Comments of P/O members to Pre-draft Software Requirements (Version 0.11, 2004-10-20) 2005-11-09

*) e – editorial, t – technical, g – general

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
1		3.1.1	INMETRO, Brasilia	e	We understand that the presentation of all General terminology must indicate de reference document and the respective clause.	Electronic measuring instrument [D11 T.1]	OK, numbers changed (obviously the numbers in D11 changed; we took the latest ones; see 100 ff.)
2		3.1.2		e		Electronic device [D11 T.2]	OK
3		3.1.3		e		Electronic sub-assembly [D11 T.3]	OK
4		3.1.4		e		Electronic component [D 11 T.4]	OK
5		3.1.8		e		Initial intrinsec erro [D 11 T.7]	OK
6		3.1.9		e		Fault [D 11 T.8]	OK
7		3.1.10		e		Significant fault [D 11 T.9]	OK
8		3.1.11		e		Durability error [D 11 T.10]	OK
9		3.1.12		e		Significant durability error [D 11 T.11]	OK
10		3.1.14		e		Influence factor [D 11 T12.1]	OK
11		3.1.15		e		Disturbance [D 11 T.12.2]	OK
12		3.1.18		e		Performance [D 11 T.15]	OK
13		3.1.19		e		Durability [D 11 T.16]	OK
14		3.1.20		e		Checking facility [D 11 T.17]	OK
15		3.1.21		e		Automatic checking facility [D 11 T.17.1]	OK
16		3.1.22		e		Permanent automatic checking facility (type P) [D 11 T.17.1.1]	OK
17		3.1.23		e		Intermittent automatic checking facility (type I) [D 11 T.17.1.2]	OK
18		3.1.24		e		Non-automatic checking facility (type N) [D 11 T.17.2]	OK
19		3.1.26		e		Durability protection facility [D 11 T.18]	OK
20		Annex E		g	We understand that the results should be classified in three levels	More Important/ Important/ Less Important	You are right, however, the results of the questionnaire only served as an initial input. As the results were not very distinct, we decided to deal with all problems but the one

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
							with least interest. It is only intermediate information for the members, the table will not be taken into the CD.
21		5.2 (6.2?)	Central Office of Measures – GUM, Poland	g	The following wording is proposed:	Specifying and separating relevant parts and specifying interfaces of parts.	The proposed wording is equal to the ORIGINAL wording. Please check your point.
22		9		g	The definition of „software process“ is required and should be added to point 3.		Note added.
23		General	METAS, Switzerland	g	Switzerland / METAS extremely appreciate the work which has been done by TC5/SC2 because it gives the answers to a real need since a long time to have overall general requirements in this field, similar to those of document D11, which are already available now.		Thanks!
24		General		g	The presented document brings the awaited foundation for the next development step towards new technologies of measurement devices in the field of legal metrology, namely the application of computers and corresponding software in spread linked systems, without taking the risk of loosing control and security.		OK
25		General		g	New configuration opportunities are offered to the owners which allow them to employ devices at the same time for legal applications as well as for other purposes not submitted to legal control. Until now this was in most of the cases not possible.		OK
26		General		g	The authors try in a very skilful way to find a wording that does not influence or even restrain the further process of		OK

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					technological development in the future.		
27		General		g	The proposed methods, from the today's (theoretical) point of view, seem to be adequate, for the manufacturers and for the testers as well, to master the new technologies while meeting the legal requirements with a reasonable expense.		OK
28		General		g	With increasing practical experience, future minor adaptations of the now existing documents will never be impossible.		OK
29		General		g	There is an obvious trend of a displacement of a part of the responsibility towards the manufacturer, who will be obliged to go deeper into the matter and objectives of legal metrology than this was the case until now. He is expected increasingly to understand the requirements of legal metrology, to interpret them and to apply them correctly in his products, at least if he wants to profit of all the new possibilities. If not, there will always be the old, conventional approach.		OK
30		General		g	Finally we pronounce the hope, that the particular TCs will appreciate the proposed solutions of this document and implement them in their recommendations as completely as ever possible.		OK, thanks
31		3.1		e		3.1 General Terminology Many of the terms are never used later in this document. Should they really be mentioned here?	We will only keep those that are used in the text and in the terminology part itself.
32		4.2			4.2 Very good and important new approach		
33		5.1.3.1		t		5.1.3.1	Do you propose a change of

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
						Even if it leaves a certain amount of interpretation we support this wording (**minimal** unintentional accidental misuse). A hundred percent will never be possible and would be misleading.	the wording? We think it is already meant this way.
34		5.1.3.2			5.1.3.2 New methods/means are explicitly mentioned and what they have to fulfil (inadmissible intervention impossible or evident)		OK
35		5.2.1.2		e		5.2.1.2 First sentence: Add the word *software* to read *..form the legally relevant software part of..* Second Point: Replace *program code* by *defined (coded) commands* to read *The interface consists of defined (coded) commands and dedicated data domains*. For the note, we would prefer the following text: *The programmer is responsible for **respecting** these constraints. There are no technical means (like sealing) to prevent a programmer from circumventing or programming hidden commands. The programmer..*	OK Here the executable code (machine code) was meant. To require “coded” commands is too specific. We changed the wording and added an explanation. OK
36		5.2.2.		t		5.2.2. We suggest the following wording: *When a display, a printout **or other output devices** are used to present information from the legally relevant part of software and information from the not legally relevant part as well,*	We don’t know which other outputs you mean. We think that a display may be analogue with a needle, electro-mechanical, digital, a window on a monitor.

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
						then the following requirement applies: The distinction ..	
37		5.2.3		e		5.2.3 We think, it would be better not to use references to existing recommendations like R117 or R49 in the final version of this document, because it will stand hierarchically for itself and above them. (This remark is valid in general and especially in this section.) Additional explanations if needed might perhaps be given in a special appendix to this document.	OK, we will consider this. For the meantime during development the references seem valuable to us to make the members aware of already existing software requirements.
38		8		t	8 We strongly support this approach. Since a long time it has been a real need to introduce severity levels in that context. Different levels of risk of fraud might have different solutions. Or in other words: if the risk of fraud is low, then the countermeasures might be not very important or even not necessary	. The same fact has to be considered for the degree of conformity and reliability, and also the possibility if a measurement can be repeated or not must be taken into account in the future.	Do you propose a change of the wording?
39		5.2.4		e		5.2.4 If a universal computer**s** is ..	OK
40		6.3 (a)		e		6.3 (a) ..described in 6.4 shall..	OK
41		6.4.3.3		e		6.4.3.3 First dash: ..should be activate**d** and checked.	OK
42		5.1.1	NMIJ/AIST Japan	t	5.1.1 "Software Identification" The information on a descriptive plate may be simplified if the software ID is displayed on a screen at the boot sequence.		This was intended to be expressed by the text in 5.1.1. Do you want a change of the wording?
43		5.1.3		t	5.1.3 "Software Protection" and 6 "Type Approval" If software is stored in a masked ROM or stored in a device which is		Yes we agree as regards protection against fraud by manipulating program code or parameter settings. Mechani-

