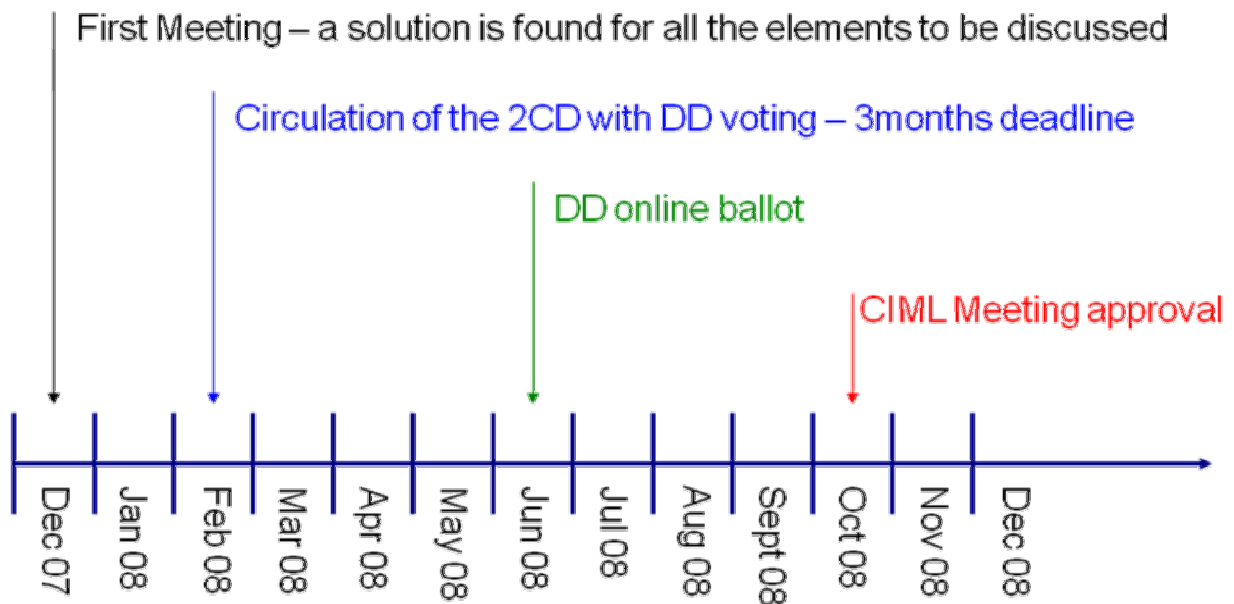


**TC 5/SC 2 – First Meeting**

**Draft Minutes**

- 1) The Draft Agenda is approved without modification. It is accepted to discuss the late comments provided by CECIP and UK Metering Forum (UKmf) at the end of the meeting.
- 2) Roll call of the delegates, presentation of the delegates. As 12 P-members were present the minimum number of participants for voting on controversial issues (11 P-members) was outnumbered.
- 3) The TC 5/SC 2 Members accept the time schedule proposed by the TC 5/SC 2 Secretariat.



- 4) Decisions on the issues discussed during the meeting are summarize in the following table.
- 5) The necessity of a future meeting before the final approval of the document by the CIML will be considered according to the future comments on the 2 CD.

## First meeting of the TC 5/SC 2 – Draft Minutes

Chapter	Country	Comments on and proposals for modifications	Secretariat's Replies	Decided during the meeting (decision)
General	US	<p>There is a disconnect between Sec. responses and text in the draft received. This is prevalent throughout all the comments.(e.g. US comment about legally relevant, Response Legally relevant: under metrological control, software/hardware or part of the software/hardware of a measuring instrument which interfere with the accuracy of the data under legal control of a measuring instrument.</p> <p>The US is unsure as to whether the correct draft was distributed.</p>	<p><b>To be discussed</b> The wording, "under metrological control" is not appropriate. It implies that all metrological quantities are legal metrology quantities: that is not true, otherwise software separation would be useless.</p>	<p>The definition proposed by the Secretariat is accepted. <i>"Legally relevant: software/hardware/data or part of the software/hardware/data of a measuring instrument which interferes with the accuracy of the measurement regulated by legal metrology or with the correct functioning of the measuring instrument."</i></p> <p>The Secretariat will add a sentence stating that OIML TCs have to identify in their Recommendations elements that are legally relevant. Furthermore national regulation may specify different elements.</p>
3.2.1	UK	<p>Clauses include the term "legally relevant" which is not defined in this Document. There are multiple types of information stored, processed, or calculated by a taximeter that may fall under some type of legal control. However, not all effect the final results. Suggest clarifying which parameters must be sealed/secured even though they might be accessed for repair or undergo maintenance. It should be transparent how much and which type of information or data is secured and tracked.</p>	<p><b>Accepted/ To be discussed</b> The definition of Legally relevant has to be discussed. <i>"Legally relevant: software/hardware/data or part of the software/hardware/data of a measuring instrument which interferes with the accuracy of the measurement regulated by legal metrology or with the correct functioning of the measuring instrument."</i></p>	Solved by the new definition of legally relevant
3.2.10				
3.2.12				
3.2.16				
3.2.17				
3.2.16	US	<p>(Legally) <del>relevant</del> <u>controlled metrological</u> parameter <u>Software</u> Parameter of a measuring instrument or a sub-assembly subject to legal <u>metrological</u> control. The following types of <del>legally relevant</del> <u>controlled metrological</u> parameters can be distinguished: type-specific parameters and device-specific parameters.</p>	<p><b>To be discussed</b> See the proposed definition of Legally relevant just above.</p>	Solved by the new definition of legally relevant
3.2.17	US	<p>(Legally) <del>relevant</del> <u>controlled metrological</u> software part The part of all software modules of a measuring instrument, device, or sub-assembly that defines or fulfils functions or represents features which are subject to legal <u>metrological</u> control. Any part of the software which has an influence on the measurement result, especially displayed, transmitted or stored measurement result. By definition, any part of the software that participates in the calculation of the measurement result is a legally <del>relevant</del> <u>controlled metrological</u> software part.</p>	<p><b>To be discussed</b> See answer to the UK above.</p>	Solved by the new; definition of legally relevant
General	US	<p>Lets do away with legally relevant. I have suggested the following adjectives, (Legally) <u>controlled metrological</u> parameter, and (Legally) <u>controlled metrological</u> software part. The word legally is in parenthesis because it is implied and need not always be stated. This is analogous to "(legal) metrological control" in the VIML. Replace all instances of legally relevant software with controlled metrological software in text outside the terminology section because it more appropriately describes our intent.</p>	<p><b>To be discussed</b> See answer to your previous comment.</p>	Solved by the new definition of legally relevant
3.1.3	CECIP	<p>It seems to be to stringent to require any sub-assembly to be equipped with either a display, a printer or a communication interface. If software identification for each sub-assembly shall be</p>	<p><b>To be discussed</b> We appreciate that for</p>	Solved by the German proposal (imprint of the version number on the housing)

