National Type Evaluation Technical Committee (NTETC)
Software Sector Meeting
October 17 & 18, 2007
Little Rock, AK

Agenda Items

Carryover Items **Page**

New Items

CARRYOVER ITEMS

1.a. NTETC Software Sector Mission No new discussion required

Source: NCWM Board of Directors

Background: In 2005 the Board of Directors established a National Type Evaluation Technical Committee (NTETC) Software Sector. A mission statement for the sector was developed at that time.

Mission of the Software Sector:

- Develop a clear understanding of the use of software in today's weighing and measuring instruments.
- Develop NIST Handbook 44 specifications and requirements, as needed, for software incorporated into weighing and measuring devices. This may include tools for field verification, security requirements, identification, etc.
- Develop NCWM Publication 14 checklist criteria, as needed, for the evaluation of software incorporated into weighing and measuring devices, including marking, security, metrologically significant functions, etc.
- Assist in the development of training guidelines for W&M officials in verifying software as compliant to applicable requirements and traceable to a NTEP Certificate. Training aids to educate manufacturers, designers, service technicians and end users may also be considered.

From previous meeting:

Discussion: The Chair asked the question: Is the sector comfortable with the Mission Statement?

The sector discussed the process of other NTETC sectors, the NCWM structure and how/why, the software sector was developed. After some lengthy discussion by the sector, there was consensus among the Sector Members that the Mission Statement is correct. However, the sector noted that there is a very broad range of items listed in the Statement. The sector agreed that the steps in the Mission Statement are correct. The steps appear to build on each other in an orderly progression. It was further agreed that whenever possible items will be addressed in the sequence of the Mission Statement.

The Chair noted that the scope of this sector is somewhat broader than some other sectors. The work of this sector is more closely aligned to that of the Grain Analyzer Sector in that focus is on development of possible language for:

- NIST Handbook 44,
- checklist criteria for NCWM Publication 14, and
- appropriate field guidelines.

1.b. NCWM/NTEP Policies – Issuing CCs for Software No New Discussion Required

Source: NCWM Reports

Background: Excerpts of reports from the 1995-1998 Executive Committee were provided to NTETC Software Sector members at their April 2006 meeting. The chair asked the sector to review the following NTEP policy decision adopted by the NCWM in 1998 relative to the issuance of a separate Certificate of Conformance (CC) for software.

> The NCWM has struggled with software issues for many years. Prior to 1995, NTEP had evaluated stand alone software (e.g.: weigh-in / weigh-out, POS, and batch controller software) and, in some cases, had issued CCs for stand alone software. The Board established a software work group to study the issues and make recommendations.
>
> Many issues were discussed by the work group, including: first indication of the final quantity, metrologically significant software, definitions, software marking, software checklist evaluation, a software EPO for the field inspector, user programmable software, and third party software. According to conference reports, it seems in 1997 some concerns were raised about the direction of the work group. In 1997, after the annual meeting, a new Software Work Group was appointed by the NCWM chair.
>
> **During the 1998 NCWM, the following recommendation was adopted as NTEP policy:**
>
> - **"Software, regardless of its form, shall not be subject to evaluation for the purpose of receiving a separate, software Certificate of Conformance from the National Type Evaluation Program."**
> - **"Remove all of the software categories from the index of NCWM Publication 5, NTEP Index of Device Evaluations."**
> - **"Reclassify all existing software CCs according to their applicable device categories."**

The policy is still in effect today.

Also noteworthy is a statement in Section C of NCWM Publication 14, Administrative Policy. It states: "In general, type evaluations will be conducted on all equipment that affect the measurement process or the validity of the transaction (e.g. electronic cash registers interfaced with scales and service station consoles interfaced with retail fuel dispensers); and all equipment to the point of the first indicated or recorded representation of the final quantity on which the transaction will be based."

Discussion: At this point in time, NTEP evaluates a "software-based device" as a functional device. The performance of the device is evaluated.