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					sealed mechanically, we think the requirements on software examination should be reduced drastically.		cal sealing is in many cases a simple, effective, and transparent method to protect software. On the other hand we think that the requirements don't need to be reduced if parts are sealed but by this technical solution of storing software the given requirements are fulfilled automatically. Furthermore, the examination intensity concerning other items like eg. conformity with the pattern or transmission via networks are not a matter of the memory technology. We think it is not wise to exclude examination steps beforehand without knowing the EUT. All validation procedures should be understood as recommendations that may be selected/reduced by TCs that implement them into Recommendations. An examiner should be equipped with a number of validation methods and he should have the freedom to decide in the particular case what the most effective examination steps are. Please propose a change of the wording if you are not content with this answer.
44		5.2.3		e	5.2.3 "Storage of data, transmission via communication systems" What is the precise definition of the		1) Wording changed. It has to be decided by the responsible TCs whether it is

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					"metrologically relevant data"? Do they mean the final values displayed or all information including transmitted intermediate data? In the latter case, it is impossible for the manufacturers to comply with all requirements in 5.2.3. Secondly, it seems impossible to ensure correctness of the time information accompanied with the measurement results because internal clocks used in measurement instruments generally are not so reliable.		necessary in a specific case to call intermediate data legally relevant or only take the final value. You did not explain why it is impossible to comply with the requirements – we suppose because of performance reasons. We would be interested in the reasons of your concern as we would like to adapt the recommendations accordingly. 2) Restriction added. Again it depends on the area of application whether a time-stamp of the measurement is necessary. The responsible TCs should decide.
45		5.2.3.1		e	5.2.3.1 “Storage of data, transmission via communication systems” What is meant precisely by "the measurement is concluded"?		Wording changed and enhanced. Please give a hint if we are getting into conflicts with existing recommendations by this requirement.
46		5.2.4		t	5.2.4 "Compatibility of operating systems and hardware, portability" According to a change in version of the operating system, the minimal configuration required for the measuring instrument may change drastically. Therefore, the requirements for the minimal configuration seems not essential to maintain the compatibility.		Wording changed.
47		5.2.6		t	5.2.6 "Maintenance and reconfiguration" Does the version of legally relevant software mean that of a source code or a binary code? In the latter case, a generated binary code may change		Reference to 5.2.5 added, wording of 5.2.5 enhanced.

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					depending on the small time difference in compilation even if it is compiled from the same source code.		
48		5.2.6.2		e	5.2.6.2 (Traced update) If an update of software in electricity meters is already approved by the electric power company, is additional approval by the end-users required?		We cannot give an answer because it had to take into consideration the specific national legislation on type approval.
49		5.2.1.1, 5.2.1.2, 5.2.4, 5.2.5, 6.1, 6.1.1 & 6.4.3.1- *Result*,	RSA	e	Because the manufacturer and the submitter are not always the same body/company we would like to add: "manufacturer/submitter". We believe the onus is on the submitter to provide all the evidence/documentation.		General note in introduction inserted.
50		Sections 3, 5 and 6	NIST, USA	e	Term " legally relevant" is found in over 20 places in the document and refers to both hardware and software. Example from 5.1.1: **"Legally relevant** software shall be clearly identified." We prefer "**under metrological control**" . Reason: improved clarity.	We prefer "under metrological control" or similar words rather than "legally relevant".	Important issue to be discussed at a meeting.
51	5	2.1		e		Add an "s" – give**s** guidance	OK
52	10	3.2.1		t	Audit trail Increased security and authentication capabilities. Clarify the draft to make the requirement very clear that the audit trail must include any event that may change the calculated quantities out of the device. The record should include old and new values and be time and date stamped. In some circumstances, consideration should be given to appropriate security levels adequate to identify who made the change. The	"Audit trail – A continuous data file containing an information record of the changes to the values of the calibration or configuration parameters of a device. Every log entry has a unique time and date stamp."	OK

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					US and Canada in HB 44 use a definition shown in proposed changes. HB 44 also defines: Event Logger – A form of audit trail containing a series of records where each record contains the number from the event counter corresponding to the change to a sealable parameter, the identification of the parameter that was changed, the time and date when the parameter was changed, and the new value of the parameter.		
53	11	3.2.11		g	Fixed legally relevant software part Would this include the basic algorithm used by the primary metering device/system, which should not be alterable at the field level? Perhaps this is covered in 3.2.13?	The requirement that the basic algorithms must be protected from intentional or unintentional alteration at the field level must be firm.	Wording changed
54	11	3.2.13		e		Change “unattended” to “unintended”	OK
55	14	3.4		e	Draft standards are not referenced.	Remove “DIS” and ”FDIS”	OK
56	14	4.2		t	Recommendations are to specify “(a) risk of fraud”	Either remove this suggestion or better define what is intended.	OK, made reference to chapter 8
57	14	4.2		t	Recommendations are to specify “(b) acceptable acchitecture (hardware, software, communication and interfaces)!”	These are prescriptive requirements, limiting the options for manufacturers, and not appropriate.	OK, made reference to chapter 8
58	14	4.4		e / g	We would prefer a restatement in the spirit of use of this as a guidance document.	“Each TC or SC responsible for a particular Recommendation shall determine how to incorporate the relevant portions of this document into their Recommendation.”	OK, tried to improve text.
59	15	5		g	“Measuring instruments shall comply with the following requirements,..” This is too strong a statement for a Document. Only the TC’s and SC’s can establish requirements.	Change language. “The TC’s and SC’s should use this guidance document to establish software related requirements in addition to the other technical and metrological requirements of the relevant Recommendation.”	OK
60	15	5.1.1		e	Software ID	“Software under metrological control	There is a contradiction to

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
				/ t	Expand first sentence to make software version unique.	shall be clearly and uniquely identified with the software version."	comment 214. We tend to follow 214.
61	15	5.1.2		e	Algorithms … Change" testable" to "verifiable"	"Algorithms and functions shall be ~~testable~~ verifiable either by …"	OK. Wording changed in order to avoid confusion with legal verification.
62	15	5.1.2		g	Algorithms … Black Box Testing should be sufficient for testing the correct functionality of the Software. Very rare exceptions involving life and death regulatory circumstances may justify providing source code.	Source Code (Intellectual Property) should not be provided.	Please see our comment to No 87. We cannot follow your argument that source code analysis should not be performed because of the property of the code. Even for a quality assessment procedure according to eg. ISO/IEC 9126 the source code has to be made available to the examiner. Why not for legal purposes? Note: Electrical schematics of the hardware are also manufacturer's know-how, but D11 requires it.
63	15	5.1.3.1		g	Prevention of accidental misuse This is a non-specific requirement and while it is a good objective it would be difficult to enforce.	May be worth a discussion in Section 9. Assessment of software processes.	Perhaps a misunderstanding? We changed the wording: …misuse *by the user* are minimal. We wanted to express the necessity of a robust user interface.
64	15	5.1.3.2		g	Fraud Protection ISO 15408 for Software / Security may provide useful concepts for adoption in implementing this section.		Application of ISO 15408 requires analysis of threats and definition of protection profiles for a certain area of application. We are afraid that this task is too big in the framework of this document. It also assumes high expenditure for the manufacturer. Basicly we agree that application of ISO 15408 would be an optimal concept for evaluating