## First meeting of the TC 5/SC 2 – Draft Minutes

Chapter	Country	Comments on and proposals for modifications	Secretariat's Replies	Decided during the meeting (decision)
		required, then a simple marking on the sub-assembly should be sufficient.	several categories of measuring instrument, this requirement may be too stringent. Specific conditions may be found for exemption.	
5.1.1	CECIP	It seems to be too stringent to require any sub-assembly to be equipped with either a display, a printer or a communication interface. If software identification for each sub-assembly shall be required, then a simple marking on the sub-assembly should be sufficient.	<b>To be discussed</b> We appreciate that for several categories of measuring instrument, this requirement may be too stringent. Specific conditions may be found for exemption.	Solved by the German proposal (imprint of the version number on the housing)
5.1.1	D	Add the end of the requirement clause:  As an exception for non-interruptible measurements an imprint of the software identification on the name plate of an instrument shall be an acceptable solution under the following circumstances:  A. The user interface does not have any control capability to activate the indication of the software identification on the display or the display does not allow technically showing the identification of the software (mechanical counter).  B. After production of a meter a change of the software is not possible or only possible, if also the hardware or a hardware component is changed.  The manufacturer of the hardware or the concerned hardware component is responsible, that the software identification is correctly marked on the concerned hardware.	<b>To be discussed</b>	The TC 5/SC 2 Secretariat will develop a specific requirement based on NMI (Paul Kok) proposal (annex to the Draft Minutes). CECIP will be consulted for validating the proposal.
5.1.1	JP	We concluded to withdraw our proposal in this section, since introducing the word "descriptive plate" would result in other problems, as the secretariat's comment suggests.	<b>To be discussed</b> Thank you for your understanding. The question is still open: Is it possible to remove/reduce the information on the nameplate of a measuring instrument if that information can be displayed/printed by the measuring instrument (software) itself?	Solved by the German proposal (imprint of the version number on the housing)
5.1.1	US	Requirement: Legally relevant software of measuring instrument/sub-assembly shall be clearly identified with the <u>metrological</u> software version <del>or another token</del> . The identification may consist of more than one part but <u>only</u> one part shall be <u>only dedicated</u> for the legal purpose. The identification shall be inextricably linked to the software itself and shall be presented or printed on command or displayed during operation. If a sub-assembly has	<b>To be discussed</b> There is no reason to reduce the identification of the legally relevant software to only one part	A detailed example of a version number (e.g. A.Y.Y.Z) will be added to the document with a rationale for each token that compose the version number.