There was a suggestion from the floor that the 1998 policy be amended. If this is done, then the sector can move toward the other steps in the process.

Discussion from the floor is on how to or if there needs to be a change to the device type in the FOR box.

The consensus of the sector is that the current NCWM/NTEP policy should be changed.

From previous meeting:

Software Requiring a Separate CC: Software which is implemented as an add-on to other NTEP Certified main elements to create a weighing or measuring system and its metrological functions are significant in determining the first indication of the final quantity. Such software is considered to be a main element of the system requiring a separate CC.

NOTE: OEM software ***may*** be added to an existing CC or have a stand-alone CC with applicable applications (e.g., a manufacturer adding a software upgrade to their ECR or point-of-sale system, vehicle scale weigh-in/weigh-out software added as a feature to an indicating element, automatic bulk weighing, liquid-measuring device loading racks, etc.) and minimum system requirements for “type P” devices (see proposed software definition below). It may be possible for a manufacturer to submit a single application for both hardware and software contained in the same device. A single CC would be issued.

In this instance, OEM refers to a 3rd party. The request to add software could be made by the original CC holder on behalf of the 3rd party. Alternatively, a new CC could be created that refers to the original CC and simply lists the new portions that were examined.

The sector recommendation will be submitted to the NTEP Committee.

Current Note: This item has not yet been submitted to the NTEP Committee for review. It is planned for this to happen during the NCWM Interim Meeting in January 2008.

2. Definitions for Software-Based Devices (Leave this one on and get to Regions and Sectors)

Source: NTETC Software Sector

Background: Discussed was marking and G-S.1.1. It was initially suggested that "not built-for-purpose" be removed from the wording in NIST HB 44 G-S.1.1. However, after further discussion this may not be the correct or final decision. There is no definition for a not built-for-purpose device in HB 44. The current HB 44 definition for a built-for-purpose device reads:

Built-for-purpose device. Any main device or element which was manufactured with the intent that it be used as, or part of, a weighing or measuring device or system. [1.10] (Added 2003)

There was also the suggestion to use the definitions from the WELMEC document for Type P and Type U instruments. They were modified by the sector. It was also suggested that a list of examples be provided.

Draft definitions for consideration:

Built-for-purpose weighing or measuring instrument (device) (type P): A weighing or *measuring Instrument (device)* designed and built specially for the task in-hand. Accordingly the embedded software is assumed to be designed for the specific task. It may contain many components also used in PCs, e.g. motherboard, memory card, etc.

A weighing or measuring instrument (device) using a universal Computer (type U): *A weighing or measuring Instrument (device)* that uses a general-purpose computer, usually a PC-based system, for performing legally relevant functions.

Examples:
Type U
Weigh-in Weigh-out
Open Architecture

Discussion: The sector agrees that the NTEP CC should reflect "software" is a separate main element. If this is true then there needs to be definition.

The Sector agrees that this change in policy and appearance on CC’s does not have a major impact on our current type evaluation process.

MC, sites three main areas of : sensing physical phenomena (mass or volume), computational, controlling the system.

After a lengthy discussion related to the terms "built-for-purpose and "not-built-for-purpose", the sector agreed that these terms were not clear and should be replaced with the terminology proposed below.

A main reference point that the sector used in this discussion was OIML R76 *Non-automatic weighing instruments* sub-sections 5.5.1. (Type P) and 5.5.2. (Type U).

(*New Definition)* **Electronic devices, software-based**. Weighing and measuring devices or systems that use metrological software to facilitate compliance with Handbook 44. This includes:

(a) **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 any interface without breaking a security seal or other approved means for providing security, and will be called a "P", or

(b) **Programmable or loadable metrological software devices (Type U).** A personal computer or other device and/or element with PC components with programmable or loadable metrological software, and will be called "U". A "U" is assumed if the conditions for embedded software devices are not met.

From Previous meeting: Conclusion and Recommendation: The above proposed definition was agreed upon to move towards submitting to the S&T. This change would clarify and define what we currently do in NTEP and represent it properly in NIST HB44 to assist the inspector.

