 6.1.3.2.1. (see AU comment below)	As the explanation provided by the note is useful, we should leave it here, rephrase it as a statement and add a reference to the respective requirement in clause 6.1.3.2.4, where it should already be covered.
NL-028	1	3.1.51		Te	We propose to add component to the first sentence	Change to: Protection of a measuring instrument or component software or data domain by a hardware of software implemented seal	Agreed. However, 3.1.51 has also been modified by SG3 and we should carefully combine both proposals.
NL-029	1	3.1.51	Note	Te	The note seems to be focused on hardware seals, because an audit trail or event counter is not removed, damaged or broken. This also does not cover cryptographic means. We propose to add a clarification concerning software seals.	Change to: Note: The hardware seal must be removed, damaged or broken to obtain access to change software. A software seal records the event, i.e. either the non-resettable counter is incremented each time an event occurs, see 3.1.17, or a data file, containing time stamped information, records the event, see 3.1.1. Or the software is protected by cryptographic means to ensure integrity and authenticity, see 3.1.8.	The first two parts of the new note appear to be in line with the current meaning of 3.1.51. The third part, however, does not seem to address any kind of seal in particular and should be left out. The first two proposed notes will become examples as they appear to illustrate the definition.
NL-030	1	3.1.52		Te	We propose to change <i>part</i> into <i>module</i>	Change to: Separation of the software in a measuring instrument or component which can be divided into a <i>legally relevant</i> module and a <i>legally non-relevant</i> module.  Note: These modules communicate via a software interface	This has also been proposed by SG3 and will be implemented in 1CD.
NL-031	1	3.1.54		Te	In this document measurement data is also stored before the measurement process is completed. See also 3.1.31: measurement data is data used during the measurement process. We understand that this is a V1 definition but nevertheless, we propose to change this to reflect the use in this document.	Change to: Device used for storing measurement data that is necessary to construct the measurement result.  Adapted from [OIML V1: 2013, 6.07]	Agreed. The term should cover all devices used for legally relevant data storage. Since the V1 definition stems from D31, we can simply inform TC1 about this change once approved by the PG.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
FR-01		3.1.55		ge	<b>Time stamp</b>  Time stamp definition always associate date and time to an event.	Keep the original more accurate definition proposed in OIML D31:2019	The problem with the old definition was the use of the word “event” which is limited to the meaning given in V1 6.06. To make time stamps also applicable for other “events”, the last part of the definition in D31:2019 was removed. Suggestion to expand the definition to the following instead: “unique value, e.g. in seconds or a date and time string denoting the date and/or time at which a certain incident (e.g. measurement or event) occurred” This would avoid conflict with the term “event”.
US-02	1	3.1.55		ed	By removing the term event the definition is too general. Under this definition also a wrist watch can be considered a time stamp.  The term time stamp is always related to a certain event. This event can be anything including measurement.	“unique value, e.g. in seconds or a date and time string denoting the date and/or time <b>at which an event occurred</b> ”	The term “event” caused problems in the old definition as it has a very limited scope, see V1 definition 6.06. This should be solved by the response to FR-01.
AU-06		3.1.56		Ed	Is the last part of the definition needed to qualify what may happen to the data after it is transmitted?	Suggest deleting “where they are further processed” from the definition.	True. Indication at the receiver would probably not qualify as “processing”. Therefore, we should generalize the definition.
AU-07		3.1.58		Ed	The wording of the example requires review.	Suggest: “Considering a measuring instrument intended for the dynamic measurement of quantities of liquids other than water, the range of kinematic viscosities of a turbine meter is a type-specific parameter, determined by the type evaluation of the turbine meter. All the turbine meters manufactured in accordance with that type use the same viscosity range.”	Agreed.
NL-032	1	3.1.59	Note	Te	It should not be possible to have undeclared interfaces because than we cannot check if it meets the requirements, i.e. is the interface protected and if not, is the interface disabled. And how can we check that communication via open software interfaces is protected by means of the operating system if these interfaces are not declared?	Delete the note	Since this topic has previously been discussed during the Dordrecht meeting, we should only modify the definition if agreed upon by the entire PG. During the PG meeting, it was agreed to delete the note.
NL-033	1	4.5		Te	Measurement data always needs to comply with the requirements. It is the responsibility of the PG to defines which data is considered measurement data that needs to comply with the requirements. We also propose to add a link to Annex C.	Change to: PGs shall decide which data is considered measurement data that shall comply with the requirements, see Annex C. The manufacturer shall document the required metadata where necessary.	As we cannot not rule out the possibility for legally non-relevant measurement data, we should rephrase the clause to: “PGs shall decide which measurement data <u>is legally relevant</u> <u>and</u> shall comply with the requirements, see Annex C...”

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-034	1	5.2	Last paragraph	Ed	Could we change security weaknesses in vulnerabilities?	Change to: A deep analysis of the software shall be performed when a raised risk level is required in order to detect software deficiencies or security vulnerabilities. On the other hand, mechanical sealing (e.g. sealing of the communication port or the housing) should be considered when choosing the examination level.	Agreed. “Vulnerabilities” appears to be the appropriate term
AU-08		6	Examples	Gen	Some example only relate to some requirements within the clause – not all requirements. There is a risk that PGs or readers will assume the examples provide a solution for the whole clause. For instance: In clause 6.1.3.1, the examples do not provide for the requirement that ‘Legally relevant software shall be secured against accidental or unintentional changes.’ In clause 6.1.5, the example does not provide for the requirement that the ‘time stamp shall be in a consistent format...’. The example only relates to the reliability of the internal clock.	Clarify the scope of examples – that is, for which requirement(s) does the example provide a solution?	All examples will be checked to ensure that they either cover all requirements in a subclause or to be marked as suggested.
AU-09		6		Gen	Some of the text refers to a measuring instrument/component. Component is not defined in this document.	Add a definition of component.	Agreed. Suggestion to use the proposed definition from NL-001.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
DE-05		6		Ed	<p>To avoid redundancy and give a better introduction, we propose to merge the introductory texts of 6.1 and 6.2 here.</p>	<p><b>6. Requirements for measuring instruments with respect to the software</b>  The requirements are separated into general requirements (6.1), applicable to all kinds of measuring instruments, and requirements for specific configurations (6.2), additional requirements for technical features not applicable in all areas of legal application.</p> <p>In the examples, where applicable, both normal and raised risk levels are shown. Notation in this Document is as follows:  (I)        Technical solution acceptable in case of normal risk level;  (II)        Technical solution acceptable in case of raised risk level (see 5).</p> <p><b>6.1 General requirements</b>  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.</p> <p><b>6.2 Requirements specific for configuration</b>  The requirements given in this clause are based on typical technical solutions in information technology, although they might not be common in all areas of legal applications. When following these requirements, technical solutions are possible that show the same degree of security and conformity to a type as instruments that are not software-controlled.</p>	<p>Okay, the proposed change would also solve the issue raised in AU-30. However, the proposed texts for 6.1 and 6.2 should be 6.1.1 and 6.2.1, instead, to comply with and harmonise the current hierarchy of clauses.</p>
AU-10		6.1.1	Note 1	Ed	<p>I am not sure that the word ‘conformable’ at the end of the second sentence correctly conveys the intent of the sentence.</p>	<p>Suggest to change sentence to:  ‘The software identification supports surveillance personnel and persons affected by the measurement to determine conformance.’</p>	<p>Agreed. For better readability we should change “conformance” to “conformance of the measuring instrument”</p>

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AU-11		6.1.1	Notes	Ed	The numbering of Notes needs to be updated.	The numbering of Notes needs to be updated.	B6-2 requires consecutive notes to be numbered. The third (unnumbered) note in 6.1.1 addresses a different aspect of the clause in a different location and therefore does not need a number. However, having such “aspects” of clauses within a clause is a violation of B6-2, too. These should be separate subclauses. The issue should be solved once DE-03 has been implemented in 2CD.
AU-12		6.1.1	Note 1	Ge	Note 1 is a requirement, which should become part of the clause.	Note 1 should be moved into the body of the clause.	Since note 1 is a requirement on the manufacturer rather than on the software (which is the concern of this document), we will have to leave it as a note. However, the rephrasing suggested in DE-07 should get rid of the normative language in the note altogether.
AU-13		6.1.1	Note 2	Ge	Note 2 theoretically applies to all of clause 6. As such it should be moved to either: <ul style="list-style-type: none"> <li>• Clause 6.1; or</li> <li>• Clause 3 as a term with an explanatory Note</li> </ul>	Move Note 2 to clause 6.1 as it applies generally to the whole clause 6.	Since the term is also used in clauses 7 and 8, we should move the note to clause 3 (general terminology).
AU-14		6.1.1		ge	A general requirement should be included that requires the software identification to be accessible while the instrument is in-service. From AU comment 3.1.48.	Suggest: “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-service.”	Agreed. To keep the current terminology of requirements, we should use “available” instead of “accessible”.
DE-06		6.1.1 Terminology		te	The clause reads “Software of a measuring instrument shall be clearly identified.” There is no official definition of the term “software” in D31.	Change to “software modules of a measuring instrument shall be clearly identified.”	Agreed. This would also follow the logic behind SG3 results.
DE-07		6.1.1		Te	Note 1 contains a requirement	Change to “If measuring instruments in use need to conform to a certified type, software identification enables surveillance personnel...”	This would solve the issue raised in AU-12.
NL-035	1	6.1.1	First paragraph	Ed	We would like to bring the requirement in line with the examples, instead of “clearly” use “unambiguously”.	Change to: Software of a measuring instrument or component shall be unambiguously identified.	Requiring an unambiguous identifier appears to be in line with the current intention of the clause.
NL-036	1	6.1.1	Note	Ed	We propose to add a reference to clause 6.1.3.2.3	Change to: Note: The software identification is a legally relevant parameters, see clause 6.1.3.2.3.	Since 6.1.3.2.3 imposes requirements on parameters but does not explain the term itself, we should keep the note as it is. However, the formatting should be updated to follow B6-2 guidelines.