## First meeting of the TC 5/SC 2 – Draft Minutes

Chapter	Country	Comments on and proposals for modifications	Secretariat's Replies	Decided during the meeting (decision)
		neither display nor printer, the identification shall be sent via communication interface in order to be displayed/printed on another sub-assembly. Purpose: Each measuring instrument in use has to conform to the approved type. The software identification enables <a href="#">surveillance verification</a> personnel and <del>persons</del> <a href="#">parties</a> affected by the measurement to determine whether the instrument <del>under consideration</del> is in <a href="#">conformity with the requirements</a> .	of the version number. As an example, it can be useful to split the software version number of a flow computer. Thus one part could represent the resident software of the flow computer, another could correspond to the type of conversion that the computer can perform (@15 °C, @ 20 °C, T only, P and T) another part could correspond to the implementation(or not) of a correction curve function...	
5.1.1	CA	Example(II): - This example implies that a checksum alone is a suitable means to identify the software. We agree that the checksum is suitable to confirm the software is unaltered in comparison to version submitted for evaluation, but question whether it serves as an identifier without the textual string described in example 1. We suggest that the checksum, in addition to the textual string be deemed acceptable, but not alone.	<b>To be discussed</b> The checksum is inextricably linked to the software in a way that for a given value of the checksum, there is only one version of the software. Thus, the checksum can be used as a version number, it is not useful but acceptable.	The Secretariat answer solves the comments
5.1.1	DK	In Requirements second paragraph after "displayed during operation" add "or at start up for measuring instruments can be turned off and on again".	<b>To be discussed</b> The possibility to display the software identification has been removed from the first WD according to Canadian comments.	Accepted
5.1.3.2	CECIP	Requirement c) for providing a method for displaying or printing the current parameter settings is not acceptable. Stile and content of parameters that fix legally relevant characteristics are very different, are not always programmable and are not always operable by the user. Only the manufacturer needs access to such parameters to configure the instruments before delivery. Therefore typically high priority password protection is used. It would be dangerous to mention these passwords in the TACs that are available to the public.  A verifying authority shall take a measuring instrument as a black bock and test this black box against the essential technical requirements. As common practice it should not be the intention of an OIML document to change requirements into technical solutions.	<b>To be discussed</b> The display/printing of these parameter facilitate verification in the field and also market surveillance.  We agree that some of the parameters do not have to be modifiable by somebody other than the measuring instrument manufacturer. Printing these parameters would not mean that these	A new sentence is proposed and accepted during the meeting: <i>Parameters that fix legally relevant characteristics of the measuring instrument shall be secured against unauthorised modification. For purpose of verification the necessary current parameter settings shall be able to be displayed or printed.</i>

## First meeting of the TC 5/SC 2 – Draft Minutes

Chapter	Country	Comments on and proposals for modifications	Secretariat's Replies	Decided during the meeting (decision)
			<p>parameters could be modifiable by just anybody.</p> <p>Additionally, passwords are not required to be revealed in the type approval certificate but it has to be stated that parameters are password protected or switch protected...</p>	
5.1.3.2	DK	Requirement (c) : "The current parameter settings must be able to be displayed or printed". This is technical not possible to fulfil for some measuring instruments.	<p><b>To be discussed</b></p> <p>We understand your concerns but we do not see when it could occur.</p>	Solved by the new sentence (see above CECIP §5.1.3.2)
5.1.3.2	CA	<p>Requirement (d): From the reference (R 105 part 13.3.1 a and R 117 part 4.3.3.1 a) we gather that a "checking" feature (R 117 terms) is required to ensure that legally relevant software and data has not been inadmissibly altered. We did not get this meaning from the requirement or examples as written. In the case of the examples, they appear to allow for electronic sealing means to meet the requirement. If the intent of this section is the same as the references, sealing is not adequate and the requirement should be stated in a clearer manner. We suggest:</p> <p>Legally relevant software shall include a means, in addition to a physical seal or electronic seal, to make inadmissible alteration of the software or data, impossible or evident.</p> <p>Example: The software contains a routine which periodically performs cyclic redundancy check on the software and relevant data and compare the results to previously determined values. If there are differences the device will indicate a fault condition or discontinue the measurement process.</p>	<p><b>To be discussed</b></p> <p>The requirement has been clarified and references to OIML Recommendation removed (inappropriate).  <i>Software protection comprises mechanical sealing and electronic or cryptographic means .</i>  <i>They shall render unauthorized intervention impossible or evident.</i></p>	The Secretariat answer solves the comment
5.1.3.2	US	<p>Requirement(d): Depending on the risk classification, mechanical sealing only is sufficient. See previous comments on audit trails.</p> <p>Protection comprises mechanical sealing <del>and</del> or electronic <del>and</del>/or cryptographic means making an inadmissible <u>unauthorized</u> intervention impossible or evident.</p> <p>Cannot mechanical sealing alone be sufficient? Is electronic sealing a requirement?</p>	<p><b>To be discussed</b></p> <p>See above answer to Canadian comment.</p>	Comment withdrawn during the meeting by the US
5.1.3.2	UK	Need to clarify the word ' <i>technical means</i> ' as it can also include 'mechanical sealing' Suggest changing to ' <i>hardware and software sealing</i> ' as this covers all possible sealing means such as electronic, mechanical, cryptographic, etc. Alternatively you need a terminology to express all possible sealing means.	<p><b>To be discussed</b></p> <p>"Technical means" obviously includes hardware and software sealing (it is specified <i>not only mechanical sealing</i>).</p> <p>The definition of sealing (§3.3.2) has been</p>	The wording "technical means" will be clarified by the Secretariat.