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
							fraud protection of a measuring system.
65	16	5.1.4		e	Support… This section can be simplified and clarified. The "TC or SC" statement is not needed, since the Document is intended for use by TC/SCs and they have the prerogative to implement as they see fit.	The manufacturer will design checking facilities and durability protection into his software.	Wording changed.
66	16	5.1.4.1		g	Support of Fault detection	Software shall deactivate device or generate an alarm / report in case a fault condition is detected.	OK, sentence added.
67	16	5.2		e	Specific Requirements May want to expand the title	Retitle "Specific requirements (not universally applicable)"	It can be seen from the context whether a requirement is applicable or not.
68	16	5.2.1.1		e	Sub-assemblies… Clarify section.	Sub-assemblies or electronic devices that perform ~~legally relevant~~ functions under metrological control ~~have to be specified as such. Interfaces of these "legally relevant" sub-assemblies and devices~~ shall be clearly defined and documented to show that their relevant functions and data cannot be inadmissibly influenced by commands received via the interface~~:~~	OK
69	16	5.2.1.1		e	This implies.. Delete the comments	Include in previous paragraph. This implies that there is an unambiguous assignment of each command to an initiated function or data change in the sub-assembly or device. The commands and their effects shall be described completely in the software documentation to be submitted for type approval.	OK
70	16	5.2.1.1		e	It also.. The manufacturer does not need to make such a statement.	Include in previous paragraph ~~It also implies that~~ ~~s~~Signals or codes that are not declared and documented as commands have no effect	We did not change this sentence because we didn't understand the motivation. The intention was that the

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
						on the sub-assembly's or device's functions and data. ~~The manufacturer shall state that the documentation of commands is complete.~~	examiner gets all information he needs to decide whether commands are allowed or not (in the sense of the relevant Recommendation). From our experience we have developed the opinion – and the result is this recommendation – that documentation of the interface of a device is essential for today's networked devices but often documented badly. This recommendation doesn't imply a technical restriction but is intended to increase the trust that all information is available for the examiner.
71	17	5.2.1.2		t / g	Separation of Software parts We have received a comment from software developer "The Software (metrological) separation should not be required. It would represent a very rigid requirement on Software Developers when developing applications."	We noted that the 2rd paragraph states: "If the separation of software is not possible or needed, the software is legally relevant as a whole." This statement should be retained to satisfy the commenter's concern.	We were not sure whether we understood your comment correctly (because of linguistic problems). Do you mean that the commenter is right or not? Please point out to the commenter that the intention behind the idea of software separation is to simplify approval procedure and reduce bureaucratic effort and costs. (At PTB, MIRS, LNE we can support this effect). If the programmer succeeds in a clever separation he is (nearly) free in software changes as most changes in complex instruments happen in software parts that are metrologically not relevant.

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
72	17	5.2.1.2		e	If the legally.. Strike non-contributing language. The manufacturer does not need to make a statement about completeness.	~~This implies that a~~All legally relevant functions and data domains of the software are described to enable an examiner to decide on correct software separation. The interface consists of program code and dedicated data domains. Commands or data are exchanged between the parts by storing to the dedicated data domain by one part and reading from it by the other part. The data domain forming the software interface shall be clearly defined and documented. There shall be an ~~unambiguous~~ assignment of each command to an initiated function or data change in legally relevant part of the software. ~~It also implies that c~~Commands that are not declared and documented as commands have no effect on the legally relevant part of the software. ~~The manufacturer shall state that the documentation of commands is complete.~~ Note: Commands may be a sequence of data that causes the legally relevant software part to perform certain functions or data changes. ~~It also implies that the~~ The declared software interface ~~is~~ shall not be circumvented.	OK, but didn't strike "unambiguous". The intention is emphasising necessity of completeness of command definition. (The complete number space of command values must be defined). Did not delete the part about the manufacturer's statement of completeness (see 70)
73	17	5.2.1.2		t	Note "*The programmer is responsible for observing these constraints*" is a meaningless statement without a means of accountability – such as using specified	Delete note	Deletion was not proposed by all commenters. We will shift the note to section 9 (see, however, 96).

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					and audited development process. The programmer can only be held accountable for following a proper development process; it is the instantiation of an appropriate, audited development process that engenders trust. In most instances examination will not be involved in observing the development process. A discussion in Section 9 may be appropriate.		
74	17	5.2.2		e	A display … Strike non-contributing language. Add statement, which allows for remote displays.	A display or printout may be used for presenting both information from the legally relevant part of software and other information. This display or printout may be at a remote location. ~~In that case the following requirement applies: The distinction between these~~ This information shall be clear ~~and unambiguous~~.	We don't understand why you want to weaken the requirement of helping the customer reading (often complex) information on displays. Importance of requirements for clear not confusing indication of measurement values is even increasing with today's windows technology. Note concerning remote displays added, but changed compared to yours.
75	18	5.2.3		e	The data … Clarify paragraph	The data shall be protected by software means to guarantee the ~~their identity,~~ correctness of the information~~.of the~~ time of measurement, authenticity, and integrity. The software that displays or further processes the measurement values and accompanying data checks ~~identity, topicality,~~ the authenticity, and integrity of the data after having read them from the insecure storage or after having received them from an insecure transmission channel. If an irregularity is detected, the data is discarded or marked unusable (OIML	Kept the idea of "topicality" (think of fraudulently "re-using" values of a former measurement) but changed the wording in "time of measurement" Deleted "identity" (=authenticity)

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
						R 117 – 4.3.5, R 49 - 4.3.3.1 and 4.3.3.2).	
76	18	5.2.3		t	For a high … The 4th paragraph conflicts with 5.1.2 examination and 5.2.5 and 6.1. which provides that no "back doors" or hidden functions are allowed.	Delete paragraph	There seems to be a misunderstanding: The sections you quoted deal with the problem of conformity between type and each device and the responsibility of the manufacturer for a correct design. However, what was addressed here is protection against fraud by users or other persons. Application of cryptography for this purpose is state of the art. As expenditure for cryptography is relatively high, the application of this requirement should be balanced with the loss or consequences caused by fraud. The responsible TCs should decide about this, we only want to provide the tools for realising this high protection level. We would like to keep the paragraph and all the resulting requirements.
77	18	5.2.4		g	Compatibility Clarify paragraph	Manufacturer shall identify minimal suitable configuration (processor, RAM, etc.) for correct operation of Software	Wording changed.
78	18	5.2.4		e	If correct, … This is a user requirement.	Delete paragraph	The user is in general not able to decide about this. One cannot assume as much technical knowledge as is necessary for solving this problem. The manufacturer alone is able to define the correct environ-