NL-037	1	6.1.1	Second paragraph	Informative	If the proposal for remote verification is accepted, we need to adjust this.		Noted.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
JP-01		6.1.1 Software identification	1 <sup>st</sup> para. and notes.	Te/ed	<p>The first paragraph is rather ambiguous in meaning. Our understanding is that “identification” of the 2<sup>nd</sup> sentence means a token identifying software defined in 3.1.48. We propose to amend this paragraph as shown in the right column.</p> <p>All notes should be placed at the end of the clause.</p> <p>It might not be appropriate to regard the whole identification as a legally relevant parameter when the identification consists of more than one part. We propose to add another sentence to the note and move it to the end as Note 3.</p> <p>To facilitate readers’ understanding, it is better to introduce the concept of software separation briefly in 6.1.1 with a link to 6.2.2.2.</p>	<p>We propose the following amendments in the 1<sup>st</sup> paragraph.</p> <p><i>6.1.1 Software Identification</i></p> <p><i>Software of a measuring instrument / component shall be clearly identified. The <u>software</u> identification (3.1.48) linked to the software may consist of more than one part. <del>But</del> at least one part shall be dedicated to the legal purpose.</i></p> <p>We propose to move the Note to the end of this clause as Note 3 with an amendment, and add Note 4 as shown below.</p> <p><i>Note 1: Each measuring .... is conformable.</i></p> <p><i>Note 2: Unless stated otherwise, .... certificate.</i></p> <p><i><u>Note 3: A software identification is a legally relevant parameter. When the software identification consists of more than one part, at least the part dedicated to the legal purpose shall be included in the legally relevant parameter.</u></i></p> <p><i><u>Note 4: A software separation (3.1.52), which includes an identification of a legally relevant part, may be considered depending on the structure of the measuring instrument/component. In this case, applicable requirements are given in 6.2.2.2.</u></i></p>	<p>The proposed editorial changes are acceptable.</p> <p>The problem of moving all notes to the end of the clause should be solved once DE-03 has been implemented in 2CD.</p> <p>The new proposed note 3 should be rephrased to avoid expressing requirements in notes: “A software identification is a legally relevant parameter. When the software identification consists of more than one part, at least the part dedicated to the legal purpose <u>constitutes</u> a legally relevant parameter.”</p> <p>The new proposed note 4 will also be included in 1CD.</p>
AU-15		6.1.2	Para 4	Gen	<p>Given the scope of this Document, it is interpreted that no hidden or undocumented functions or parameters only relates to legal metrology. Depending upon the application and/or jurisdiction in which a measuring instrument and software module is being used, there may be a separate requirement to hide certain functions from some users.</p>	<p>An advisory note should be included to clarify that the requirement regarding hidden functions only applies to legal metrology. Separate national regulations may govern software functions outside the scope of legal metrology.</p>	<p>Agreed. The wording could be as follows: “The requirement regarding hidden functions only applies to legal metrology.</p>
NL-038	1	6.1.2	Second paragraph	Ed	<p>We deleted accompanying information elsewhere, we propose to do the same here.</p> <p>We propose not to use measurement result here to highlight again that measurement result relevant data needs to be specified by the specific recommendations or national legislation.</p>	<p>Change to:</p> <p>The measured quantity value and measurement result relevant data required by specific Recommendations or by national legislation shall be displayed or printed correctly.</p>	<p>Agreed. This occurrence of “accompanying information” appears to be left over from the previous revision.</p>
AU-16		6.1.3.1	Para 1	Gen	<p>This Document generally seems to use ‘shall’ in relation to requirements, and ‘should’ in relation to guidance for the reader.</p>	<p>Replace: ‘The presentation of the measurement results <i>should</i> be unambiguous for all parties affected.’</p> <p>With: “The presentation of the measurement results <i>shall</i> be unambiguous for all parties affected.’</p>	<p>Actually, “should” as a normative verb allows exceptions from a requirement if they are properly explained. In the PG meeting, it was agreed to change the verb to “shall”.</p>
DE-08		6.1.3.1		Te	<p>Prevention of misuse (6.1.3.1) is not a protective measure (6.1.3)</p>	<p>Turn 6.1.3.1 into 6.1.x as a separate requirement clause.</p>	<p>Since the requirement would still be the same, moving it to a separate clause is acceptable.</p>



Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
FR-02		6.1.3.1		ge	<b>App for smartphones</b>  The word “app” is used in many examples but never defined nor having specific requirements on use.	A definition should be given first. Then, requirements concerning specificities compared with software should be studied. Conditions on legally relevant apps should also be implemented in the document.	At the meeting, it was agreed to provide a definition from an ISO document or from a similar source. After the meeting the following wording was proposed by France: “computer program or software application designed to run on a mobile device such as a phone, tablet, or watch” cited from the Cambridge Dictionary. This will be included in D31.
FR-03		6.1.3.1		te	<b>Smartphones</b> <b>Smartphones are introduced in several examples in the document. The use of this type of tools will increase in the future. A clause with minimal requirements for smartphone seems necessary.</b>	Create a paragraph dealing with minimal requirements for smartphones.	During the PG meeting it was concluded that such a clause is not needed given various additions to existing clauses proposed in NL comments (in particular with respect to components).
KR-01		6.1.3.1		Ge	Regarding Example 2), We think the definition and scope for 'matrix code' is required.	Please define “matrix code” in terminology.	This should be solved by the changes resulting from JP-03.
KR-02		6.1.3.1		Ge	Should smartphone app considered a legally relevant part? If so, smartphone app should be included in the scope of software verification		This is correct. However, this will depend on the individual implementation, of course.
NL-039	1	6.1.3.1		Te/Ed	We propose to reword and reshuffle this clause. The example is aimed at obtaining correct measurement results therefore we propose to moved the last two sentence below the example.	<p>The software of a measuring instrument shall be designed in such a way that no unreasonable demands are required from the use to obtain a correct measurement result.</p> <p>Note: Software-controlled instruments are often complex in their functionality. The user needs good guidance for correct use and for achieving correct measurement results.</p> <p>Examples: 1)(I) The user is guided by menus. The legally relevant functions are combined into one branch in this menu. If any measurement data might be lost by an action, the user is warned and requested to perform another action before the function is executed. See also 6.2.3.</p> <p>The software and measurement data shall be secured against unintentional or accidental changes and intentional misuse.</p> <p>The presentation of the measurement results should be unambiguous for all parties affected.</p>	Moving the last two sentences below the example would make clause and example more easily comprehensible. The suggested rewording, however, would change the focus of the clause from possibilities of misuse to demands for obtaining a correct result. Instead the PG should discuss if an additional requirement for demands on the user is needed. This was agreed upon during the PG meeting.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-040	1	6.1.3.1	Example 2	Te	<p>Example 2 needs to be discussed. How should the instrument be physically protected? And is physically protected sufficient since the smartphone app is probably communicating with the instrument through Bluetooth or Wi-Fi?</p> <p>Why only one single command and what can this single command initiate? Zero-setting and tare setting, which might be necessary to obtain a correct measurement result.</p> <p>How can a consumer validate the signature contained in the matrix code?</p> <p>If we want to ensure that the consumer trust the send result is it not better to require that the instrument displays the measurement result as well so the consumer can compare the received value? Of course, we than limit the use of the smart phone to a terminal with a secondary display.</p> <p>We would argue that we should first discuss what functions are possible with a smartphone before given requirements for smartphones.</p>		<p>The example clearly states that there is only one command that can be entered through communication interfaces to start a measurement. The functionality of the command should, therefore, be clear. Protection for such a scenario is already described in 6.2.2.1.</p> <p>As agreed during the PG meeting, it would appear to be useful to limit the discussion to tablets/smartphones etc. used as a component of the measuring instrument that is owned by the user of the measuring instrument (as opposed to bring-your-own device). If such a dedicated device is used for legal purposes, protection is necessary. A pure software solution might also be possible. Project groups might impose additional restrictions.</p> <p>Regarding the consumer's trust in displayed measurement results, this should be solved by the responses to NL-003.</p>
US-03	1	6.1.3.1	Example 2	ed	<p>"Matrix code" is not a commonly used term. It might raise questions. For clarity it might be better to stick to more common terminology to explain the example</p>	<p>"... the result is cryptographically signed and sent back to the smartphone as clear text accompanied by <b>metadata</b> that contains measurement result and cryptographic signature. In case of doubt, the correct indication of the result can be checked by all parties by validating the signature contained in the <b>metadata</b> ..."</p>	<p>This should be solved by the change proposed in JP-03.</p>
JP-02		6.1.3.1 Prevention of misuse	Example 2)	Te/ed	<p>Although the second example mentions proper treatment of measurement results, this content is not for prevention of misuse.</p>	<p>We propose moving this example to 6.2.5.3 (protection of transmitted data).</p>	<p>The purpose of the example was to address prevention of misuse on consumer devices. Based on the outcome of the smartphone discussion at the PG meeting, the example will be revised.</p>
JP-03		6.1.3.1 Prevention of misuse	Example 2)	Ed	<p>The meaning of "matrix code" is unclear. Does it mean a two-dimensional bar code?</p>	<p>It is better to use an expression "two-dimensional bar code".</p>	<p>Agreed. "Two-dimensional bar code" is better.</p>

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AU-17		6.1.3.2		Gen	This section may need review for its scope and use of the terms: The clause is titled ‘Evidence of intervention’, but the terms ‘software protection’ and ‘sealing’ are broader than evidence of intervention. For instance, clause 6.1.3.2.1 example 1 does not provide for evidence – but rather preventing swapping of software by encryption. Clause 6.1.3.2.2 does not relate to evidence of intervention at all. Clause 6.1.3.2.4 talks about making intervention impossible or evident.	Rename clause 6.1.3.2 or restructure.	Agreed. Apart from 6.1.3.2.2, however, all subclauses appear to fit under the title “evidence of an intervention”. Since we also address interface protection (6.1.3.2.2) and prevention of intervention (6.1.3.2.4) we could rename 6.1.3.2 to “Evidence and prevention of intervention”
DE-09		6.1.3.2		Ed	The title of the clause has the same meaning as 6.1.3 see definition 3.1.51.	Merge this requirement with 6.1.3. See also our comment on 6.1.3.1.	Once 6.1.3.1 has been moved outside 6.1.3, 6.1.3.2 will be the only subclause left and can become 6.1.3. The title will be amended as put forth in response to AU-17.
DE-10		6.1.3.2		Ed	Multiple requirements in a single clause. Not all of them fit the topic “software protection”.	The phrase “Software shall be secured against...” is not fitting for “software protection” and should be moved to a different location.	The solution proposed in AU-17 should solve this issue.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-041	1	6.1.3.2		Te/Ed	We propose to add the note of 6.1.3.2.4 here and reword the clause.	<p>Change to:</p> <p>Software shall be protected against unintentional or accidental changes, for example due to physical effects, and intentional misuse, i.e. modification, loading or changes by swapping the memory device, unauthorised updates.</p> <p>Note 1: Downloading software into the measuring instrument or component is allowed if the requirements for download are fulfilled, see 6.2.8.3 and 6.2.8.4.</p> <p>Software shall be protected in such a way that evidence of an intervention shall be available. Mechanical sealing or software seals shall be used to protect the measuring instruments or components.</p> <p>In case of a software implemented seal, a checking facility shall check the integrity of the software and in the case of an irregularity an appropriate reaction shall be required. See 6.1.4.1.</p>	<p>Currently, 6.1.3.2.1 requires protection against <b>any</b> kind of intervention and we should, therefore rephrase the first proposed sentence to “Software shall be protected against any changes, for example due to physical effects, and intentional misuse, i.e. modification, loading or changes by swapping the memory device, unauthorised updates.” The extended list of examples will be added.</p> <p>Moving the note from 6.1.3.2.4 here is acceptable.</p> <p>Agreed. However, if SG3 results are accepted, this will be part of the definition of “software protection”, anyway, which might make this change superfluous.</p> <p>Regarding checking facilities, we should follow the proposal in response to NL-005 and add: “Note: In case of a software implemented seal, see clause 6.1.4.1 regarding requirements on checking facilities and appropriate reactions.”</p>
AU-18		6.1.3.2.1		ge	Include a specific requirement regarding the nature of the seals. From AU comment 3.1.51. Unless 6.1.3.2.4 is considered equivalent and sufficient.	<p>Suggest additional requirement: “Where seals are used (either mechanical or electronic), they shall provide evidence of intervention. Access to legally relevant software modules shall require that the seal(s) is removed, damaged or broken.”</p> <p>Or not if 6.1.3.2.4 is considered equivalent and sufficient.</p>	6.1.3.2.4 should already cover this aspect. The new reference in 3.1.51 (see response to AU-05) should provide sufficient additional explanation.
AU-19		6.1.3.2.1	Note	Ed	The note uses the term “consumer device”, we suggest this is changes to “universal device” to align with 3.1.59.	Change “consumer device” to “universal device”.	As agreed during the PG meeting, we will focus on “dedicated devices” for the time being. Therefore, the term “universal device” will be used here.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AU-20		6.1.3.2.1	Example 1	Ge	This example includes the text ‘The key for decryption is hidden in a program that is part of the legally relevant software...’. This is confusing given clause 6.1.2 states ‘No hidden or undocumented functions or parameters shall exist’.	Clarify the meaning of hidden.	Agreed. The sentence will be changed to “The key for decryption is included in a program...”