## First meeting of the TC 5/SC 2 – Draft Minutes

Chapter	Country	Comments on and proposals for modifications	Secretariat's Replies	Decided during the meeting (decision)
			improved: <i>To set a special protection to serve as an indicator for the case of unauthorised access to the device's hardware or software part. It can be achieved by hardware, software or a combination of both.</i>	
5.1.3.2	US	Note (a): This requirement implies that technical means, <u>in addition to</u> <del>not only</del> mechanical sealing <del>are</del> <u>may be</u> necessary for measuring instrument having an operating system or an option to load software. When the software is stored on an inviolable memory device (e.g. sealed masked ROM) that <u>the need for</u> technical means are <del>consistently</del> <u>considerably</u> reduced.	<b>To be discussed</b> See above modification proposed to Canada.	The First part of the comment is Accepted Instead of <i>consistently</i> or <i>considerably</i> , <i>accordingly</i> will be utilised in the document.
5.2.3	JP	(1) Our concern is, as the secretariat supposed, the performance problem. The storage device easily comes to its limit if every intermediate measurement data is to be stored. Since the definition of legally relevant data is out of the scope of this document, we agree that our concern above should be considered at the responsible TC, rather than here.	<b>To be discussed</b> Legally relevant data are not out of the scope of the document, the definition of legally relevant data is induced by the definition of legally relevant. The requirement has been split into two different requirements, thus OIML TCs/SCs will have the possibility to select this requirement or not.	Solved, see answer to Canada § 5.2.3.1 below
5.2.3.1	CA	The R 117 reference (3.5.3) has changed in the DR 2 version presented to the CIML for vote. The 3.5.3 section (1995) is now 3.5.4 in DR 2.  The new R 117 3.5.4, now allows for data to be automatically deleted if the transaction is completed, or the data has been printed.	<b>To be discussed</b>	Accepted, 3.5.2, 3.5.3 and 3.5.4 of R 117-1 2007 will be included in the document.
5.1.4.1	CECIP	Cyclically checksum calculation should be an example for raised severity level (II). When is a measurement interruptible and when not?	<b>To be discussed</b> Do you mean that the parity bit is sufficient for the security level (I) or that it is not necessary for the security level (I)?  Interruptible has been added to terminology <i>Interruptible and non-interruptible measuring instrument</i> <i>An interruptible measuring instrument is a measuring</i>	Easily and rapidly will be removed from the definition of interruptible.

## First meeting of the TC 5/SC 2 – Draft Minutes

Chapter	Country	Comments on and proposals for modifications	Secretariat's Replies	Decided during the meeting (decision)
			<i>instrument in which the measurement process can be stopped easily and rapidly (this does not include an emergency stop). In other cases the measuring instrument is considered to be non-interruptible.</i>	
5.2.1.1	NL	In order to avoid misunderstandings, we suggest adding a note to this example: <i>"Note: It must be noted that the text of this example is not applicable to the traditional electronic weighing instruments consisting of one or more analogue (strain gauge) load cell(s) connected to a load cell indicator with analogue input."</i>	<b>To be discussed</b> The requirement deals with the identification of the part of the measuring instrument that performs legally relevant functions. An analog load cell has the same legally relevant function as a digital load cell.	Comment withdrawn during the meeting. Load cell examples will be removed in the whole document and replaced by <i>digital sensor</i> .
5.2.1.2	CECIP	Example c) is not a good workaround for examples a)/b) because the main problem (omitting a call of the legally relevant procedures) is not solved by the suggested solution in c) at all.	<b>To be discussed</b> There seems to be a misunderstanding: Example (c) is not meant as a work-around for (a)/(b). It was intended to show how to realise the priority of the legally relevant task or program over others. Other tasks/programs may have higher priority allotted by the operating system but in this example they cannot process legally relevant data <b>before</b> the relevant program has processed and optionally exported them to other programs.	Comment withdrawn during the meeting
5.2.2	UK	Suggest clarifying the text ' <i>windows based operating system</i> , as this might be taken to mean the Microsoft Windows operating system and not 'indications in multiple windows on the same display, as is intended.	<b>To be discussed</b> windows → window	<i>Multiple windows user interface</i> will be used instead of <i>windows based operating system</i>
5.2.3	CECIP	By introducing any cryptographic methods in requirement c) for high protection and by requiring i.g. RSA 1024 bit key length in the note 9) the technical level and the cost is raised without any profit for security. Because any cryptographic system is absolutely insecure without a complete key management system according to FIPS Pub. 140. But introducing such a key management	<b>To be discussed</b> Cryptographic methods described here are state of the art and at least in	Comment withdrawn during the meeting