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
							ment for his software. If the user could even unintentionally change it and disturb the measurement the technical solution would not be suitable for the legally relevant purpose. Merged paragraph with the following.
79	18	5.2.4		e	If a universal … Universal is not a good description of a not built for purpose device. Strike the non-contributing language.	If a ~~universal~~ computer~~s~~ is performing legally relevant functions, it may be necessary to keep the environment of the legally relevant software fixed (hardware, operating system and configuration of whole system~~) especially if requirement 5.2.5 has to be fulfilled for high conformity~~.	A question to you and other native speakers: is "General–purpose computer" a better term? Merged paragraph with previous one, changed wording. Enhanced 5.2.5.
80	19	5.2.5		g	The manufacturer … Obligations are not requirements.	The manufacturer <u>shall</u> ~~is obliged to~~ produce devices and the legally relevant software <u>that</u> conform<u>s</u> to the approved type and the documentation submitted.	OK; we added definitions for levels of conformity
81	19	5.2.6		g	Maintenance & Reconfiguration Finding/Fixing Bugs in Software as well as adding new features and functionality is a very common practice. Evaluation and Approval procedures should be easy to follow and expeditious.		Do you propose change of the wording?
82	19 - 20	5.2.6.1 & Figure		g	Re-verification of updates (and especially software) is emphasized consistently with FDA requirements in 21 CFR Part 820 for re-validation of software changes software used in production of medical devices. Traced electronic updates appear to require an electronic audit trail entry for the instance of the update; however, non-traced updates in the Figure appear not	A suggestion might be to indicate that a manual (i.e. paper) re-approval or paper audit trail is necessary for these updates.	Sentence added.

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					to require an audit trail. Potentially, non-traced updates might require an audit trail that is manifested as an update to the approval certificate or in essence sort of a paper audit trail.		
83	21	5.2.6.2.3		t	The instrument can not know good from bad	Technical means shall be employed to guarantee the authenticity of the loaded software i.e. that it originates from the owner of the type approval certificate. ~~If the loaded software fails this test, the instrument shall discard the loaded software.~~	Explanation added.
84	21	5.2.6.2.4		t	The instrument can not know good from bad	Technical means shall be employed to guarantee the integrity of the loaded software i.e. that it has not been inadmissibly changed before loading. ~~If the loaded software fails this test, the instrument shall discard the loaded software and use the previous version of the software~~	Explanation added.
85	21	6.1		e	For type approval… Obligations are not requirements.	For type approval the manufacturer of the measuring instrument shall ~~is obliged to~~ declare and document all program functions, relevant data structures and interfaces that are implemented in the instrument.	OK
86	21	6.1		g	"*There shall not exist any hidden undocumented functions*" is a meaningless statement without there being a means of reasonably showing that "use, misuse, or abuse" of the system does not result in any illegal or unexpected behavior.	This calls for the incorporation of the structured, systematic and transparent inclusion of ergonomics knowledge in an appropriate, audited development process. Perhaps a discussion in Section 9.	This recommendation doesn't imply a technical restriction but is intended to increase the trust that all information is available for the examiner. The objective is to enable the examiner to give a substantiated finding that **all** functions of a measuring instrument comply with the Recommendations. This is not a specific problem of the software development

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
							process. Please refer to a similar problem discussed in No. 70. The difference in the evaluation of mechanical/electro-mechanical/electronic measuring instruments compared to software-controlled instruments is that not all features are apparent for the latter ones. This deficiency is intended to be compensated by the quoted recommendation.
87	22	6.1		t	In some cases… What cases and what will be done with the source code? Source code is proprietary property of the manufacturer. In lieu of source code, a high level flow diagram provides needed information in conjunction with "black box" testing.	Delete requirement to provide source code.	Added an explanation. We see your point as you also refuse/deny the validation methods that are based on source code analysis. We assume that if high level conformity (5.2.5 (d)) or high level fraud protection is required, the high level validation methods are suitable. The responsible TCs should decide about the level of validation, we only want to provide the tools for realising this level. We would like to keep the paragraph and all the corresponding requirements in section 6.4. Example (relevant today in some countries): Evidential measurements require high trust in the software of the device which can only be attested before the court on the basis of source code analysis.
88	22	6.1		e	The unambiguous…	The ~~unambiguous~~ unique software	"umambiguous" deleted

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					The word “unambiguous” provides no measurable contribution. This adjective cannot be used in enforcement.	identification and instructions for obtaining it from an instrument in use.	
89	23	Table 6-1		g	Clarification of table information	The 5.2.1.2 row of Table 6-1 has an acronym defined DFA/WT where WT is not defined in Table 6-2.	Corrected: CIWT
90	23	Table 6-1 Validation procedure B		t	We have difficulty understanding the circumstances in which type approval would require Validation procedure B. Data flow analysis (6.4.3.4), Code inspection and Walk through (6.4.3.5) and Software module testing (6.4.3.6) are all beyond what should be required for type approval, and almost certainly beyond the capability of most type approval laboratories. We believe that only the software developer has the full capability to perform these types of evaluations.	Delete source code test requirements and Procedure B.	Please refer to 87. FDA “General Principles of Software Validation; Final Guidance for Industry and FDA Staff” considers software validation.
91	22-24	6.2, 6.3, 6.4		g	Improve general flow and understanding of document.	A suggestion might be to present sections 6.3 and 6.4 prior to section 6.2 so that the terminology & acronyms in Table 6-1 after section 6.2 are defined prior to reviewing the table.	OK
92	22-24	6.2, 6.3(c)		g	Improve consistency of this draft document with FDA requirements and guidance for measuring instruments used in design, development, and manufacturing of medical devices	For consistency with FDA guidance, a suggestion might be to discuss in more detail the relationship of risk to level of effort of activities for review of the measuring software. For example, if the measuring equipment is used in an “area of application” such that if the measurement software/equipment fails, then product could be shipped to a customer that causes serious injury or death, then the most scrutiny using methods in 6.4 should be employed, etc.	OK. We propose to incorporate this idea in chapter 8 of the document. **To be done.**
93	24	6.3(a)		e	Reference: to 6.3 change to 6.4	“described in ~~6.3~~ 6.4 shall”	OK

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
94	24	Table 6-2		t	CIWT No source code	Delete source code test requirements	Please refer to 87
95	27	6.4.3.5		t	Code Inspection… Description .. No source code "The examiner tries to understand…" This statement exemplifies the point. This is proprietary property that an examiner has no right to "evaluate".	Delete source code test requirements	Please refer to 87
96	29	9		g	Many subjective statements in the pre-draft involve what should be discussed in this section "Assessment of software processes". It is important to determine the target audience for this discussion. The responsibility for the software development process rests with the instrument/device manufacturer. The successful integration of the software and hardware depends on the processes used during the design, development, validation, verification, maintenance and use of the instrument/device. Documentation of these processes is an integral part of the requirements for medical devices. However, such documentation has not been required in other areas of legal metrology.		OK. We agree. However, we propose to deal with this subject in a second step. Firstly, type approval in a conventional way only evaluating and examining a pattern without knowing anything about the production process of the measuring instrument is still the standard procedure in most (all) countries. Secondly, we think that defining requirements and validation steps for software – what we try with this document - is a precondition for defining rules for software production. Therefore we propose to only make a note in section 9 and elaborate the subject when we have finished the document D-SW (leaving section 9 empty for the time being).
97	38	Annex F 14		g	Event logger, audit trail The Canadian Draft Requirements and US HB44 describe audit trails when there is unlimited access to the instrument. OIML R117 Draft Recommendation describes software security as requir-		Thank you for the hint. However, we should delete all references to existing Recommendations in the final document (see 154).