KR-03		6.1.3.2.1 Note		Ge	The assumption that the legally relevant software runs on the consumer device such as smartphone seems unrealistic. We think that the legally relevant software should be within the scope of the "meters and peripheral components".	Please change the syntax to the actual use cases.	The majority of comments to the smartphone examples seem to indicate, that we should restrict ourselves to dedicated devices as part of the measuring system, rather than “bring-your-own-device” scenarios. As agreed during the PG meeting, we will focus on “dedicated devices” for the time being. The note will be revised accordingly.
NL-042	1	6.1.3.2.1	Note	Te	<p>This restricts the use of an instrument to a terminal, see also the example under 6.1.3.1. We would like to discuss this.</p> <p>Software should be protected.</p> <p>If we protect the measurement data than we can check if the App did not modify the measurement data but not if the software behaves correctly.</p> <p>This also suggest that the App does not need to be protected. In our opinion this is not correct. Perhaps replacing the App cannot be avoided but the App can be protected against changes</p> <p>We propose to discuss the possible uses of the App and the necessary securing and protection measures before we finalize this.</p>	To be discussed	As discussed during the PG meeting, requirements for dedicated devices will ensure that the software (app) cannot be modified or exchanged. The note will be amended accordingly, see also response to KR-03.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-043	1	6.1.3.2.1	Example	Te	<p>The first example does not only describe a securing measure to avoid exchange of the legally relevant function but also a way to protect the measurement data to be used by non-legally relevant software.</p> <p>However, this function is not incorporated in the clause, we therefore propose to add that measurement data shall be protected and secured.</p> <p>This then also covers the requirement in the note that measurement data shall be protected.</p> <p>We are not sure if the link in example 1 to 6.2.2.2.4 is correct.</p>	<p>Add after the first sentence of 6.1.3.2.1</p> <p>Measurement data shall be protected and secured.</p> <p>We are not sure if the link in example 1 to 6.2.2.2.4 is correct. Should it not be 6.2.2.2.2?</p>	<p>Currently, we only require protection of software, while measurement data are protected during transmission or storage.</p> <p>The proposed change will need to be discussed with the entire PG.</p> <p>Regarding the reference, it should be updated to 6.2.2.2.2. This will be corrected.</p> <p>Rephrased proposal from the PG meeting: During processing, measurement data shall be protected and secured.</p> <p>Proposal for a new note from the PG meeting: Protection of the measurement data can be achieved by ensuring that only legally relevant software can process them and that all interfaces are protected.</p>
SI-1		6.1.3.2.1	Note	te	<p>Since the intention of the usage of the smartphones was only for indication (if understood correctly), the Note is written to broad and opens the usage of smartphones for hosting of LR SW where protection against exchange of LR SW is practically impossible for example under Android or iOS.</p>	<p>Should be discussed under D1 what is the intention/scope of usage of smartphones and other consumer devices (BYOD).</p>	<p>Comments from other member states indicate that the revision should also address processing of Data on smartphones. The comment was withdrawn by the proponent at the PG meeting.</p>
AU-21		6.1.3.2.2	Para 1	Ed	<p>Suggested change to make the wording clearer. Also is there a difference between ‘legally relevant parameters’ (which are defined) and ‘legally relevant characteristics’ (which are not defined)?</p>	<p>Any function that can be activated by the user interface shall:</p> <ul style="list-style-type: none"> <li>- be clearly documented (see 7.1)</li> <li>- not able to influence the legally relevant characteristics of the instrument</li> </ul>	<p>The term “characteristics” will be replaced, see response to NL-11.</p> <p>Proposal to use a combination of this suggested change and the one from NL-044:</p> <p>All inputs from the user interface are handled by a protected interface. Any function that can be activated by the user interface shall:</p> <ul style="list-style-type: none"> <li>- be clearly documented (see 7.1)</li> <li>- not able to influence the legally relevant characteristics of the instrument</li> </ul>
AU-22		6.1.3.2.2	Para 1	Ge	<p>What is the intent of the note? It seems to only be saying the requirement is assessed by the examiner. This would seem to be true for all requirements. Is it needed?</p>	<p>Remove the note or clarify the meaning.</p>	<p>The note is needed, as we usually do not limit the functionality of the instrument in other clauses.</p> <p>Suggestion to rephrase the note to: “The type evaluation authority decides whether the list of documented functions is acceptable.”</p>
AU-23		6.1.3.2.2	Note	Ed	<p>Should examiner be more generally expressed as ‘type evaluation authority’ or ‘relevant authority’?</p>	<p>Consider changing ‘examiner’ to ‘type evaluation authority’.</p>	<p>Agreed. “Type evaluation authority” should be the correct term.</p>

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AU-24		6.1.3.2.2	Example	Ge	The example appears to only provide a solution for activating documented functions. How does this check/ensure these documented functions do not influence the legally relevant characteristics? Is this assumed to be true, or is it assessed elsewhere?		In combination with the type evaluation authority's approval of the list of commands, the required protection of the interface should be achieved. The example will be modified to explain this.
DE-11		6.1.3.2.2		Ed	Not related to software protection	Relates to (current) 6.1.3.1 and should be merged with it.	The solution proposed in AU-17 should solve this issue.
NL-044	1	6.1.3.2.2		Te	<p>It seems that much of the protection measures include a protective interface. We are in favour of explicitly mentioning this in the requirement.</p> <p>See also the remarks of the secretariate at 6.2.2.1.2: change proposed after review of D31 in TC9/SC1/p1. This already appeared to be required by the next sentence, which focuses on the examiner/manufacture rather than the instrument.</p> <p>Characteristics are usually maximum measuring range, temperature range, etcetera. Typically type- and device specific parameters fix the legally relevant characteristics.</p> <p>In our opinion the legally relevant software, parameters and measurement data should be protected.</p> <p>We propose to change this throughout the document to avoid possible misinterpretations.</p>	<p>Change to:</p> <p>All inputs from the user interface are handled by a protected interface. Only clearly documented functions, see 7.1.1, shall be activated, which do not influence the legally relevant software, parameters and data of the instrument or component.</p>	<p>Agreed. This clarification appears to be in line with the current focus of 6.1.3.2.2. Suggestion to combine it with the proposal from AU-21, see response to AU-21.</p> <p>All other instances of interface protection will be checked accordingly and modified where necessary.</p>
NL-045	1	6.1.3.2.2	Example	Te	<p>The example describes a protected interface, we propose to make this explicit.</p> <p>We believe that by definition a protected interface is parts of the legally relevant software, see 3.1.43, so we can delete the last sentence.</p>	<p>Change to:</p> <p>All inputs from the user interface are redirected to a protected interface that filters incoming commands, it only allows the commands to trigger the documented functions and discards all others.</p>	Agreed. See also response to NL-044.
DE-12		6.1.3.2.3		Te	The term secured is used in conjunction with "evidence of an intervention", which does not fit (secured -> preventing unauthorised access).	Split into two requirements and move the securing part to a different location (see our second comment to 6.1.3.2)	See solution proposed in response AU-17, which would appear simpler to implement than moving all parts of the clause to different locations.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
DE-13		6.1.3.2.3		Te	The last sentence is a requirement regarding indication of parameters, but not for evidence of intervention	Move to a different location.	Since other indication requirements are also distributed all over the document, we should either leave them where they are or move them all to one location. This should be briefly discussed with the entire PG. At the meeting, it was decided to propose this for a potential next revision. For documentation requirements, the collection into one clause will be implemented now.
NL-046	1	6.1.3.2.3		Info	If we accept the proposals for remote verification than this needs to be revised		Noted. A proposal for amendment of 6.1.3.2.3 is included in SG2 results.
NL-047	1	6.1.3.2.3		Te	Manipulation or accidental changes of parameters is considered a significant defect. Should we not reflect that here by requiring a checking facility? See also 6.1.4.1	Add after the first sentence: In case of a software implemented seal, a checking facility shall regularly check the integrity of the legally relevant parameters and in the case of an irregularity an appropriate reaction shall be required. See 6.1.4.1	Following the proposal in response to NL-005, we should add a note, instead: "Note: In case of a software implemented seal, see clause 6.1.4.1 regarding requirements on checking facilities and appropriate reactions."
NL-048	1	6.1.3.2.3	Note 1	Te	According to us parameters are either legally relevant and should therefore be secured and protected or they are not legally relevant and can be accessed and altered by an authorized person.  There are according to us no legal relevant parameters that shall not be protected.  Even in the case of a dynamic setting device as mentioned in R51, the facility is protected with an event logger.  We propose to replace this note with the content stated in clause 6.2.8.5.	Delete note 1 and 2 and replace this with the following note:  The relevant Recommendation may require the setting of certain device-specific parameters to be available to the user. In such a case, the measuring instrument shall be fitted with a facility to automatically and non-erasable record any adjustment of the device-specific parameter, e.g. an audit trail, see 6.2.8.5 and 6.1.3.2.5.	The given argument is sound. Nevertheless, the proposed change constitutes a requirement and should be treated as such. In addition, such a drastic change needs to be discussed with the entire PG. Proposal from the PG meeting: If that is so, the measuring instrument shall be fitted with a facility to automatically and non-erasable record any adjustment of the legally-relevant device-specific parameter, e.g. an audit trail, see 6.2.8.5 and 6.1.3.2.5.
NL-049	1	6.1.3.2.4		Te	We propose to change electronic to software	Change to:  Software protection means shall comprise appropriate sealing by mechanical, software and/or cryptographic means, making an intervention impossible or evident.	Agreed.



Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-050	1	6.1.3.2.4	Note 2	Te	We propose to move this note 2 to 6.1.3.2.1 because this clause is about the means of software protection and clause 6.1.3.2.1 deals with what should be protected.	Move Note 2 to 6.1.3.2.1	Agreed. This appears to have been overlooked, when 6.1.3.2.1 was rephrased during the previous revision.
NL-051	1	6.1.3.2.4	Example 1	Te	Change electronic to software	Change to:  1) (I) Software sealing	Agreed.
AU-25		6.1.3.2.5		Ed	The reference to traced updates should be to clause 6.2.8.4.8.	Change reference to clause 6.2.8.4.8.	Agreed. 6.2.8.4.8 would indeed be the correct reference.
FR-04		6.1.3.2.5		te	<b>Audit trail</b>  In case of legally relevant parameter change identification of user having modified should be contained in audit trail.	<ul style="list-style-type: none"> <li><i>in the case of a parameter change:</i></li> </ul> Add the sentence: If a login is required, the identification of user having modified the parameter.	<p>If a user is allowed to change parameters, what additional information would the user ID provide? Nevertheless, this new requirement should be discussed within the PG.</p> <p>The following rephrased proposal from the PG meeting will be implemented: “If applicable the source of the modification shall be recorded in the audit trail.”</p> <p>This could also solve the issue of changes done to an ML algorithm by an internal learning facility. We should also check if the time/date of the change is logged.</p>
NL-052	1	6.1.3.2.5	Paragraph 1	Te	An event counter should also be part of the legally relevant software, so we propose to add this here.	Change to:  6.1.3.2.5 Audit trails and event counters are part of the legally relevant software and shall be secured and protected as such, making an intervention evident. It shall not be possible to delete or change the data in the event counter or audit trails and it shall not be possible to exchange the audit trails or the value of the event counter when the software is updated.	Agreed. Mentioning evidence of an intervention here, however, would be an unnecessary repetition of 6.1.3.2.1 and should be omitted. Suggestion to rephrase to “Audit trails... secured and protected as such. It shall not be possible to...”
NL-053	1	6.1.3.2.5		Te	Deletion of the audit trail is considered a significant defect. Should we not reflect that here by requiring a checking facility?	Add: A checking facility shall regularly check the presence and integrity of the audit trail and event counter, and in case the audit trail or event counter is not present or in the case of an irregularity an appropriate reaction shall be required. See 6.1.4.1	Since it is up to the relevant Recommendation to require checking facilities, we should not restrict possible implementations unnecessarily here.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-054	1	6.1.3.2.5	Last paragraph	Te	The event counter should be included here as well.  We have not included it here yet but if the proposal for remote verification has been accepted, we need to modify this clause accordingly.	Change to:  The audit trail and value of the event counter shall be displayed or printed on command. The certificate shall describe how the audit trail or the value of the event counter may be displayed or printed.	Agreed.