## First meeting of the TC 5/SC 2 – Draft Minutes

Chapter	Country	Comments on and proposals for modifications	Secretariat's Replies	Decided during the meeting (decision)
		<p>system would generate cost of approximately a few hundred thousand Euro.</p> <p>Example (a) clock should be accessible without the need of reverification after setting.</p>	<p>some countries they are required in some areas of application in legal metrology.</p> <p><b>To be discussed</b> When the clock of a sub-assembly is utilised for time-stamping, if the clock setting is not considered as legally relevant, it can be very easy to perform a fraud simply by resetting the clock which means to falsify the time-stamp.</p>	<p>The Secretariat answer solves the comments</p>
5.2.6	US	<p>The control of adjustment parameters (calibration) has not been addressed to this point. We would view this as maintenance and should be added to this section.</p>	<p><b>To be discussed</b> The adjustment parameters are individual device specific parameters. In this case requirement 5.1.3.2 applies. The contents of 5.2.6 aims at updating of programs only that are type specific. Possibly the heading should be changed.</p>	<p>The requirement 3.2.3 of OIML R 51-1 2006 will be included in the document. A definition of event logger will be added.</p>
5.2.6.2.5	US	<p>Comment: US requirements recognize physical seals only, a log book is sufficient for those cases. Appropriate <del>technical</del> means, e.g. an audit trail <u>or log book</u>, shall be used to ensure that traced updates of legally relevant software are adequately traceable within the instrument for subsequent verification and surveillance or inspection. This requirement enables inspection authorities, which are responsible for the metrological surveillance of legally controlled instruments, to back-trace traced updates of legally relevant software over an adequate period of time (that depends on national legislation). The audit trail <u>or log book</u> shall contain the following information: success / failure of the update procedure, software identification of the installed version, software identification of the previous installed version, time stamp of the event, identification of the downloading party. An entry is generated for each update attempt regardless of the success. <del>The traceability means and records are part of the legally relevant software and should be protected as such. The software used for displaying the audit trail belongs to the fixed legally relevant software.</del> Comment: Requirements on audit trails should be dealt with in a separate section.</p>	<p><b>To be discussed</b> See answer to your previous comment in 3.2.1</p>	<p>See above (§5.2.6) answer to the US comment. The wording <i>audit trail</i> is kept and <i>event logger</i> is removed to keep the document consistent.</p> <p>Separation of the requirement needed by the inclusion of 3.2.3 of OIML R 51-1:2006.</p>
6.1	USA	<p>An interface may be public (visible to many other modules), trusted (visible to a small group of</p>	<p><b>To be discussed</b></p>	<p>The wording <i>legally relevant</i> is added before <i>interface</i> in</p>



## First meeting of the TC 5/SC 2 – Draft Minutes

Chapter	Country	Comments on and proposals for modifications	Secretariat's Replies	Decided during the meeting (decision)
		specific modules), or private (completely contained within a single module). Is the Secretariat suggesting that all interfaces, even those that cannot be seen from outside a program module, must be documented for Type Approval and potentially tested? Perhaps the words "external" or "public" could be added to the definition of the term "interface" or added to its usage when appropriate, such as in section 6, Type Approval.		the documentation chapter.
6.1.1	USA	An interface may be public (visible to many other modules), trusted (visible to a small group of specific modules), or private (completely contained within a single module). Is the Secretariat suggesting that all interfaces, even those that cannot be seen from outside a program module, must be documented for Type Approval and potentially tested? Perhaps the words "external" or "public" could be added to the definition of the term "interface" or added to its usage when appropriate, such as in section 6, Type Approval.	To be discussed	The wording <i>legally relevant</i> is added before <i>interface</i> in the documentation chapter.
General	US	New Terms:  Embedded software devices (Type P). A device or element with software used in a fixed hardware and software environment that cannot be modified or uploaded via an interface without breaking a security seal or other approved means for providing security,	To be discussed "Embedded software devices" is not used in the document.	Some guidance related to the use of universal computer will be added in chapter 8. This guidance will explain the difference of risks between using a built for purpose measuring instrument and a PC based measuring instrument.
3.2.1	US	Event. An action in which one or more changes are made to configuration parameters or adjustments are made to one value (or values for a set of values) for a calibration parameter (e.g., adjustments for a set of calibration factors to linearize device output), while in the adjustment mode. If no adjustment is made, then there is no event. In the case of a centralized audit trail, the same values for the same parameter sent to multiple devices shall be considered to be the same event. In the case of a centralized event logger, the event logger must identify both the device and the parameter that was changed.  Event counter. A nonresettable counter that increments once each time the mode that permits changes to sealable parameters is entered and one or more changes are made to sealable calibration or configuration parameters of a device.  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.	To be discussed Redundant with the definition of audit trail; this is a requirement and not a definition.  To be discussed Not used in the document. Example for a technical solution.  To be discussed Not used in the document. Example for a technical solution.	Add the definition of an event, event counter and modify examples to include event counter.  The wording <i>event counter</i> will be included in the example, the definition of an <i>event</i> and an <i>event counter</i> will be added to the terminology.

## First meeting of the TC 5/SC 2 – Draft Minutes

## 6) Additional comments discussed during the meeting:

Country	Chapter	Comments	Answers
UKmf	General	There are references to IEC standards eg in 6.3.2 and to others documents but there is no section on Reference	This chapter is already included in the document (Bibliography chapter). Will be updated.
UKmf	Explanatory notes	Insert in last line "(as interpreted in a practical sense by Welmec). Welmec Guide 7.2 is actually an interpretation of the MID software requirements by Welmec – it may be possible to comply with th MID's essential requirements in others ways	You are right. The explanatory notes will be deleted in the final document.
UKmf	Foreword	Clarify. The acronym CIML is not explained	Accepted, will be replaced by International Committee of Legal Metrology (CIML)
UKmf	1	Clarify or delete. The meaning of this is not understood – the CD does not seem to actually give guidance on implementing OIML recommendations	Answer to previous comments will clarify the situation. This OIML Document is composed of several sets of requirement that OIML TC/SCs shall select when drawing up an OIML Recommendation. For each proposed software requirement, TC/SCs have to select the appropriate severity level bearing in mind the guidance provided by the chapter 8.
UKmf	Terminology	Expand This is says that definitions of the VIM are used but the definitions of D 11 and ISO/IEC are also used and should be mentioned	Accepted
UKmf	Terminology	Put in alphabetical order Definition in 3.2 and 3.3 are in alphabetical order- those in 3.1 are not	Accepted, see below answer to Canada
UKmf	Terminology	Fault An event or phenomena which causes the error of indication to differ from the initially measured intrinsic error, usually to increase it. It may be expressed as a numerical value... The definition as written is a peculiar way to define a fault as it only refers to faults which affect accuracy – if the fault causes the	Considered. The current definition of fault comes from the D 11. Failure will be addressed in the event definition. Usually, system failure are not considered as fault because they are supposed being