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					ing a single or multiple levels of password security.		
98	5	1	NMi, The Netherlands	e	It will be difficult to make this Document automatically applicable to existing OIML Recommendations.	Delete the words "*existing and future*" and replace "*International*" by "*OIML*"	OK
99	5	2.3		e	We are not sure what you mean in **this** sub clause with *"relevant Recommendations"*: If (in accordance with the definition in 2.2) you mean "*OIML Recommendations*", this could be understood such that OIML Recommendations would only apply to software-controlled measuring instruments or electronic devices. And this is absolutely not the case. If you mean something like "*recommendations in this OIML Document*" (and that is what we expect), please use a different expression here.	Replace "*The relevant Recommendations*" in this sub clause by (for instance): "*The requirements in this Document*". Alternative possibilities might be: - instructions - advices - encouragements	OK
100	6	3.1.1		e	Add a more detailed reference	[D 11**, 3.1**]	OK
101	6	3.1.2		e	Add a more detailed reference	[D 11**, 3.2**]	OK
102	6	3.1.2		e	Use the actual reference [2]	Replace "*P1*" by the new reference "*B3*" and complete the references in Annex A	OK
103	6	3.1.3		e	Add a more detailed reference The new OIML D 11 (2004) has been published in the beginning of 2005)	[D 11**, 3.3**]	OK
104	6	3.1.4		e	Add a more detailed reference	[D 11**, 3.4**]	OK
105	6	3.1.5		e	Consider also referring to D11, clause 3.5	Consider	OK
106	6	3.1.5		e	Please note that the VIM is being revised and in the present draft, "*error of indication*" is defined in A6	Take note	OK
107	6	3.1.6		e	Consider also referring to D11, clause 3.6	Consider	OK
108	6	3.1.6		e	Please note that the VIM is being re-	Take note	OK

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					vised and in the present draft, "*MPE*" is defined in A10		
109	6	3.1.7		e	Consider also referring to D11, clause 3.7	Consider	OK
110	6	3.1.7		e	Please note that the VIM is being revised and in the present draft, *"intrinsic error*" is defined in A13	Take note	OK
111	7	3.1.8		e	Add a more detailed reference	[D 11, **3.8**]	OK
112	7	3.1.9		e	Add a more detailed reference	[D 11, **3.9**]	OK
113	7	3.1.10		e	Add a more detailed reference	[D 11, **3.10**]	OK
114	7	3.1.10		e	4th line: It seems the text has blindly been copied from draft D11	Replace "..... *defined in 3.10*" by "..... *defined in this definition*".	OK
115	7	3.1.11		e	Add a more detailed reference	[D 11, **3.11**]	OK
116	7	3.1.12		e	Add a more detailed reference	[D 11, **3.12**]	OK
117	7	3.1.12		e	3rd line: It seems the text has blindly been copied from draft D11	Replace "..... defined in 3.12" by "..... defined in this definition".	OK
118	8	3.1.14		e	Add a more detailed reference	[D 11, **3.13.1**]	OK
119	8	3.1.15		e	Add a more detailed reference	[D 11, **3.13.2**]	OK
120	8	3.1.16		e	Please note that the VIM is being revised and in the present draft, there is another definition (4.8)	Take note	OK
121	8	3.1.17		e	Please note that the VIM is being revised and in the present draft, definition 4.10, *"testing"* has been replaced by "*evaluating*" and there are new notes.	Take note	OK
122	8	3.1.18		e	Add a more detailed reference	[D 11, **3.16**]	OK
123	8	3.1.19		e	Add a more detailed reference	[D 11, **3.17**]	OK
124	8	3.1.20		e	Add a more detailed reference	[D 11, **3.18**]	OK
125	9	3.1.21		e	Add a more detailed reference	[D 11, **3.18.1**]	OK
126	9	3.1.22		e	Add a more detailed reference	[D 11, **3.18.1.1**]	OK
127	9	3.1.23		e	Add a more detailed reference	[D 11, **3.18.1.2**]	OK
128	9	3.1.24		e	Add a more detailed reference	[D 11, **3.18.2**]	OK
129	9	3.1.26		e	Add a more detailed reference	[D 11, **3.19**]	OK
130	9	3.1.27		e	Add reference to D 11	[D 11, **3.20**]	OK
131	9	3.1.28		e	Add reference to D 11	[D 11, **3.20.1**]	OK
132	9	3.1.29		e	Add reference to D 11	[D 11, **3.20.2**]	OK
133	9	3.1.30		e	Add reference to D 11	[D 11, **3.20.3**]	OK
134				e	We suggest adding a definition for	Add definition	To be done! We need the lat-

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					"*evaluation*"		est draft VIM to copy the definition.
135	10	3.2.1		e	Does this mean that, for instance for a counter scale, the results of every individual weighing have to be logged?	Please clarify	OK, definition enhanced
136	10	3.2.2		e	Please note that the word "*verification*" as used here seems not to comply with the definition in the VIM and the VIML	Please clarify	OK. Is term "checking" better?
137	10	3.2.8		e	In the way it has been described here, it is a description, not a definition	Please clarify	This section is headed "Software Terminology". The intention is to explain how certain established terms are used in this document. It is not intended to give binding definitions for these terms.
138	10	3.2.9		e	According to our opinion, the word "*calibration*" has been used wrongly here. Ref. VIM 6.11	Replace "*calibration*" by "*adjustment*"	OK
139	10	3.2.9		e	The sentence "*they are .... the instrument*" is a requirement, not (part of) a definition.	Move to the requirements	OK. Moved to 5.1.3.2 (iii)
140	10	3.2.9		e	The sentence "*Device-specific .... product vendor*" gives possible solutions which should not be a part of a definition.	Move to a note to 3.2.9 or to a note in the requirement.	OK. Moved to 5.1.3.2 (iii)
141	11	3.2.13		e	We suggest adding "*repair, or maintenance*".	Add "*repair, or maintenance*".	OK, done
142	11	3.2.18		e	Please note that "*measuring instrument*" has been defined in the VIM, 4.1	We suggest moving this definition to the "general definitions" in 3.1 and adapting the definition of VIM 4.1	OK
143	12	3.2.25		e	We suggest replacing "*... an irrelevant part ...*" by "*... a **legally** irrelevant part.*"	Replace	OK
144	12	3.2.29		e	The last sentence "*They are .... the instrument*" is not (part of) a definition.	Move to the requirements	OK
145	13	3.3.2		e	Replace "*pattern*" by "*type*" (refer to VIML)	Replace	OK
146	13	3.3.8		e	Please note that the word "*verification*" has another meaning in VIM and VIML !	Reconsider this expression.	OK