US-04	1	6.1.3.2.5		ed	Audit trails that do not secure legally relevant aspects do not need to be part of the legally relevant software	“Audit trails <b>that secure legally relevant aspects</b> are part of the legally relevant software and shall be secured and protected as such. ...”	According to V1, 6.05, audit trails only address legally relevant aspects. Other recording measures would need to be addressed by a different term.
AU-26		6.1.4.1	Para 2	Ed	Common language used with reference to significant faults and checking facilities is that they “act upon” the significant fault – rather than “react”. Suggest this language is retained in the discussion of significant defects.	Reword as follows: “If software is involved in the detection of significant defects, an appropriate <b>action</b> shall be required.”	“Action” would likely confuse the reader if it is not mentioned in the context “acted upon”, since “action” usually refers to an activity by the user. Suggestion to rephrase to: “If software is involved in the detection of significant defects, it shall appropriately act upon any detected defect.”
AU-27		6.1.4.1	Para 3	Ed	Common language used with reference to significant faults and checking facilities is that they “act upon” the significant fault – rather than “react”. Suggest this language is retained in the discussion of significant defects.	Reword as follows: “The documentation to be submitted for type evaluation shall contain a list of the significant defects that will be detected by the software and the expected <b>action</b> ...”	See response to AU-26. Suggestion to rephrase to: “The documentation to be submitted for type evaluation shall contain a list of the significant defects that will be detected by the software and how it will act upon these defects.”
NL-055	1	6.1.4.1	First paragraph	Te	Add a statement that the PGs also have to specify at what time or timeframe checks needs to be carried out.	Change to:  The relevant Recommendations may require functions for significant defects and specify at what time and or in which timeframe a check shall be carried out.	Agreed. Highlighting this obligation for other PGs here makes sense.
NL-056	1	6.1.4.1	Second paragraph	Ed	We propose to make some editorial changes	Change to:  If software is involved in the detection of significant faults an appropriate reaction shall be required. For example, the relevant Recommendation may prescribe that the instrument or component is deactivated or an alarm and or record in an error log is generated in case a significant defect is detected.	Since “significant defect” is more general than “significant fault”, we should keep that term. All other changes will be implemented.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AU-29		6.1.4.2		Ed	See AU comment regarding 6.1.4.1.	Reword as follows: “If software is involved in the detection of significant defects, an appropriate <b>action</b> shall be required.” ... “The documentation to be submitted for type evaluation shall contain a list of the significant defects that will be detected by the software and the expected <b>action</b> ...”	See response to AU-26. Suggestion to rephrase to: “If software is involved in the detection of significant defects, it shall appropriately act upon any detected defects.” ... “The documentation to be submitted for type evaluation shall contain a list of the significant defects that will be detected by the software and how it will act upon these defects.
DE-14		6.1.4.2	1 <sup>st</sup> paragraph	Te	The first paragraph is not a requirement.	Make the first paragraph a note, see also our comment to 6.1.5.	Agreed.
NL-057	1	6.1.4.2	Second paragraph	Ed	We propose to make some editorial changes	Change to:  If software is involved in durability protection, an appropriate reaction shall be required. For example, the relevant Recommendation may prescribe that the instrument or component is deactivated or an alarm and or record in an error log is generated in case durability is detected as being jeopardised.	Agreed. Suggestion to change to “...and/or record...”.
AU-28		6.1.5	Para 2	Ge	Depending on the application it may be possible (and even desirable) that the time stamp is read from a network, and not directly from the instrument, although the instrument may also source its time from the same network.	Possibly reword to allow for the alternative provision of the time stamp from an external network.	This change should be discussed with the entire PG. During the previous revision it was consensus that an internal clock must be used. At the PG meeting the following proposal was agreed upon: “Automatic setting of the time shall only be possible if legal time is used as a time base in an authenticated manner.”
DE-15		6.1.5	2 <sup>nd</sup> paragraph	Te	The requirement states that time stamps shall be read from the clock of the measuring instrument. But there is no requirement, that an instrument shall have a clock.	Proposal for the second paragraph: If time stamps are used, the instrument shall contain an internal clock which shall be used for the creation of the time stamp. 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 6.1.3.2.3).  Also transform all following paragraphs to notes, as they contain no requirements.	Regarding the remaining paragraphs, these will be turned into notes as suggested. The conditional clause may need to be rephrased.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
FR-05		6.1.5		te	<b>Time stamp</b>  Requirements on synchronization and traceability to UTC are needed to ensure appropriate level of confidence of time stamps given with networks or internal clock.	Add the sentence: Method of synchronization and traceability to UTC should be described	Currently, we do not require synchronization with UTC. However, we can add the following: "If an internal clock is synchronized with UTC, the method of synchronization and traceability to UTC shall be described"
DE-16		6.2		ed	Title of the clause should be changed to correct its grammatical structure.	Change to "Requirements for specific configurations"	Agreed.
AU-30		6.2.1	Para 1	Ed	The text says 'The requirements given in this clause are based on...'. It is assumed that 'this clause' refers to clause 6.2 – not 6.2.1.	Replace 'this clause' with 'clause 6.2'	Agreed. The clarification would help. The proposed change should be combined with the proposal from DE-05.
NL-058	1	6.2.2	Title	Ed	We propose to change the title to include components and modules	Change to:  Specification and separation of legally relevant components and modules and requirements for interfaces	Agreed.
NL-059	1	6.2.2		Te/Ed	The user interface is mentioned here as well but that is already covered under 6.1.3.2.2.  Apart from that we propose some editorial changes, change part into modules or components.  We also added devices, these are not under legal control (if they were, they would be components) but may nevertheless not influence the measuring instrument or component or module.	Change to:  This requirement applies if the measuring instrument or components has interfaces for communicating with other devices, components or with other software modules besides the legally relevant modules within a measuring instrument or component.  Note: With respect to the user interface, see 6.1.3.2.2  Legally relevant software modules or hardware components shall not be inadmissibly influenced by another device or by other modules or components of the measuring instrument.  Recommendations may specify the software, hardware and data or part of the software, hardware or data that are legally relevant.	Agreed. Since user interfaces are not mentioned in any of the subclauses of 6.2.2, we can omit them here.
AU-31		6.2.2.1.1	Note	Ed	Should examiner be more generally expressed as 'type evaluation authority' or 'relevant authority'?	Consider changing 'examiner' to 'type evaluation authority'.	Agreed.
AU-32		6.2.2.1.1	Example 1	Te	The electricity meter example may be an acceptable solution only where the meter has a local display. Without a local display it may not be acceptable.	Restrict the example to an electricity meter with a local display.	The existence of a local display will be mentioned in the revised example.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-060	1	6.2.2.1.1		Te	We would like to propose to add a note here that the requirements 6.2.2.1 and 6.2.2.2 are strongly related to each other.	Note: with respect to separation of software modules, see 6.2.2.2.	Since the note may help readers in navigating D31, it should be implemented.
AU-33		6.2.2.1.2	Example 1	Te	The use of the word ‘quantities’ in this example is confusing. The corresponding example in 6.2.2.1.1 refers to measurement result.	Replace ‘quantities’ with ‘measurement results’.	Although a measurement result does consist of a measured quantity value, the proposed modification will help align examples from 6.2.2.1.1 and 6.2.2.1.2.
NL-061	1	6.2.2.1.2		Te	We propose to add the requirements mentioned in clause 6.2.6.2 here as well.	Change to:  6.2.2.1.2 It shall not be possible to inadmissibly influence the legally relevant software, parameters or measurement data through the hardware interfaces, either by means of a protective interface or sealing access to the hardware interface or by disabling the hardware interface through the operating system, see 6.2.6.2.	Since repetition of requirements within a document should be avoided, we should insert the following rephrased version between sentences 1 and 2: “It shall not be possible to inadmissibly influence the legally relevant software, parameters or measurement data through these interfaces, see also 6.2.6.2.”
NL-062	1	6.2.2.1.2		Te/Ed	Regardless if a command comes from a legally relevant or non-legally relevant part, the LR SW, parameters and data shall not be inadmissibly influence.  We also propose some editorial changes.	Change to:  A software-controlled component shall communicate with other components or devices through a protective interface. It shall be demonstrated that the legally relevant software, parameters, and data of the legally relevant components cannot be inadmissibly influenced by commands received via the protective interface.	Agreed. This will be combined with the change resulting from NL-061.
NL-063	1	6.2.2.1.2	Note	Te/Ed	We propose to add an additional note and some editorial changes	Change to:  Note 1: If legally relevant components transmit measurement data to other legally relevant components, refer to 6.2.5  Note 2: If the legally relevant component is equipped with an operating system, refer to 6.2.2.2.2	Since “interaction” is more general than “transmission” (as it also covers data input), we should leave note 1 as it is. Since 6.2.2.2.2 addresses software separation rather than hardware separation (components) note 2 would probably confuse readers.
US-05	1	6.2.2.1.2		ed	This is only applicable to legally relevant components.	“A <b>legally relevant</b> software-controlled component shall communicate with other components or devices through a protective interface. ...”	Since other clauses in 6.2.2 also explicitly point out that something is legally relevant, we can do the same here.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
US-06	1	6.2.2.1.2	Example 1	ed	The term ‘measurement result’ is a common term and easily interpreted differently than the official definition. In order to have the reader become more used to the actual definition it wouldn’t hurt to repeat its meaning and leave the striked-out part.	Leave the striked-out part	Okay, if the explanation in brackets helps users of the document becoming used to the new terminology, we should leave it there.
AU-34		6.2.2.1.3		Ed	Express requirements using ‘shall’.	Replace ‘... these pairing parameters are legally relevant and should be protected...’, with ‘... these pairing parameters are legally relevant and shall be protected...’	This should already be solved by the suggested change from NL-064.
KR-04		6.2.2.1.3		Ge	Definition and scope of the paring parameters are not shown within D31.	Please define “pairing parameters” in terminology.	This should be solved by the new example introduced in response to JP-04.
NL-064	1	6.2.2.1.3		Te	We propose to add a requirement with respect to exchanging component to make is clear why we mention pairing.	Add a clause 6.2.2.1.3:  PGs may decide that legally relevant components shall be protected against exchange.  If software seals are used to prevent components from being exchanged and pairing parameters are part of the seal, than these pairing parameters are legally relevant and shall be secured and protected in such a way that evidence of an intervention is available, see 6.1.3.2.3  Note: Pairing parameters could also include network or internet (IP) address.	Agreed. This appears to be a valid expansion of the current clause 6.2.2.1.3. Suggestion to rephrase the note to “Pairing parameters may also...”
US-07	1	6.2.2.1.3		ed	What is meant with “pairing parameters”?	??	This should be solved by the new example introduced in response to JP-04.