## First meeting of the TC 5/SC 2 – Draft Minutes

Country	Chapter	Comments	Answers
		instrument to cease working then the error is infinite. This concept is not actually used anywhere in the document – 5.1.4.1 refers to fault detection but the meaning is clear without the need of definition.	obvious.
UKmf	Terminology	Revise style Use of “it” or “to” differs in style from other definitions	Accepted
UKmf	Terminology 3.2.9 3.2.22 3.3.2 3.3.3	Software should be define in the document	Accepted a definition based on relevant IEC standards will be added in the terminology chapter of the document
UKmf	3.2.12 footnote 3	Revise Not good English	
CA	Terminology	Sort the terminology in alphabetical order	Accepted, the French version of the document will have its terminology unsorted in order to keep the numbering identical for both versions. Furthermore an index will be added at the end of the document.
CECOD	3.2	I am missing in the chapter 3.2 Software terminology an explanation for the designation “Firmware”.  “Software” is able to run on different hardware platforms like universal computers (general purpose, U device) Firmware is a subgroup of the “Software” and is special designed to run only on special designed hardware (built for purpose, P device).	It is not necessary to define firmware since the document does not dissociate firmware from other software.
UKmf	3.4	Correct IEC=International Electrotechnical Commission	Accepted
UKmf	3.4	Review?	Accepted

## First meeting of the TC 5/SC 2 – Draft Minutes

Country	Chapter	Comments	Answers
		"Not applicable" is more commonly written as "n/a" not N.A.	
UK	5.1.1	Delete the word sub assembly in the document	The use of device/electronic device/sub-assembly will be checked in the whole document to improve its consistency
CECOD	5.1.1	In some cases it is not possible to get direct access to the firmware version of a programmable device. Some reasons could be that there is neither a display nor a communication port where the firmware version could be read out or the communication port is only for factory set up and afterwards the port will be sealed. Other reasons could be that the device is installed in a hazardous area where it is not possible to get easy access to a communication port. Such devices are not foreseen according this document	Comment withdrawn during the meeting
CECOD	5.1.2	<p>Software protection Example (II) If a rewritable device is used, the <b>write-enable input is inhibited by a switch that can be sealed.</b></p> <p>Parameter protection Example (c): Device specific parameters to be secured are stored in a non-volatile memory. <b>Its write-enable input is inhibited by a switch</b> that can be sealed or may be software controlled.</p> <p>The red marked text has to be rewritten. The write-enable input of a device is very sensitive and should never go through the whole device. In some cases it is impossible to do so because of explosion proof protection. It must be possible to have a complete SW controlled solution for firmware updates or to protect the parameter. Mechanical switches are in some cases not possible because of environmental conditions or durability conditions. A switch is every time a weak point in the hardware construction</p>	This is just an example. Obviously other solutions that fulfill the requirement exist.
UKmf	5.1.2	<p>Clarify</p> <p>This has a different style from other sections (no "Purpose" or</p>	<p>Accepted</p> <p>Style will be modified according to the rest of</p>

## First meeting of the TC 5/SC 2 – Draft Minutes

Country	Chapter	Comments	Answers
		"Example". Is this intentional?	the document.
UKmf	5.1.3.2	Insert There is a footnote number in Example (a) but there is no footnote	Accepted The footnote number will be removed.
CECOD	5.1.3.2	Example (d-1), page 15 The initial value of the counter has been <b>imprinted on the plate of the instrument at</b> legal verification.  This is very restrict and in some cases not possible. It should also be possible to use other solutions, i.e. to make a print out. This print out of the number will be stamped by the W&M officer. This paper belongs to the other official paper of the system	Comment withdrawn during the meeting
DK	5.2.1.2	Last paragraph: It is a too strict restriction to put on severity level II that software separation is not to be used. It will cause that it will be nearly impossible to get severity level II included in any Recommendation.	The software separation alone is not sufficient for an increased security level. Additional guidance will be added.
CECOD	5.2.3	Requirement c) footnotes 6 and 7 Please add: or equivalent to 6) and 7).  In some cases an algorithms is not useful because of lack of memory or lack of processor speed. This is the case especially in embedded systems.	Accepted <i>or equivalent</i> will be added in the footnotes
CA	5.2.6	Inoperable instead of hibernate	Accepted
US	5.2.6.1	Add a reference to 5.2.6 in the flow chart of the verified update to remind that verification belongs to national regulation	Accepted
CECOD	5.2.6.1	A person responsible for verification must be on the installation site of the measuring instrument.  For what reason? I don't understand this sentence.	Withdrawn during the meeting, see answer to the US above (§5.2.6.1).
CECOD	5.2.6.2.4	If the loaded software fails the test, the instrument shall discard it and use the previous version of the software  I am missing the red signed text below as used in 5.2.6.2.3. If the loaded software fails the test, the instrument shall discard it	Accepted.  5.2.6.2.3 will be enhanced (with a suitable reference in 5.2.6.2.4): ... <i>or switch to an inoperable mode. In this mode measuring</i>