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
147	14	4.1		e	Replace the 1st "*R-documents*" by "*OIML Recommendations*" and the 2nd "*R-documents*" by "*OIML Documents*".	Replace	OK
148	14	4.2 (b)		t	This document should give more guidelines for an acceptable architecture.	Add such guidelines.	Introduction to Chapter 4 changed. Guideline for acceptable architecture to be added, if still necessary.
149	15	5.1		e	We suggest adding at the beginning: "*At the time of publication of this Document, the general ....*"	Add	OK
150	15	5.1		e	Add: "*considered in all **OIML** Recommendations.*"	Add	OK
151	15	5.1.1		e	The term "*interruptible measuring instruments*" needs to be defined in chapter "Terminology"	Add	OK. Term deleted in the text.
152	15	5.1.2		t	Please note that in a few cases price calculation is purposely incorrect from a mathematical point of view (rounding off prices)	Consider	OK
153	15	5.1.3.2(i)		t	What is "*hardware memory*": - ROM's ?	Please clarify	OK
154	16	5.1.3.2(iv)		e	In this stage of the development of this Document it certainly makes sense to refer here to these Recommendations. But in the final version, reference from a "Horizontal Document" ("D") to a Recommendation ("R") should be avoided.	Remove these references in the final version.	OK. To be done.
155	16	5.1.4.1 and 5.1.4.2		t	A Recommendation (legislation!) should not recommend appropriate technology	Delete this sentence.	OK, wording changed.
156	16	5.2		t	The expression "*conventional instruments*" is not defined.	Replace "*conventional instruments*" by *"instruments that are not controlled by software"*.	OK
157	17	5.2.1.2		e	As the expression "*examiner*" is not usual in OIML terminology, we suggest to replace this word by *"testing authority"* or "*type approval authority*"	Replace	OK
158	17	5.2.1.2		e	Note at the end:	Replace "*programmer*" by "*manufac-*	OK

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					It is the manufacturer (company) of the measuring instrument who is responsible; not the programmer (person or sub-contractor).	*turer of the measuring instrument*", and either consider deleting the last sentence "*The programmer ..... .requirements.*", or add in the last line: "*... instructed **by the manufacturer** about ...*"	
159	17	5.2.2		e	In this stage of the development of this Document it certainly makes sense to refer here to R 125. But in the final version, reference from a "Horizontal Document" ("D") to a Recommendation ("R") should be avoided.	Remove these references in the final version.	OK
160	18	5.2.3		e	The expression "***deferred** legally relevant use*" is not generally applied	We suggest to replace "*deferred*" by "*future*".	OK
161	18	5.2.3		e	Last paragraph: "*... shall be kept secret ...*". Who may have access to these keys? - The manufacturer of the measuring instrument? - A Subcontractor (programmer)? - A service engineer working for a distributor of the manufacturer - An independent service engineer? - The test lab (type test/evaluation)? - The body performing the initial or subsequent verification? - The inspection body? -	Please clarify	OK
162	18	5.2.3.2		e	Replace "*must*" by "*shall*". (OIML terminology; refer to the OIML "Directives for the Technical work")	Replace	OK
163	18	5.2.4		e	4th line: The manufacturer of the measuring instrument or the manufacturer of the software?	Please clarify	OK, wording changed, the manufacturer of the measuring instrument is addressed.
164	18	5.2.4		e	Last paragraph: "*computer*" singular or plural?	Replace "*computer**s**"* by "*computer*".	OK
165	19	5.2.5		e	Title: replace "*pattern*" by "*type*".	Replace	OK
166	19	5.2.6		t	The OIML Recommendations shall give	Replace "*depends on the legal regu-*	OK

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					the guidelines for "legal regulations in a country".	*lations in the country"* by "*depends on the kind of instrument and is to be worked out in the relevant OIML Recommendation*."	
167	19	5.2.6.1		t	Last words (in brackets): Also in the relevant OIML Recommendation such information can be included.	We suggest to add: *"(if not .... **in the relevant OIML Recommendation or** in the ...)"*	OK
168	19	5.2.6.2		t	The OIML Recommendations shall give the guidelines for "national legislation".	Replace "*national legislation*" by "*the relevant OIML Recommendation*."	OK
169	19	5.2.6.2		e	We suppose that by "*the verification*" the secretary means "*subsequent verification*" (VIML 2.16)	Replace "*the verification*" by "*a subsequent verification*".	OK, Fig. 5-1 to be changed
170	20	Fig 5-1		t	"*Request software update*" by whom: - automatically (periodically via network or Internet)? - by user? - by person authorized by owner (I.e. QA manager)? -by service engineer of manufacturer? - by independent service engineer?	Please clarify	It is not clear to us why you want to identify the person who requests an update. Important from our point of view is only the fact that an update occurs. Securing means should be independent from the reason for the update and from the party who requested it. Anyone who has authorised access to the measuring instrument should be able to perform it.
171	20	Fig 5-1		t	"*Loading of updated files*": Replacing existing files or (temporary) stored ?	Please clarify	OK added a note with an explanation
172	20	Fig 5-1		t	We miss a block with the action in case neither the integrity is valid nor the authenticity is valid	Please clarify	OK. Box added (to be done). Failed update is recorded (enhanced wording in 5.2.6.2.5).
173	20	Fig 5-1		t	We miss a block with the action in case the verification was not successful	Please clarify	There is no action. Added a box in the branch "Successful verification" instead.
174	21	5.2.6.2.5		e	3rd line: replace "*controls*" by "*verification and surveillance or inspection*". 6th line: Replace "*The traceability..*" by "*This traceability ...*"	Replace	OK
175	21	5.2.6.2.5		t	"*...on national legislation*". We would prefer to have this "*adequate period of*	Specify the "*adequate period of time"*	We believe that in a Document no general prescriptions can

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					time" specified (proposed) in this document.		be made. If possible at all the responsible TCs have a better chance to define an acceptable value for the kind of instrument or area of application under consideration.
176	21	5.2.6.2.6		t	For reasons already given above, remove *"Relevance ...national legislation"*.	Remove	There may be laws beyond Legal Metrology that regularise the responsibility of the owner.
177	21	6.1		t	*"there shall not exist any hidden undocumented functions"*: We think, it will be difficult to check for any hidden undocumented functions.	Please clarify	For lower conformity level this is stated by the manufacturer. For high level conformity it is to be verified by an appropriate validation method (eg. DFA/CIWT)
178	22	6.1.1		e	6th line on page 22: Replace "*approval examiner*" by "*testing authority*" or "*type approval authority*".	Replace	OK
179	22	6.1.1		t	19th line: Replace "*..., **if not** described ...*" by *"... **to be** described ..."*	Replace	Wording changed.
180	22	6.2		e	We propose to add: "*It is the aim **of the type test** to validate ..."*	Add 4 words	OK
181	24	6.3		e	We think, the reference to 6.3 should be to 6.4.1	Please check	OK
182	24	6.3		e	What are *"A and B type*" ?	Please clarify	OK, reference added
183	24	6.3		t	We suggest adding a 4th dot: "*Risk of wrong measurement result due to operating errors*" This can in particular be applicable for measuring instruments for the police, like radar equipment for measurement of the speed of vehicles.	Add	OK
184	24	6.4.1		t	VFTM: Price calculations are on purpose not always exactly correct in cases the price to pay is rounded to the nearest (for instance EU 0,05). The same may apply for counting scales, where the number of for instance nails	Please take note	OK