JP-04		6.2.2.1.3 and Annex B	1 <sup>st</sup> sentence of 6.2.2.1.3	Te	The meaning of “pairing parameter” is unclear. Does it mean a pairing of Bluetooth or a pair of parameters in cryptography? This term is also used in the row of “6.2.2.1 Separation of components” in the table of Annex B.	Please explain this term practically in 6.2.2.1.3.	An example for pairing parameters using authentication based on secret keys will be added to the clause.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-065	1	6.2.2.1.4		Te	We propose to add a requirement with respect to a checking facility that checks the authenticity, integrity and availability of another software-controlled component.	<p>Add a clause 6.2.2.1.4</p> <p>PG may decide that legally relevant components shall check the authenticity, integrity and/or availability of another software-controlled component.</p> <p>In case the authenticity and/or integrity process fails, or the component is not available an appropriate reaction shall be required. See 6.1.4.1.</p> <p>If automatic storage is required, no measurement shall be possible if the storage device is not available, see 6.2.4.4.4</p> <p>In the case of simple recipient printers it could be that only availability needs to be checked.</p>	<p>Agreed. However, we should use “integrity check” rather than “integrity process”.</p> <p>The new component requirement on storage devices should be moved to 6.2.4.4.1.</p>
NL-066	1	6.2.2.1.5		Te	We propose to add a requirement that if a component is shared by multiple other components than these multiple other components shall be unambiguously identified.	<p>Add a clause 6.2.2.1.5</p> <p>If a component is shared by multiple components, e.g. one display for multiple sensors, then all the components that share another component shall be unambiguously identified.</p>	The only plausible use case for the proposed requirement would be inspection of an instrument and its parts. During the PG meeting it was agreed that the requirement is acceptable as long as the manner of identification is flexible.
NL-067	1	6.2.2.1.6		Te	In some cases, it might be necessary to ensure that only the appropriate component has access to another component, certainly in the case where components are placed in the cloud. We therefore propose to add a requirement that access to components shall be validated.	<p>Add a clause 6.2.2.1.6</p> <p>PG may decide that access to legally relevant components shall be validated to ensure the authenticity of the requesting component and to validate that this component has access rights. In case of increased security, two-stage authentication is required.</p> <p>Access right can have the form of only reading rights or read/write rights.</p> <p>For example, it might be necessary to secure access to the cloud storage device by a specific component in such a way that only that component can read the data from the cloud storage device but can not write to the cloud storage device.</p>	If all components have proper interface protection (see 6.2.2.1.2), this requirement would appear obsolete. Furthermore, access restrictions are normally not part of legal metrology and we should refrain from instantiating them here. This might be solved by the response to NL-068.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-068	1	6.2.2.1.7		Te	<p>In those cases where measurement data is transmitted between components it might be necessary to ensure that only legally relevant software can use the measurement data. We therefore propose to add a requirement for that.</p>	<p>Add a clause 6.2.2.1.7</p> <p>PG may decide that measurement data shall be protected and secured in such a way that only legally relevant software can process the measurement data.</p> <p>Examples: (I)(II) A measuring instrument consists of two components, one containing the main metrological functions incorporated in a housing that is sealed. The other component is a universal device with an operating system. Some functions such as the indication are located in the software of this device. To ensure that only the legally relevant software on the universal device can further process the measurement data the measurement data is encrypted. The key for decryption is hidden in a program that is part of the legally relevant software of the universal device. Only this program knows the key and is able to read, decrypt and use the measurement data. Other programs cannot be used for this purpose as they cannot decrypt the measurement data (see also example in 6.2.2.2.4).</p>	<p>Data privacy has never yet been an issue in D31 and in legal metrology in general. Therefore, we should refrain from introducing the concept here. The change could be seen as prohibiting legally non-relevant software from processing measurement data, which would also be in conflict with this document. However, to ensure trust in measurement results indicated on a device, we could include a generalized version of the proposed requirement.</p> <p>During the PG meeting it was agreed to rephrase the proposal as follows: “In case the completeness of the measuring instrument cannot be visually checked (e.g. wireless or network-connected components), non-legally relevant software modules shall be prevented from calculation/presenting/spoofing the measurement result.” It was also agreed to provide additional examples as well as an explanation of the underlying problem.</p> <p>Keeping measurement data private by means of an encrypted connection between sensor and display could then be included as an example.</p>



Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-069	1	6.2.2.1.8		Te	<p>It might be necessary to restrict the functionality of certain components or modules, i.e with respect to cloud storage no further processing of the measurement data is allowed because functionality and required securing or protection measures are strongly related.</p> <p>If only limited securing and/or protection can be achieved than the functionality shall be limited accordingly.</p>	<p>Add a clause 6.2.2.1.8</p> <p>PG may decide that functionalities in certain components shall be restricted, for example the functionality of apps on smartphones or when cloud storage devices are used.</p> <p>In case components with limited functionality and securing/protection are applied, they shall have limited access to the measurement data, i.e. they shall use the measurement data without modification or further processing.</p> <ul style="list-style-type: none"> <li>• The measurement data shall be prepared for transmission or storage for further processing by a component that can be fully secured and protected, that component ensure that the data is complete and protected.</li> <li>• The measurement data shall be received or retrieved for further processing by a component that can be fully secured and protected, that component ensure that the data is complete and shall check its integrity. That component also ensure that the measurement result is printed or indicated in case of a dispute.</li> </ul>	<p>During the PG meeting, it was agreed to accept the first proposed bullet point as long as it only applies to components that cannot be fully protected and secured. The second proposed bullet point was also accepted after highlighting that it only refers to legally relevant components.</p>
NL-070	1	6.2.2.1.9		Te	<p>A smartphone or tablet is a mobile device which will not always be on side. This possess problems because for some instruments you need a display to verify the measuring instrument, in certain recommendation a display is even mandatory. For others the printer can be used, for example in the case of a weight price labeller or automatic gravimetric filling machines.</p> <p>We therefore propose to add a clause to address this problem.</p>	<p>Add a clause 6.2.2.1.9</p> <p>PG may decide that certain components shall be connected and available on site, for example a display or a printer.</p> <p>Example: In the case an indication of a result is mandatory, a display shall be connected and available with the measuring instrument.</p>	<p>Agreed. If a PG does see the need for certain components to be physically available (e.g. for the purpose of verification), we should give them that possibility.</p>
DE-17		6.2.2.2		Ed	<p>Harmonise title with 6.2.2.1</p>	<p>Change to: Separation of software parts</p>	<p>Agreed. However, “parts” will likely be replaced by the term “modules”, see SG3 results and response to NL-071.</p>

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-072	1	6.2.2.2		Te	<p>As we understand clause 6.2.2.2 it is about software modules within either a complete instrument or within a component.</p> <p>Even in the case of cloud computing, we consider this as a separate component with a specific function that has one or more software modules.</p> <p>This is not about software modules communicating with each other in different components, so clause 6.2.5 does not apply here.</p> <p>Also, a software module in one component processing the measurement data, transmitting that data to a software module in another component for price calculation, is covered by 6.2.2.1 separation of components and not by this clause.</p> <p>We propose to make that clear here.</p>	<p>Add:</p> <p>Software separation takes either place in the complete measuring instrument or in a specified component.</p> <ul style="list-style-type: none"> <li>• For separation of components, see 6.2.2.1</li> <li>• For communication between components, see 6.2.5</li> </ul>	<p>Agreed, the proposed clarification might make differentiation between 6.2.2.1 and 6.2.2.2 easier for new users of the guide.</p>
NL-073	1	6.2.2.2		Te	<p>We propose above for components requirements regarding pairing, availability, authenticity, integrity, unique identification, access rights, protection of data and restrict functionality, which might also be necessary to require for software modules.</p> <p>We would like to discuss this. See also the remark above about software separation.</p>	<p>Depending on the acceptance of the proposal above, we need to formulate requirements concerning pairing, availability, authenticity, integrity, and so.</p>	<p>Noted. Since trust in paired software modules without hardware protection is a difficult subject, it should definitely be discussed with the entire PG.</p> <p>The comment was withdrawn by the proponent in the PG meeting.</p>
NL-071	1	6.2.2.2.	Title	Ed	<p>We propose to change part to module</p>	<p>Change to:</p> <p>Specification and separation of software modules</p>	<p>This is already included in SG3 results and will be implemented. The title will be reduced to “separation of software modules” in response to DE-17.</p>

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-074	1	6.2.2.2.2		Te/Ed	<p>We propose to make this more explicable, in line with 6.2.2.1.2.</p> <p>We also propose to change software parts to software modules and make reference to the appropriate clauses.</p> <p>We wonder if the last paragraph should not be included in the definition of protected interface through a note because this seems to explain what is expected of the protected interface and what is part of the protective interface.</p>	<p>Change to:</p> <p>A software-controlled module shall communicate with other modules through a protective interface.</p> <p>It shall be demonstrated that the functions and data of modules that are legally relevant cannot be inadmissibly influenced by commands received via the protective interface.</p> <p>The legally relevant software module and the protective interface shall be clearly documented, see 6.2.2.2.3 and 7.1. All legally relevant functions and data domains of the software shall be described to enable a type evaluation authority to decide on correct software separation.</p> <p>The protective interface consists of program code and dedicated data domains. Defined coded commands or data are exchanged between the software modules by storing to the dedicated data domain by one part of the protective interface and reading from it by another part of the protective interface. The writing and reading code is part of the protective interface.</p>	<p>Agreed. Harmonization of 6.2.2.2.2 and 6.2.2.1.2 makes sense as we will now have identical requirements for two almost identical scenarios. Moreover, the provided interpretation appears to be line with the current intention of clause 6.2.2.2.2.</p> <p>However, we should not add the last paragraph as a note to clause 3.1.43 since the paragraph details requirements which should remain in requirement clauses. In addition, we should use “software module” instead of “software-controlled module” to comply with terminology.</p>
NL-075	1	6.2.2.2.2		Te	We would like to propose to add a note here that the requirements 6.2.2.1 and 6.2.2.2.2 are strongly related to each other.	<p>Add:</p> <p>Note: Software modules can be installed in a measuring instrument or in a component. With respect to separation of components, see 6.2.2.1.</p>	Agreed. See also responses to NL-060 and NL-072.
NL-076	1	6.2.2.2.2		Te	<p>The example: The digital sensors send the measurement data in encrypted form. The key for decryption is hidden in the library. Only the procedures in the library know the key and are able to read, decrypt measurement data, and display measurement results.</p> <p>Seems to be a requirement to protect the measurement data in the case of software separation. We propose to add this as a requirement in the clause.</p>	<p>Add</p> <p>Measurement data received shall be protected in such a way that only legally relevant software can process the data, see also 6.1.3.2.</p>	<p>As in the case of separate hardware components obtaining access to measurement data, data privacy should not be introduced here as a new concept in legal metrology. During the PG meeting the following rephrased proposal was agreed upon:</p> <p>“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.”.</p>
AU-35		6.2.2.2.3	Example 2	Te	With reference to the last sentence, it is not clear how an operating system could ensure that the configuration cannot be modified without breaking a seal.	Clarify how this could be achieved to assist in the use of the example.	Okay, an explanation to that effect (mentioning a sealed administrator password) will be added.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-077	1	6.2.2.2.3		Ed	Change part to module in the first sentence.	Change to:  There shall be an unambiguous assignment of each command to all initiated functions or data changes in the legally relevant software module	This is already included in SG3 results and will be implemented.
NL-078	1	6.2.2.2.4		Ed	Change part to module	Change to:  Where the legally relevant software module has been separated from the non-relevant software module, the legally relevant software module shall have priority using the resources over non-relevant software module.	This is already included in SG3 results and will be implemented. However, we should allow for the possibility of having more than one legally relevant software module.
AU-36		6.2.3	Example 1	Ge	With reference to the first two sentences. There are multiple examples and instruments in the previous clauses. Further, 6.2.2.2.4 does not appear to guarantee that only the legally relevant software part can read and display the measurement results. 6.2.2.2.4 only relates to priority for legally-relevant software (where there is separation).	Clarify the first sentence. Delete the second sentence.	The first sentence will be amended to directly refer to the appropriate examples. Regarding the second sentence, it will be rephrased to “The means described in 6.2.2.2.4 guarantee that the legally relevant software part can read and display measurement results before such data are made available to other legally non-relevant software.”