## First meeting of the TC 5/SC 2 – Draft Minutes

Country	Chapter	Comments	Answers
		and use the previous version of the software <b>or switch to a hibernating mode</b>	<i>functions shall be inhibited. It shall only be possible to resume the download procedure, without omitting any step in the flow diagram for Traced Update.</i>
CECOD	5.2.6.2.4	<b>hibernating mode</b> It should be possible to start a new download in the hibernating mode. This could be the case of a power failure during the download or a bad transmission line that the download has failed and must be repeated	Not addressed during the meeting It is already included in the <i>traced update</i> process. It is assumed that integrity or authenticity will be altered in case of power failure thus, the process restart with the item request for update.
UKmf	6.2 and 6.3.1	As previously indicated the standards quoted should appear in a "Reference" section.	Accepted, see answer to your comment above (§General)
UKmf	6.3.2.1 References	There is a reference to chapter 0. There is no chapter 0	Accepted, in fact it is the chapter 5.
UKmf	6.3.2.1 References	Clarify What is FDA	FDA= Food and Drug Administration
UKmf	8.2 (d)	Clarify The meaning of this is obscure. How does it impinge on risk	Accepted
UKmf	Annex D Test Report	Revise style All the text should be in italic for consistent style	Accepted
CECOD	Annex D Test Report	Is it possible to get also a test certificate? How will be handled SW changes after issuing the test report?	It is currently under consideration. TC 5/SC 2 provides the materials in order that TCs have the possibility to decide on that matter.

## 7) Any other business

The TC 5/SC 2 Secretariat proposes a new work item to consider: How to check software conformity in the field?

Several Members are interested in such a work; the Secretariat proposes to draw up a draft proposal for this new work item. This draft proposal will be circulated within TC 5 /SC 2 before any formal proposal to the CIML.

## ANNEX

Paul Kok, NMI, proposal 5.1.1:

*Requirement:*

Legally relevant software of measuring instrument/sub-assembly shall be clearly identified with the software version or another token. The identification may consist of more than one part but one part shall be only dedicated for the legal purpose.

The identification shall be inextricably linked to the software itself and shall be presented or printed on command or displayed during operation. If a sub-assembly has neither display nor printer, the identification shall be sent via communication interface in order to be displayed/printed on another sub-assembly or on the instrument.

As an exception for non-interruptible measurements an imprint of the software identification on the nameplate of an instrument shall be an acceptable solution under the following circumstances:

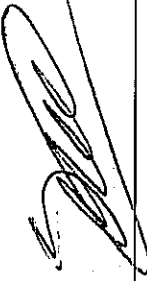
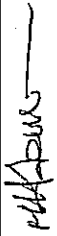

- A. The user interface does not have any control capability to activate the indication of the software identification on the display or the display does not allow technically showing the identification of the software (mechanical counter).
- B. The instrument does not have an interface to communicate the software identification.
- C. After production of the instrument a change of the software is not possible or only possible, if also the hardware or a hardware component is changed.

The manufacturer of the hardware or the concerned hardware component is responsible, that the software identification is correctly marked on the concerned hardware.

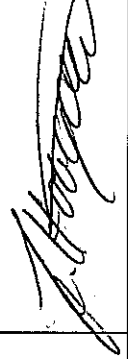


Meeting  
**OIML TC5/SC2 „Software“**  
 13/14 December 2007, Berlin

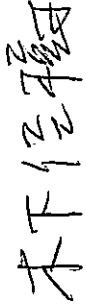
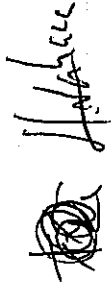

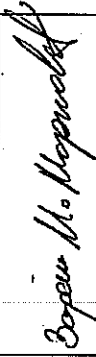



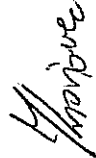
*Participants*




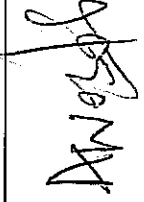
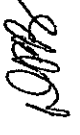
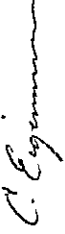

(so far registered by 11 December 2007)


Firstname	Surname	Institute/Company	Email Address	Country	Signature
1. Maxim	Shabanov	BELARUSIAN STATE INSTITUTE OF METROLOGY (BelGIM)	<a href="mailto:metrol@belgim.by">metrol@belgim.by</a>	Belarus	
2. Nebojsa	Jandric	Institute of Metrology of BiH	<a href="mailto:Nebojsa.jandric@met.gov.ba">Nebojsa.jandric@met.gov.ba</a>	Bosnia and Herzegovina	<i>Present at the first day.</i>
3. Zijad	Dzemic	Institute of Metrology of BiH	<a href="mailto:Zijad.dzemic@met.gov.ba">Zijad.dzemic@met.gov.ba</a>	Bosnia and Herzegovina	<i>Present at the first day.</i>
4. Esad	Tuzovic	Institute of Metrology of BiH	<a href="mailto:Esad.tuzovic@met.gov.ba">Esad.tuzovic@met.gov.ba</a>	Bosnia and Herzegovina	<i>Present at the first day.</i>
5. Marcos J. H.	Senna	INMETRO	<a href="mailto:senna@inmetro.rs.gov.br">senna@inmetro.rs.gov.br</a>	Brazil	
6. Dennis	Beattie	Measurement Canada	<a href="mailto:beattie.dennis@ic.gc.ca">beattie.dennis@ic.gc.ca</a>	Canada	