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					or screws is calculated by the scale.		
185	24	6.4.1		e	VFTSw: we suggest adding: "*protection against operating errors*" (for instance measuring instruments for the police)	Add	OK
186	25	6.4.2		e	In the title, we suggest to replace *"Specifics"*: by *"Details"*.	Replace	OK
187	25	6.4.2		e	5th line: we suggest to remove the words *"try to*".	Remove	OK
188	25	6.4.2		e	last paragraph: remove the word "*approval*" (refer to the VIML)	Remove	OK
189	25	6.4.3.1		t	*Description*: these "checklists" should preferably be included in the Test Report Format.	Add	OK. To be done.
190	25	6.4.3.1		t	*Result*: add at the end: "*included in the Test Report Format of the relevant Recommendation".*	Add	OK, done
191	26	6.4.3.2		e	References: Which specific OIML Recommendations?	Please clarify	To be done.
192	28	7		t	Delete the 1st part of the 1st sentence: "I*f a metrological ...in a country."* And delete at the end: *"(and possible ...in the country)"*	Delete	OK, done.
193	28	7		e	Replace *"pattern*" by *"type*".	Replace	OK, done.
194	29	8.2 (a)		t	"*Social and societal impact of errors*" can also be others than fraud; for instance getting an undeserved fine based on a wrong measurement by the police. This example was the reason of this expression in the new D 11.	Reconsider the text	OK
195	29	8.2 (c)		e	What have "*electrical and electromagnetic conditions*" to do with software? (obviously copied from D 11)	Reconsider this text	We have generalised the item; we think that the environmental conditions may be taken into consideration when deciding on the level of (software) fault detection and durability protection.
196	29	9		e	Is it the intention of the secretary to complete this text before the final ver-	In the 2nd case, delete this clause	It is intended to complete the text later (see comment 96).

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					sion of this document, or is it to be considered later?		
197	31	Annex B		e	Title: replace "*for*" by *"of"*.	Replace	OK
198	32	Annex C		e	Add in the 1st line: "*The **Technical Committees or** sub-committees …*"	Add	OK
199	32	Annex C		e	The expression "*Test Certificate*" is (so far) not common in OIML. Also there is no definition or any other occurrence of Test Certificate.	Replace "*Test Certificate*" by "*OIML Certificate of Conformity*"	OK
200	32	Annex C		e	Text in bold face: Replace "*DF101*" by "*DF100*"	Replace	OK
201	33	Annex C		e	Typing error in the 9th line.	Replace "*document*" by "*document**s***".	OK
202	33	Annex C		-	We hearty welcome our new colleagues Fehler and Problème !	-	OK. The author for this funny wording was Jan Jacobson, SP, Sweden, on another occasion.
203			Measurement and Safety Service, New Zealand				
204		5.1.2, 6.2, 6.3 and 6.4	Measurement Canada / Mesure Canada		The validation methods seem logical. It would now be up to the TCs working on the recommendations to judge which feature required which level of treatment. (good)		OK
205		5.1.2, 5.1.3			5.1.2 covers the general requirement for software to be designed in such a way that it is capable of producing accurate results. 5.1.3.1 deals with unintentional misuse. The intent of regulations 66 and 68 [Canada's Draft Metrological Software Specifications] are to eliminate possibilities of fraud, which could be deemed as <u>intentional misuse.</u> 5.1.3.2 (ii) This section deals with fraud via user interfaces (good).	Suggest the wording [of 5.1.3.1] be modified so that both unintentional and intentional misuse was addressed.	OK. See also 215.

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					6.1 also prohibits “back doors” or undeclared features		
206		5.1.3.2			5.1.3.2 (i) covers this comment [on Fraud Protection in Questionnaire] adequately.		OK
207		5.2.3			5.2.3 covers this comment [on Questionnaire] well, stating conditions under which legally relevant data may be transmitted.		OK
208		5.1.4 regarding stopping of measurement process: we think it can not be generalized			Understand response and agree that TCs working on individual recommendations would able to define this requirement for specific situations. (agree with comment and section)		OK
209		5.1.4, 5.2.4 regarding stopping of measurement process: we think it can not be generalized			The stopping or preventing of the software from running in this case, is purely a software environment issue. In the case where a software program determines that it doe not have adequate resources or other software is interfering with its operation, shutting down is a logical response. Perhaps this can be addressed by TCs working on recommendations, but some guidance may be required.		OK. The effects you are addressing (too small resources, interference of other programmes) are of different nature compared to faults addressed here. Faults originate from statistical physical effects and are non-deterministic whereas limits of the software resources are calculable in principle (maybe it is difficult but possible in many cases). Instead of constructing software that detects lack of resources as you propose, it would be a better solution to calculate the needs for resources and perhaps oversize them. This is proposed in requirement 5.2.4. The detection

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
							of interference – your 2nd point – is dealt with in 5.2.1.2.
210		5.2.1.2			Identification of parts, interfaces 5.2.1.2 has taken this comment into account. Developers are given the option to separate metrological software if they choose.		OK
211		6.1.1			Documentation 6.1.1 gives a thorough list of what documentation is expected to contain.		OK
212		5.2.5, 5.2.6			Conformity 5.2.5 obligates a manufacturer to only produce software the same as approved. (good) 5.2.6 deals with updating the software in a particular device after it has been initially inspected. The comment was directed at creating a less stringent approval process for updates to software to correct bugs, not to add feature.		Should we change the wording or add something?
213		5.2.1 Agree, different procedures proposed, see chapter 6.2, 6.3 and 6.4. Please consider and let us know your opinion			The current draft does not distinguish built for purpose devices from utility computers. This may be seen (by manufactures) as imposing rules on the software in built for purpose devices without justification.		The draft doesn't explicitly use these terms but still distinguishes between simple and complex computer systems: section 5.1 gives general requirements for all kinds of software controlled instruments whereas 5.2 contains the requirements for more complex systems. The result is a system of requirements that can easily be adapted by the responsible TCs to the needs for the kind of instruments under consideration.

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
		5.1.1 5.1.3, 5.2.6					
					The 2nd comment was intended to generate thought as to whether or not all aspects of metrological software required approval. The thought is that if the device provides a dependant customer enough information that they can confirm the calculations were perform correctly, then there is not a need for the software to be approved. Perhaps this is something that can be addressed by TCs when they work on specific recommendations.		It should be decided by the responsible TC which kind of instruments or auxiliary devices shall be subject to the requirements.
					The final paragraph of the comments was suggesting that the software document address the idea of sealing software. It was included in the Canadian specification because it was not addressed elsewhere in the legislation,. As well, it was felt that the flexibility allowed developers of software should be offset by tools to assist the persons doing the verifications to see what has been changed, when the software has been modified (audit trails). If this is not addressed here, there will be a variety of approaches taken for different instrument types. Currently R 117 requires that only the last intervention be saved. This is based on the premise of providing the same level of protection as a mechanical seal. In reality, when mechanical devices were sealed, they typically only had one feature to seal, the adjust-		We have added a requirement concerning audit trails with multiple entries (see 5.2.6.2.5)

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					ment. Current electronic devices have many features which were simply not possible with mechanical devices under seal. If only one e vent is recorded, the person conducting a verification would have no clue what had been changed. It is again suggested that a section on audit trails be included. It could contain multiple level of protection dependant on the environment the device is being used in. These could be modelled after existing requirements for which compliance has been demonstrated. TCs could then choose if it were appropriate to include such requirements in the individual recommendations.		
214		5.1.1	Dennis Beattie		5.1.1 It is not clear whether the identification needs to be unique (as in a serial number) or generic (as in a model number). Unique would be more difficult for manufactures and could disrupt the ability to distinguish if a program is the same as the version approved. You would not be able to do a checksum or bit by bit comparison for unique.		Should be generic not unique.
215		5.1.3.1			5.1.3.1 This section requires the manufacture to protect against accidental misuse. While this is important, it is more important to protect against intentional misuse (hacking). Wording could be revised to cover both. Section 5.1.3.2 (ii) addresses this as well.		OK. See also 205.
216		5.1.3.2			5.1.3.2 (iv) This section or a whole new section should go into much greater detail with regards to what is acceptable with respect to electronic sealing. Some of the current recommendations are very weak in this area. Having sev-		OK we agree. Should we add a separate section with acceptable solutions (not only for this item)?