AU-37		6.2.3	Example 3	Ge	Example 3 talks about a smartphone and an LED on the phones (should be phone’s) housing. Is this a realistic example? Would the legally relevant app have the ability to override the operations of all other apps such that the LED is activities during their use?	Clarify or amend the example to provide a more realistic notification of the distinction between the operation and display of legally relevant and non-legally relevant applications. It is more likely that the legally relevant application should directly notify the user of its legal relevance, rather than activating the LED (or any other signal/alarm) while any other app is in use.	The example will be revised, see responses to FR-06 and KR-05.
FR-06		6.2.3		te	<b>Smartphones</b>  The example mentions a LED as an example for smartphones use in “shared indications” paragraph. LED are no more present on smartphones.	The example should be more up to date.	During the PG meeting it was agreed that the legally relevant application shall indicate operation of legally relevant software. Additional restrictions e.g. on the accessibility of legally relevant measurement data can be imposed to prevent spoofing of the indication.
KR-05		6.2.3		Ge	The context "Whenever legally non-relevant apps are used, the smartphone’s operating system activates an LED on the phones housing" is considered undesirable as an example.		From the majority of comments on smartphones, it is clear that “bring-your-own-device” scenarios are probably not suitable for legal metrology at the moment. During the meeting, it was agreed that the legally relevant application itself shall indicate the operation of legally relevant software, see response to FR-06.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-079	1	6.2.3	Example 3	Te	<p>We would like to discuss the use of a smart phone first.</p> <p>The reference to 6.2.6 we understand but in clause 6.1.3.2.1 it is stated that a smart phone cannot be secured or protected. We find that confusing.</p> <p>We don't understand the meaning and function of the LED on the smart phone housing.</p>	To be discussed.	6.1.3.2.1 only states that software protection may not be achievable in case of a consumer device. We should clarify this in all examples that do not use consumer devices. In the mentioned example 3, the LED would indicate the use of the display by legally non-relevant software. During the PG meeting, an alternative means for indicating the operation of legally relevant software was agreed upon, see response to FR-06.
NL-080	1	6.2.3	Last sentence	Ed	We propose to change should to shall	In that case a component shall exist with increased securing means that is able to display the measurement results.	Agreed. Since this sentence has been in D31 for some time, however, we should discuss it with the entire PG. Rephrased proposal from the PG meeting: "If so, a component shall exist with..."
US-08	1	6.2.3	Example 3	te	<p>Smartphones don't have LED's. They just have a graphic display.</p> <p>The main use of a smartphone is for non-legally relevant activities and has constantly varying software/apps. The requirement should focus on the status of the legally relevant app and not on the status of non-legally relevant apps.</p>	"A smartphone app is used to indicate measurement results calculated on a separate component. Since the smartphone is also used for other legally non-relevant purposes, the operating system of the smartphone is configured according to clause 6.2.6. Whenever <b>the legally relevant app is hidden or deactivated, further processing of legal transactions (e.g. printing the receipt) are inhibited.</b> "	Agreed. The example will be revised once the PG has reached consensus on the use of smartphones and similar technologies like tablets etc. During the PG meeting, an alternative means for indicating the operation of legally relevant software was agreed upon, see response to FR-06.
SI-2		6.2.3	Note	te	We believe that operating system of the smartphone cannot fulfil all of the 6.2.6 requirements, especially if we talk about the BYOD concept.	As already indicated should be discussed under D1 if smartphones and other consumer devices (BYOD) are acceptable for current requirements on the LR SW.	During the PG meeting, it was agreed to focus on "dedicated devices" for the time being. It was also agreed that for certain components, requirements on the operating system shall be fulfilled but depending on the role of the component, there might be exceptions.
JP-05		6.2.3 Shared indications	Example 3)	Te/ed	Activation of an LED may be effective if the smartphone is mostly used for legal purposes. In reality, however, the smartphone is likely to be used mostly for non-legal purposes, and the LED will be lighted frequently. Therefore, this requirement may not be realistic.	We propose removing this requirement to LED.	Agreed. See response to FR-06.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-081	1	6.2.4.1		Te	<p>This is still open to interpretation. Under the current definition is stated under measurement data:</p> <p><i>data used during the measurement process</i></p> <p><i>Note: Measurement data includes measurement result relevant data and measurement process data.</i></p> <p>This excludes “The measured quantity value” which should be included.</p> <p>Under the proposal for revision of the Terminology we have covered this but under the old terminology not. I have assumed that the new terminology will be accepted so I have mentioned this problem only here.</p> <p>Stored for legal purposes sounds vague to me. I would suggest:</p> <p>If measurement data is stored for later use to construct the measurement result, the requirements of 6.2.4.2 to 6.2.4.4 apply.</p>	<p>Change to:</p> <p>If measurement data is stored for later use to construct the measurement result, the requirements of 6.2.4.2 to 6.2.4.4 apply.</p>	<p>Concerning the ambiguity of the term “measurement data”, this should be solved by SG3 results.</p> <p>During the previous revision, it was decided to make this clause also applicable to scenarios where other measurement data (apart from those needed to construct the measurement result) are stored. We should keep it that way, unless we want to repeat the discussion from the previous revision. Moreover, narrowing 6.2.4 down to the measurement result would directly contradict storage requirements for remote verification purposes (see SG2 results).</p>
NL-082	1	6.2.4.2		Te	<p>We propose to clarify what is meant by future use and add a note with reference to Annex C</p>	<p>Change to:</p> <p>The stored measurement data shall include the measurement result relevant data necessary to construct the measurement result.</p> <p>Note: The PGs defines what should be included in the measurement result relevant data, see 3.1.18 and Annex C.</p>	<p>During the previous revision, the clause was intentionally kept generic to also account for other possible storage scenarios apart from the measurement result. Suggestion to include reconstruction of the result as an example in the sentence and to rephrase the proposed note to a requirement: “PGs shall decide which measurement data (e.g. measurement result relevant data necessary to construct the measurement result) shall be stored.” Otherwise we would also explicitly exclude storage of data for the purpose of remote verification (see SG2 results). This was probably not the intention of the comment.</p>

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AU-38		6.2.4.3	Para 1	Ge	In the last sentence of paragraph 1, the software should never (automatically) discard data if an irregularity is detected.	Remove discarded as an option. Also relevant to example 1 which discards data sets assumed to be falsified.	Depending on the damage done to a stored dataset, discarding might be the only option, especially if the dataset is illegible otherwise. Therefore, the option should remain in place. We could, however, add a note, that PGs may define the appropriate reaction.
AU-39		6.2.4.3	Para 1	Ge	It is unclear why the first sentence specifically mentions 'if necessary correctness of the information concerning the time of measurement.' If the time of measurement is needed, it is captured by 'stored measurement data' and the statements of authenticity and integrity. Also, in sentence 2, what does it mean to 'check the time of measurement'? Similar sentences appear in other clause such as 6.2.5.3.	Suggest to replace sentence 1 with: 'The stored measurement data shall be protected by software means to guarantee authenticity and integrity' Suggest to replace sentence 2 with: 'The software that displays or further processes the measurement data shall check the authenticity and integrity of the data after having read them from the storage.' Suggest to make similar changes to other clauses including 6.2.5.3	Agreed. In light of the revised D31 terminology, the time of measurement will (depending on the application) be part of the measurement data, anyway.
AU-40		6.2.4.3	Example 1	Ge	Terms and abbreviations like 'CRC32' should be defined. The second sentence then talks about using a secret initial value...instead of the value given in the standard. What standard?	Define 'CRC32' and clarify 'the standard'.	Okay. "CRC32" will be added as an abbreviation in clause 3.2 with reference to IEEE 802.3 Cyclic Redundancy Check.
AU-41		6.2.4.3		Ge	Is it always necessary/appropriate for software to actively protect/check stored data? With a normal risk level, should D 31 provide for other possibilities? For example, could it be sufficient for a measuring instrument (such as an electricity meter) to be sealed and to check that software does not allow for data to be modified without breaking a seal.	Provide for protection of stored data through sealing and assessment of software, rather than through active protection methods that 'check' authenticity and integrity.	On modern storage systems, integrity protection will already be provided by components like a storage controller. At the PG meeting it was agreed to change "protected by software means" to "protected by appropriate means".
FR-07		6.2.4.3		ge	<b>Cloud</b>  <i>Example 3)</i> The cryptographic signature could be more detailed.	<ul style="list-style-type: none"> <li>A definition of cloud should be given in the Document D31</li> <li>A minimum level of requirements concerning the cryptographic signature could be given in the example.</li> </ul>	We could use something like the following as a definition: "servers that are accessed over the Internet, and the software and databases that run on those servers" Regarding the example, we cannot impose requirements there, but we could make the example more specific by providing additional detail on the signature.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-083	1	6.2.4.3		Te	The requirement that a storage device shall have sufficient permanency to ensure that the stored measurement data are not corrupted under normal storage conditions is now mentioned under 6.2.4.4.1 but that covers automatic storing. We propose to move it from there and include it here, since this is about protection of stored data. We also propose to use storage component instead of storage device to make it clear that the storage facility is part of the instrument.	Move the second paragraph of 6.2.4.4.1 to here:  The storage component shall have sufficient permanency to ensure that the stored measurement data are not corrupted under normal storage conditions.	Agreed. 6.2.4.4.1 should be moved to the more general clause on storage protection 6.2.4.3.
NL-084	1	6.2.4.3		Te	We propose to make a reference to clause 6.1.4.1 and reword the sentence a little bit.  We also propose to leave it up to the PGs to define an appropriate response, could be that measurement results are to be stored in a separate register.	Change to:  If an irregularity is detected an appropriate response shall be required, see 6.1.4.1, for example the measurement data shall be discarded or marked unusable.	Since 6.1.4.1 only addresses support of hardware features, adding the reference could be misleading. Nevertheless, the modified wording appears to be in line with the intention of 1WD.
NL-085	1	6.2.4.3	Example 3	Te	We would like to discuss use cases for cloud storage first.  We don't understand why a reverification is needed after a dataset is lost. If a dataset is lost, the measurement result cannot be constructed, and no transaction can be made. That is a problem for the user, but I doubt if that is a problem for the consumer.  A dataset on a hard disk can also get corrupted but that is not a reason for reverification, see 6.2.4.4.1	To be discussed	The topic will be discussed at the PG meeting in May. During the PG meeting it was decided that reverification in case of a data loss is not necessary. Instead, user and customer shall be informed that data are lost. This is already covered by existing storage requirements. The example will be amended accordingly.
US-09	1	6.2.4.3	Example 3	te	Missing data might be unwanted but it does not lead to any incorrect transactions. The focus should be on data corruption instead of missing data. If missing data is regarded as a non-compliance then external storage on a removable storage device (e.g. USB stick) is no longer possible.  Furthermore, it goes too far to require a reverification after detection of corrupted or missing data. Preventing of further legally relevant processing is sufficient.	Rewrite example 3	Comment NL-085 also suggests that missing data would not be a problem and no reverification should be required, see response to NL-085.
US-10	6	6.2.4.3	Third paragraph	Ed	The last sentence before the examples refers only to the first two of the examples and not the third (new one). A descriptive clause could be added to refer to the third example.	Example 3 deals with data stored on cloud systems.	Agreed. A descriptive sentence will be added.



Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-086	1	6.2.4.4.1	First sentence	Te	Data also needs to be stored to ensure that it not lost during transmission or until another component acknowledge that it has received the measurement data, see the example below. We propose to delete the last part of the sentence	Change to:  When, considering the application, data storage is required, measurement data shall be stored automatically	Agreed. The rephrased version appears to be more generally applicable and fits the rest of 6.2.4 better.
NL-088	1	6.2.4.4.1	Second sentence	Te	We propose to move this to 6.2.4.3 Protection of stored data	Move to 6.2.4.3 Protection of stored data	Agreed. The second sentence does appear to address protection of stored data rather than automatic storage.