7.	Petr	Klapetek	CMI		<a href="mailto:pklapetek@cmi.cz">pklapetek@cmi.cz</a>	Czech Republic	<i>Present at the first day.</i>
8.	Jens	Hovgård	DELTA Acoustics & Electronics		<a href="mailto:jhj@delta.dk">jhj@delta.dk</a>	Denmark	
9.	Tuomo	Valkeapää	TUKES		<a href="mailto:tuomo.valkeapaa@tukes.fi">tuomo.valkeapaa@tukes.fi</a>	Finnland	
10.	Samuel	Just	OIML		<a href="mailto:samuel.just@oiml.org">samuel.just@oiml.org</a>	<del>France</del>	
11.	Dieter	Richter	Physikalisch-Technische Bundesanstalt (PTB)		<a href="mailto:Dieter.richter@ptb.de">Dieter.richter@ptb.de</a>	Germany	
12.	Ulrich	Grottker	Physikalisch-Technische Bundesanstalt (PTB)		<a href="mailto:Ulrich.grottker@ptb.de">Ulrich.grottker@ptb.de</a>	Germany	<i>Grottker</i>
13.	Reiner	Letsch	Mettler-Toledo (Albstadt) GmbH		<a href="mailto:reiner.letsch@mt.com">reiner.letsch@mt.com</a>	Germany	<i>Present at the first day.</i>
14.	Heike	Wippich	PTB Physikalisch-Technische Bundesanstalt (PTB)		<a href="mailto:heike.wippich@ptb.de">heike.wippich@ptb.de</a>	Germany	<i>Wippich</i>
15.	Satoshi	Matsuoka	NMIJ		<a href="mailto:matsuoka@ni.aist.go.jp">matsuoka@ni.aist.go.jp</a>	Japan	<i>松岡聡</i>

16.	Yoshiki	Kinoshita	National Institute of Advanced Industrial Science and Technology (AIST)	yoshiki@m.aist.go.jp	Japan	
17.	Hideki	Nahara	ISHIDA CO., LTD.	nahara@ishida.co.jp	Japan	
18.	Yoshio	Kitano	Teraoka Seiko Co., Ltd.	Yoshio kitano@aist.go.jp	Japan	<i>Present at the first day.</i>
19.	Paul	Kok	NMI Certin	pkok@nmi.nl	Netherlands	
20.	Zoran M	Markovic.	Directorate of Measures and Precious Metals	zoran.markovic@szmdm.s v.gov.yu	Serbia	
21.	Tomáš	Terifaj	Slovak legal metrology, n.o.	terifaj@slm.sk	Slovak Republic	
22.	Eduard	Gombala	Slovak legal metrology, n.o., Slovakia	gombala@slm.sk	Slovak Republic	
23.	Aleksander	Premuš	Metrology Institute of the Republic of Slovenia	Aleksander.Premus@gov. si	Slovenia	
24.	Damjan	Krašovec	Metrology Institute of the Republic of Slovenia	DAMJAN.KRASOVEC@GOV.SI	Slovenia	

25.	Bulelani	Maqekeni	SABS		<a href="mailto:magekebb@sabs.co.za">magekebb@sabs.co.za</a>	South Africa	
26.	Walter	Madima	SABS		<a href="mailto:madimawz@sabs.co.za">madimawz@sabs.co.za</a>	South Africa	
27.	Thomas	Krebs	METAS		<a href="mailto:thomas.krebs@metas.ch">thomas.krebs@metas.ch</a>	Switzerland	
28.	Morayo	Awosola	NWML		<a href="mailto:Morayo.awosola@nwml.gov.uk">Morayo.awosola@nwml.gov.uk</a>	United Kingdom	
29.	Doug	Bliss	Mettler Toledo		<a href="mailto:doug.bliss@mt.com">doug.bliss@mt.com</a>	USA	
30.	Cassie	Eigenmann	DICKEY-john Corporation		<a href="mailto:ceigenmann@dickey-john.com">ceigenmann@dickey-john.com</a>	USA	
31.	Ambler	Thompson	NIST		<a href="mailto:ambler@nist.gov">ambler@nist.gov</a>	USA	

32. Michael FREISINGER BEV - AUSTRIA [michael.freisinger@bev.gv.at](mailto:michael.freisinger@bev.gv.at) AUSTRIA 

33. Günther TREUBAUER BEV - AUSTRIA [guenther.treubauer@bev.gv.at](mailto:guenther.treubauer@bev.gv.at) AUSTRIA 

34. JAMES PETTINARO FMC TECHNOLOGIES [jim.pettinaro@fmc.ti.com](mailto:jim.pettinaro@fmc.ti.com) USA