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					eral levels of audit trails for TCs to choose from based on the risk requirements may be an approach.		
217		5.2.6.1			5.2.6.1 This section is putting in place a mandatory inspection each time a devices software is changed. Depending on the device, this may or may not be truly necessary. Currently we do not require this.		The application of mandatory inspection seems to differ in the various countries. We tried to show the idealised cases. Please make proposes for alternatives that may be generalised.
218		5.2.6.2			5.2.6.2 This section details a procedure for updating software on a device. It should be made mandatory that a device employs this technology if there is an option for (radio frequency) RF data exchange.		OK we agree. But it is up to the responsible TCs to require this.
219		5.2.6.2.2			5.2.6.2.2 This section requires a very low level program that oversees the software update process not to be updateable. It is not clear how this can be done, particularly with universal computers. The lowest level of software is the BIOS and even it these can be updated.		We agree. The described procedure is not possible with an off-the-shelf general purpose computer. A specific additional hardware in such a computer is necessary to fulfil 5.2.6.2.
220		5.2.6.2.6			5.2.6.2.6 This section requires the device to have a means which to prevent software update unless the device owner has given his permission. While I'm not clear what form such means might take, I question why this is a requirement. If a manufacturer discovered a bug in his program that resulted in errors which were in the favour of the owner, this section would give him the option not to rectify the problem.		OK we see your point. Do you propose to delete this item?
221		6.1.1			6.1.1 Under the second º, it lists "Tools necessary...". This section is defining what the documentation should include. Perhaps it requires "A descrip-		OK deleted the item.

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					tion of the tools....", but I suspect it is a requirement for the actual text editing software, and therefore should be listed separately.		
222		6.1.1			6.1.1 The documentation should also include a description on the logic or methods employed in the fault checking routines. (The second paragraph under 5.1.4.1, indicates that this is required. It could simple be repeated here)		OK done.
223		6.4.2			6..4.2 When it is not clear how to validate a function of a software program the onus to develop a test method should be placed on the manufacturer. In addition, the services of the programmer should be made available to the examiner for the purposes of answering questions.		OK done (new item in 6.4.3.1)
224		8.2			8.2 Under section(a) there should be two more bullets as follows - Platform (built for purpose or universal computer) - exposure to sources of potential fraud (unattended self service device)		OK done.
225			Jacques Senave, (CITEF, Association of European Electricity Meter Manufacturers), <jsenave@skynet.be>	g	We have received your mail but we wonder if there is duplication beween the works of OIML TC 5 and WELMEC WG 7 chaired by Mr Schwartz (PTB) on the same subject. Have you any explanation?		WELMEC guides are mainly based on the European regulations that are not relevant outside Europe. OIML has to observe other international regulations, too. Therefore, the structure of the document differs from WELMEC WG7 documents – hopefully not the contents.
226			Hans		(Wants to be added to the mailing list.)		

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
			Lamot Regulatory approvals director Chairman CECOD TC, Lamot@bladel.tokheim.com				
227			Michel TURPAIN CECIP Permanent Secretary, <tur-pain.cecip @wanadoo .fr>		(Confirmation of receipt only)		
228			Ludwig Paul - Pro-gramme Manager Standards Develop-ment (STDDEV) CEN - European Committee for Stan-dardization Rue de Stassart 36, B-1050 Brussels, <lud-		(Confirmation of receipt only)		

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
			wig.paul@cenorm.be>				
229			Sabine Froning, Euroheat & Power Av. de Tervuren 300 B-1150 Bruxelles, <sabine.froning@euroheat.org>		(Confirmation of receipt only)		
230			Dr. Brian W. Petley NPL (IUPAP) International Union of Pure and Applied Physics <Brian.Petley@npl.co.uk>		Terminology: (1) I notice that you cite the VIM definitions. (i) As you probably know, the VIM is currently under revision and amendments have been proposed to many of the definitions in the first edition. (ii) The original intention of the form of words chosen for the VIM definitions was that in each case the word or phrase could be replaced by the definition and still make grammatical and physical sense in the context in which they were used.		We will use the latest version of the VIM definitions.
231		5.1.2 Correctness of algorithms and			(2) If we consider the saying 'garbage in, garbage out' then, since the Software generates the latter from the former, the Software can only said to be validated if the outcome is no worse than the input data - in all circumstances.		If an overall examination is done both failures in the transducer or caused by the software algorithms may be detected. The validation method proposed here (6.4.1 “VFMT”) takes this into consideration.

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
		functions			I am not at all sure that one can necessarily completely separate the measurement algorithm from the characteristics of the actual measuring transducer. This implies that one cannot validate the Software, in toto, as a separate entity.		
232					Thus, an innocuous seeming instruction 'take a reading every second' could cause measurement problems if the instruction did not distinguish between sampling synchronously or asynchronously with respect to the mains' power frequency. Such problems could cause software to be valid in one country and invalid in another, according to the respective power frequencies. Further, the accuracy of the process of obtaining an average from repeated measurements would depend on the accuracy analogue to digital conversion process - leading to an inaccurate variance. For example, the last digit may be read as a '1', but this does not mean that it lies within 0.5 and 1.5 with uniform probability. One could not necessarily obtain an extra decimal place (1.2, for example), as a result of repeated averaging. A print-out of the standard error of the mean would have to take account of this rounding problem if more than a limited number of results had been averaged.		At the end it is the intuition of the examiner that is needed to find out effects you described – no matter whether the instrument is software controlled or not.
233					Further, I would have thought that a flow measuring instrument such as that		Thank you for the hint. We have improved the example

No	Page	Section	Author	*	Comment, Problem *) e – editorial, t – technical, g – general	Proposal for Correction	Changes in Document Draft (D-SW_v11.doc)
					cited in the example could not be properly validated if it did not include a measurement of the temperature of the liquid as part of the measurement process.		accordingly.
234					Software validation procedures are essential, but are best regarded as being 'necessary, but not sufficient'. I would therefore be inclined to suggest that any certificate of compliance for the Software should be accompanied by a caution.		We agree absolutely. The software requirements and validation methods have to be applied in addition to the various metrological requirements and test procedures described in the existing OIML Recommendation.