NL-089	1	6.2.4.4.1	Third sentence	Te	We propose to add the requirement mentioned in the example that If the local buffer reaches its limit, further measurements shall be disabled.  And we propose to refer to 6.2.5.4 where the same applies.	Change to:  There shall be sufficient memory storage for the intended application. If the local buffer reaches its limit, further measurements shall be disabled, see 6.2.5.4.	We should probably leave that conclusion to PGs and rephrase the new clause to: "PGs shall decide which action needs to be taken if the memory limit is reached (e.g. disabling further measurements)."
NL-090	1	6.2.4.4.1	Note 3	Te	We propose to move Note 3 to 6.2.4.2 Completeness of stored data	Move note 3 to 6.2.4.2 Completeness of stored data	As 6.2.4.2 addresses completeness of datasets rather than availability, we should move the Note to the general clause 6.2.4.1.
NL-091	1	6.2.4.4.1	Example	Te	The last sentence is a requirement, so this should be included above, see our proposal under 6.2.4.4.1 third sentence.		Noted. Regardless of the changes relating to NL-089, the technical description provided by the sentence is clearly part of the example and should remain there.
NL-092	1	6.2.4.4.2		Te	We have two forms of measurement data: intermediate data and the measurement result.  Intermediate data can be deleted if the next module state a proper completion of expected actions engaged.  The measurement result can be deleted if <ul style="list-style-type: none"> <li>the transaction is settled, or</li> <li>these data are printed by a printing device subject to legal control.</li> </ul>	Change to:  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 measurement result can be deleted if <ul style="list-style-type: none"> <li>the transaction is settled, or</li> <li>the measurement result is printed by a printing device subject to legal control.</li> </ul> <p>Note: Other general national regulations (e.g. for tax purposes) may contain strict limitations for the deletion of stored measurement data or results. PGs may define alternative conditions for data deletion.</p>	The proposed change was amended by the proponent after the PG meeting, see insertions marked in red. The modified proposal appears to be in line with the intentions of the clause and opens up the possibility to delete measurement data that are no longer needed. The proposed change will be implemented.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-087	1	6.2.4.4.4	Addition	Te	If automatic storing is required than we propose to add a checking facility that checks the availability of the storage device. If the storage device is not available no measurement shall be performed.	Add after the first sentence:  a checking facility shall regularly check the availability of the storage and in the case the storage device is not available no measurement shall be possible. See 6.1.4.1	Here (assuming that 6.2.4.4.1 rather than 6.2.4.4.4 is meant), a checking facility does appear to be the only possible protection measure. Therefore, the proposed change will be implemented.
JP-06		6.2.5 Transmission via communication lines	Title	Te/ed	Although this clause is titled for wired transmission, these requirements may be applicable also to wireless communication. This clause should be retitled regardless transmission method.	We propose to change the clause title to “6.2.5 Data transmission”.	Agreed. Generalization of the clause title appears useful.
NL-093	1	6.2.5.1		Te	We propose to clarify the term used for legal purposes	Change to:  If measurement data are transmitted for later use to construct the measurement result, the requirements of 6.2.5.2 to 6.2.5.4 apply.	Depending on a PG’s decision (see response to NL-081) the measurement result might be included, but we should keep the wording as generic as possible to also account for other use cases, such as remote verification (see SG2 results).
NL-094	1	6.2.5.2		Te	We propose to clarify the term used for legal purposes, i.e. refer to measurement result relevant data.	Change to:  The transmitted measurement data shall include the measurement result relevant data.	This should be solved by the proposal in response to NL-081 which should be copied here to align clauses on transmission and storage.
AU-42		6.2.5.3	Para 4	Ge	The last sentence says ‘Means shall be provided whereby these keys can only be input or read if a seal is broken.’ What are ‘these keys’?	Clarify.	Agreed. The sentence will be changed to “Means shall be provided whereby cryptographic keys used by these methods can only be input...”.
AU-43		6.2.5.3	Example 1	Ge	Same comments as provided against clause 6.2.4.3.	Define ‘CRC32’ and clarify ‘the standard’.	Okay, see response to AU-40.
NL-095	1	6.2.5.3		Ed	We propose some editorial changes and to make a link to 6.1.4.1	Change to:  The transmitted measurement data shall be protected by software means to guarantee the authenticity, integrity and, if necessary, correctness of the information concerning the time of measurement. The software that displays or further processes the measurement data shall check the time of measurement, authenticity, and integrity of the measurement data received from a transmission channel. If an irregularity is detected an appropriate reaction shall be required, see 6.1.4.1, for example the measurement data shall be discarded or marked unusable.	The editorial changes are acceptable. Since 6.1.4.1 limits possible reactions to deactivating the instrument or producing an error log entry, we should refrain from including the reference here. The current phrasing, for instance, also allows data to be marked as unusable.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-096	1	6.2.5.4		Te	In clause 6.2.4.4.1 we specify that if the local buffer reaches its limit, further measurements shall be disabled. Should we not make a reference to that article here as well?	Add and change  The measurement shall not be inadmissibly influenced by a transmission delay or interruption. If network services become unavailable or very slow, no measurement data shall be lost. If the local buffer reaches its limit, further measurements shall be disabled, see 6.2.4.4.1.	Similar to the proposed response to NL-089, we should leave the actions to be taken to PGs and rephrase the existing clause to: “PGs <b>shall</b> decide upon appropriate requirements and mechanisms intended to preserve measurement data ( <b>e.g. disabling further measurements</b> ) where transmission interruptions are possible in the relevant application(s).”
AU-44		6.2.6.1		Ge	Are the requirements here applicable to operating systems associated with remote displays? In particular, the requirements here don’t seem to be able to be met through a universal device such as a mobile phone. Does/should D 31 provide solutions for the primary display this way, or does D 31 effectively disallow this?		At the PG meeting, it was decided to focus on dedicated devices for the time being. Since such devices are interpreted as components that cannot be fully secured and protected, not all operating system requirements would be applicable. This will be clarified in the revised clause 6.2.2.1. See also responses to NL-068 and NL-069.
AU-46		6.2.6.2	Examples	Ed	Both examples are numbered 1. Also the second example needs editing around ‘...is selected required...’	Number second example as 2, and clarify the wording/meaning.	Assuming the comment refers to clause 6.2.6.4, the requested editorial changes will be implemented.
NL-097	1	6.2.6.2		Te	We believe that the legally relevant software is equipped with a protective interface, not the hardware.  An example is not a requirement, so even if it is mentioned in a example, we need to specify the requirement.  We also believe that under 6.2.21.2 we required that components shall communicate with other components or devices through a protective interface, so this requirement should be added there as well. See our proposal above.  This comes back in 6.2.6.6, are they not the same requirements?	Change to: Interface  It shall not be possible to inadmissibly influence the legally relevant software, parameters or measurement data through the interfaces, either by means of a protective interface, or sealing access to the hardware interface or by disabling the hardware interface through the operating system, see 6.2.2.1.2 and 6.2.6.6.	There are some technologies (like direct memory access DMA) that avoid operating system and application layer altogether. For these, 6.2.6.2 needs to remain in place, despite its similarity to 6.2.6.6. The other assets mentioned in the proposed change (parameters and measurement data) will be included.
NL-098	1	6.2.6.2	Example 1	Te	We propose to reword the examples, see also 6.2.6.6	Change to:  Examples: 1) (I) A legally relevant software module interprets all commands reaching the legally relevant software part and discards the inadmissible ones. 2) (II) All open interfaces are physically protected or disabled by the operating system.	Rewording “legally relevant application” to “legally relevant software module” in example 1 is acceptable. As there can surely be different reactions of instruments to inadmissible input, we can include the proposed change as example no. 2. The current second example would then be no. 3.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AU-45		6.2.6.3.2 and 6.2.6.3.3		Ge	Should 'chain of trust' be considered as an acceptable technical solution, rather than the requirement?	Generalise the requirement to allow for potential alternative to 'chain of trust'.	Agreed. Suggestion to rephrase to "the boot process shall ensure integrity and authenticity of the legally relevant software part." Since 6.2.6.3.3 allows for exceptions from the chain of trust solution, we should keep it as an option if a chain of trust is implemented.
DE-18		6.2.6.3.5	1 <sup>st</sup> example	Te	The example mixes secured and protected Since the sentence only echoes the note of the definition of securing, its relevance is debatable.	Change to: The boot loader is secured with a secure password.	In response to NL-099, the example will be moved to 6.2.6.3.4, which should solve the issue.
NL-099	1	6.2.6.3.5	Examples	Te	We believe that the examples given here belongs to 6.2.6.3.4  The example only mentions a secure password but that is not protection, but we are not sure if the boot configuration can be protected in such a way that evidence of an intervention is available.	Move example to 6.2.6.3.4 The boot configuration shall be secured and protected  Discuss the term secure password.	Agreed, the example will be moved. The term "secure password" appears to be commonly used in IT security, but we can discuss possible minimum requirements in the PG meeting. After discussion at the PG meeting, it was decided to replace the example altogether.
AU-47		6.2.6.4		te	The availability of system resources is also relevant to overall system design.	Include an additional requirement that the design of the system shall provide appropriate resources for the operation of the legally relevant software part. Or is 6.2.6.8 sufficient in this regard?	6.2.6.8 already appears to address the proposed requirement.
US-11	6	6.2.6.4	Example box	Ed	In the example, there are two "(1)" listed prior to the indication (I) and (II). Please use only one form of indexing and be certain to index the second example correctly.		This will be corrected.
US-12	6	6.2.6.4	Example box; Example II	Ed	As written, the sentence is not clear. "The smallest number of operating system parts is <b>selected</b> <b>required</b> to ensure the measurement process can be executed." Selected or required?	"The minimum number of operating system parts is utilized to ensure the measurement process can be executed." Alternatively, "The smallest number of operating system parts are required to ensure the measurement process can be executed."	The first proposed sentence will be implemented in 1CD.
AU-48		6.2.6.5.3		Ge	The requirement is not clear. What is meant by access control, and what is meant by 'the intended use'?	Clarify this requirement.	"Access control" is a commonly used term for operating systems. We can try to clarify the clause by rephrasing it to: "The access control feature of the operating system shall be configured in such a way that the intended use of the measuring instrument cannot be inadmissibly influenced."
US-13	6	6.2.6.5.4	Note	Ed	May wish to put "administration task" in quotes in the Note. Otherwise, the sentence may be confusing.	The term "administration task" addresses all reconfigurations and updates of the operating system.	Agreed.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-100	1	6.2.6.6		Te	Have we not already covered this in 6.2.6.2?  In any way, we propose to add the requirement that is also mentioned in 6.2.2.2.2 and include a reference to 6.2.2.2.2	Add after the first sentence:  It shall be demonstrated that the legally relevant software, parameters, and data of components that are legally relevant cannot be inadmissibly influenced by commands received via the protective interface, see also clause 6.2.2.2.2	6.2.6.6 is broader in scope since it also explicitly addresses hardware and the operating system. The proposed addition will be included.
NL-101	1	6.2.6.6	Examples	Te	Example 2 only does not seem to be a good solution. We propose to reword this.	Change to:  2) (II) All open interfaces are physically protected or disabled by means of the operating system.	Agreed.
NL-102	1	6.2.6.7.1	Examples	Te	Please add access to interfaces to the relevant list	Add:  Access to interfaces	Agreed. This should already be covered by “user privileges” but mentioning the item specifically will not hurt.
FR-08		6.2.6.7.2		ge	<b>Operating system update</b>  An update of legally relevant operating system could lead to a dysfunctioning of the instrument.	Delete the word “generally” in Note 2 could give assurance of needed requirements “verified update” or “traced update” are applied of such operations.	Agreed, the word “generally” should be removed from the note, especially since it only addresses legally relevant operating system parts.
NL-103	1	6.2.6.7.2		Remark	The secretariat states that “protection” already implies evidence of an intervention. More important is the traceability of changes. But that is only the case if we accept the proposal for the new terminology.	No change, we assume that the new terminology will be accepted.	Noted. The secretariat assumes the same.
US-14	1	6.2.6.7.2		te	“Configuration settings of the operating system shall be protected”. This makes sense if it comes to security settings or adding/removing legally relevant components of the measuring system.  But updates of operating system program code should be kept out of the scope of legal control. It places an unnecessary burden on the manufacturer while the risk involved with non-verified updates of these software packages is extremely low (see the comment below).	Limit the protection of configuration settings of the OS only to the relevant configuration files and exclude the executable code.	The clause will be rewritten to “Legally relevant configuration settings of the operating system shall be protected, i.e. changes to the legally relevant configuration shall be traceable.” As executable code is not mentioned at all, there should be no need to mention it.
NL-104	1	6.2.6.9		Te	We propose to add a requirement concerning the build-for-purpose device	Add:  In the case of a built-for-purpose device the operating system cannot be accessed directly	Requirements need to contain normative language. The proposed change appears to be a description rather than a requirement. Since the statement is already included in definition 3.1.4, no change is needed.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AU-49		6.2.7		Ge	OIML D 34 (Conformity to type) uses the term ‘approved type’, rather than ‘certified type’.	Suggest to include a note to clarify the use of the terms ‘certified type’ and ‘approved type’ and their relationship with respect to the evaluation, certification and/or approval of legally relevant software modules.	Agreed, such a note will be included here to bridge the terminology gap to D34.
NL-105	1	6.2.7		Te	Add components to the requirements and replace devices with measuring instruments.	Change to:  The manufacturer shall produce measuring instruments, components and legally relevant software that conform to the certified type and the documentation submitted	Agreed. This is also in line with proposal NL-059.
NL-106	1	6.2.8.2	First paragraph	Ed	We propose some editorial changes to the last sentence of the first paragraph.  Not only the device specific parameters shall be unchanged by the update but also the type-specific parameters.  Of course, we could refer to the legally relevant parameters, but we believe this is clearer.	In the case that type- or device specific parameters are modified by the update, only a verified update is possible.	An update will almost certainly modify type-specific parameters such as the software version number or a reference value for a hash. Therefore, the current wording should remain. Otherwise a traced update would be impossible.
AU-50		6.2.8.3		Ge	The text requires a person to be on the installation site of the measuring instrument to check that the updated software has been installed correctly. Firstly, this implies there is an installation site, which may not be applicable for all instruments (such as hand-held). Further, there may be other technical solutions than having a person on site.	Suggest D 31 sets the requirement for checking for successful update. One technical solution could be to have a person at the installation site. Others include remote verification processes.	Agreed. This clause will be updated according to SG2 results.
AU-51		6.2.8.4.1		Te	Include additional sentence at the end of the paragraph regarding the means of demonstrating the efficacy and validity of a traced update.	Suggest to include the following sentence at the end of the clause: “PGs may specify procedures to test and evaluate traced updates to provide evidence that they do not affect the legally relevant parameters of the measuring instrument, and otherwise comply with all relevant requirements for traced updates.”	Since PGs are free to specify additional test procedures, the suggested change should be in line with the current intention of D31. These procedures, however, would not count as software requirements. Therefore, we should likely make this a note.
AU-52		6.2.8.4.2		Ge	Content may not be required. As such the second sentence should be amended to reflect this.	Amend second sentence as follows: “In this case, the measuring instrument...”	Agreed. The implication from the first sentence appears obvious.
NL-107	1	6.2.8.4.2	First sentence	Remark	The secretariat states that “protection” already implies evidence of an intervention. More important is the traceability of changes. But that is only the case if we accept the proposal for the new terminology.	No change, we assume that the new terminology will be accepted.	Noted. The secretariat assumes the same.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-108	1	6.2.8.4.2	Last sentence	Te	We would like to reword this to make clear that if there is no consent, the update should not start.  With respect to owner denies consent in clause 6.2.8.4.9 we propose to move that requirement to this clause. 6.2.8.4.9 deals with the audit trail.	Change to:  If the feature is enabled, each traced update needs to be initiated by the user or owner.  If the user or owner denies consent, the update procedure should not start at all. If it is disabled, no activity by the user or owner is necessary to perform a traced update.	Agreed, moving that part of 6.2.8.4.9 here would improve readability of the clause.
US-15	6	6.2.8.4.2		Ed	Not clear what edited sentence should read. With cross-outs it looks like, “The measuring instrument shall have a feature for the user <del>or owner to express their consent, e.g. a push</del> button, before the update starts.”	The text reads correctly if the entire sentence is left out.	Since the requirement is still needed, we could rephrase the sentence to: “The measuring instrument shall have a feature for the user to express consent prior to an update.”
AU-53		6.2.8.4.3		Ge	Does a traced updated need to automatic? And what does automatic mean in this context? The Note suggests that they are not always.	Please clarify and/or provide the option of a traced update being deployed manually (whatever that means in this context).	Clarification will be provided stating that “After initiation of the update procedure, a traced update of software shall run automatically.”
JP-07		6.2.8.4.3	Note	Ge/ed	The contents of this note are similar to those mentioned in 6.2.8.4.2 above.	Delete this note if the contents are redundant.	The note is indeed redundant, but it should help understanding clause 6.2.8.4.3 which is the sole purpose of a note. To avoid confusion, a reference to the requirement in clause 6.2.8.4.2 will be added to the note.
NL-109	1	6.2.8.4.4		Te	There are more protections measures than audit trails or event counters, i.e. cryptographic means, hidden keys, private keys, etcetera.  We propose to make this more general.	During a Traced update, any existing protection measures shall be retained, for example audit trail information and event counters shall be retained.	Agreed. For better readability, we should rephrase this to “During a Traced update, any existing protection measures, e.g. audit trail information and event counter values, shall be retained.”
AU-54		6.2.8.4.8		Ge	What is meant by the fifth dot point ‘identification of the downloading party if available’? Is the ‘downloading party’ the user or owner that expressed their consent, or is it someone else associated with the manufacturer or responsible person providing the software update?	Clarify.	The bullet point probably addresses the source of the update (which would qualify as the “uploading party”). This will be clarified.
NL-110	1	6.2.8.4.8		Te	We would like to discuss the requirement that a seal has to be broken if the audit trail has reached his capacity, see our comment at 6.2.8.4.9	See our proposal at 6.2.8.4.9	Noted.

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
AU-55		6.2.8.4.9		Ge	If the audit trail has no more capacity – how is this resolved? Clause 6.2.8.6 requires that the audit trail should not be erased or overwritten, but clause 6.2.8.4.8 provides for limited capacity. Clause 6.2.8.4.8 suggests the need to break a seal, but it is unclear if this is only if there is no capacity for the last two verifications. Is it possible to overwrite old entries in the audit trail (older than the last two verifications) without breaking a seal?	Clarify.	This should be solved by the changes proposed in NL-112.
NL-111	1	6.2.8.4.9		Te	We propose to move the consent of the user or owner to 6.2.8.4.2, so that this clause only covers the audit trail	Move if the user or owner denies consent, the update procedure should shall not start at all to 6.2.8.4.2.	Agreed, moving that part of 6.2.8.4.9 to 6.2.8.4.2 would improve readability of the clause.
NL-112	1	6.2.8.4.9		Te	We propose to reword the requirement If the audit trail has no more capacity, the update procedure shall not start at all.	Change to:  The audit trail needs to have sufficient capacity (6.2.8.4.8) depending on the use of the instrument. If the audit trail has no more capacity, an appropriate response is required, i.e. either the latest entry may be deleted, or the update procedure shall not start at all.  Note: PGs need to define the sufficient capacity for the audit trail and need to define the appropriate reaction.	Agreed. Generalization of this clause appears appropriate. However, since the first proposed sentence is already included in the previous paragraph, we do not need to repeat it here. We should also replace "latest" with "oldest" to avoid repeated deletion of the most recent entry in the audit trail.
NL-113	1	7.1		Ge	We propose to go through the final document and list all the documentation requirements to check if everything is listed here.		Agreed, this would also be in line with comment DE-19 and NL-013.
DE-19		7.1.2		ed	Currently, many documentation requirements are spread throughout the document, while a few are also listed in clause 7.1.2.	Move all documentation requirements to 7.1.2 and replace current occurrences with references to that clause.	Agreed. Also related to NL-13, NL-113.
NL-114	1	7.3.1	Table 2	Te	Add under 6.2.6.9 that is should be checked that in the case of a built-for-purpose device the operating system cannot be accessed directly	Add in table 2 under 6.2.6.9:  Check that in the case of a built-for-purpose device the operating system cannot be accessed directly.	Since 6.2.6.9 was not modified, there is no need for the addition here, see response to NL-104.
AU-56		8.1	Para 1	Ge	What is meant by ‘the validity of the adjustment’? There is no mention of an adjustment.	Clarify	The sentence seems to address verification after parameter adjustment. It will be rephrased to: “...the validity of parameter adjustments and...”
AU-57		8.1	Dot point 3	Ge	What does this mean? What are unwanted side effects? This term is not defined or used anywhere else.	Clarify	Agreed. We should use the term “inadmissible influence” instead.



Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
NL-115	1	8.1		Te	We propose to add protection to the list	<p>The verification of the software shall include</p> <ul style="list-style-type: none"> <li>• an examination of the conformity of the software to verify that it is the certified version (e.g. check of the software identification, check of securing and protection means),</li> <li>• an examination of the configuration to verify that it is compatible with the declared minimal configuration, if given in the certificate,</li> <li>• an examination of the inputs/outputs of the measuring instrument to verify that they are free of unwanted side effects, and</li> <li>• an examination of the device-specific parameters (especially the adjustment parameters) to verify that they are correctly set and a check of the securing and protection means to check the integrity of the parameters.</li> </ul>	Agreed.
NL-116	1	Annex B		Remark	We propose to review Annex B if all the proposals have been implemented.		Annex B will, of course, be revised during preparation of 1CD.
NL-117	1	Annex C		Remark	We propose to review Annex C if all the proposals have been implemented.		Annex C will, of course, be revised during preparation of 1CD once SG3 results have been implemented.
NL-118	1	Annex D		Remark	The same as for Annex B and C.		Annex D will, of course, be revised during preparation of 1CD.
Annex A		Annex A			Update Annex A.	Update Annex A.	

Country Code <sup>1</sup>	Part	Clause/ Sub clause	Paragraph / Figure/ Table/	Type of comment <sup>2</sup>	COMMENTS	PROPOSED CHANGE	OBSERVATIONS OF THE CONVENER/PG on each comment submitted
US-01	1	New		te	<p>In general, general-purpose third-party software such as Windows, Linux, Google Chrome, Appel Safari etc. should be exempt from certification. Legal control over these software packages is not realistic and unnecessary for the following reasons:</p> <ul style="list-style-type: none"> <li>• These software packages are free of fraudulent aspects. The creators of these software packages (e.g. Microsoft, Apple) have no motive to commit or facilitate fraud with measuring instruments.</li> <li>• These packages are constantly updated for security threats and bugfixes. Therefore, security is optimal and chances of unintentional corruption are minimal.</li> <li>• Updates are beyond control of the manufacturer of the measuring instrument.</li> <li>• Legally relevant functions of these packages are limited only to low level tasks such as communication drivers, printing drivers and display drivers. Metrological functions are very specific and therefore always part of the high-level manufacturer's software package.</li> </ul> <p>If it is deemed that these kind of third party should be under legal control then it should be only for very high risk instruments where the instrument is operating standalone without a connection to the internet and updates are issued by the manufacturer only.</p>		Noted. It is precisely for this reason, that clause 6.2.6 currently limits itself to the “legally relevant configuration” of an operating system.