Current Comment: The Sector is asked to review this item and be certain that they still agree.

3. Software Identification / Markings (Leave in)

Source: NTETC Software Sector

Background: At the last meeting there was discussion on specific sections of the WELMEC document that deal with TYPE P and TYPE U requirements. The comments and recommendations under consideration are contained in the following.

Discussion: There was lengthy discussion on the value and merits of markings. This included the possible differences in some types of devices and marking requirements. After hearing several proposals the sector agreed to the following recommendation.

Technical changes represented below:
1. CC No. must be continuously displayed or marked,
2. Version must be software generated, not hard marked,
3. Version required for embedded (Type P),
4. Print option Created
5. Command or operator action option created,
6. Type P must display or hard mark make, model, S.N.

Recommendation:

TYPE U Shall meet one of the methods:

Method	NTEP CC No.	Make/Model	Software Version/Revision
Hard-Marked	X[1,2]	X	Not Acceptable
Continuously Displayed	X[2]	X	X
Via Menu (display) or Print Option	Not Acceptable	X	X

[1] – Only if no means of displaying this information is available
[2] – Information on how to obtain the remaining items (Make/Model, Version/Revision) shall be included on the C of C.

TYPE P Shall meet one of the methods

Method	NTEP CC No.	Make/Model/Serial No.	Software Version/Revision
Hard-Marked	X	X	Not Acceptable
Continuously Displayed	X	X	X
By command or operator action	Not Acceptable	Not Acceptable	X

Note: Information on how to obtain the remaining items (Make/Model, Version/Revision) shall be included on the C of C.

The "Via Menu (display) or Print option" may be supplemental for devices that use the hard-marked or continuously displayed identification method for the NTEP CC Make/Model, Serial No. information.

From Previous Meeting: The sector will forward these items, when completed, to the Regional S&T committees for consideration.

Current Comment: Sector is asked to complete the work on this item.

4. Identification of Unapproved/Unauthorized Software (Need to have Sector work out)

Source: NTETC Software Sector

Background: During the last meeting much discussion was generated. Many comments were addressed.

Segregation of parameters is currently allowed. (see table of sealable parameters)

Right now there are two methods, physical seal, audit trail, does the sector believe that there needs to be some other category?

Currently, industry does protect software, but it is not audit trail.
There is an issue of audit trail, if the software is not running, or have a software service, the changes could be made and not tracked by audit trail.

There is no way to tell someone how to do sealing, you can say what needs to be accomplished.

Examples of methods of sealing.
authentication
access control
X509 Certificates,
PCATS certifies vendors
Version Number, application (checksum) There is a challenge response with different certifications. They validate who they are, there may also be limits set. receive data verification

The sector was in general agreement that HB 44 does not need to be changed.

The sector agreed that W&M needs to know that software is not being manipulated,

X509 is a standard for a public key infrastructure (PKI). This is a system where a third party holds the key to decode an encrypted program, to ensure no one messes with it

Scale System Controller
The scale system controller has approval certifications for USA and the European Union. In this case, a Commercial Off The Shelf (COTS) PC is used in conjunction with a scale system (terminal and weigh platform). The scale system provides the PC with approved gross weight and accepts commands to zero the weight indication. The PC application program

- stores and recalls weights
- computes net weight using a stored weight or manually entered weight
- provides the user display of net weight
- may compute price based on the net weight and a selected commodity code
- may print a weigh ticket

Protection of configuration and price parameters
Metrologically significant parameters are maintained within the scale terminal and are controlled there. Other parameters are stored in a password protected database. The user controls password protection access and distribution.

Separation of software
Separation of metrological and application software as described in the WELMEC documents is maintained.

Protection of software
Metrologically significant software is supplied only as binary code. Each such module is protected by a CRC32 checksum. The expected checksums, revision levels, and dates are kept in an encrypted configuration file. If run-time values differ from expected values the system will not operate. The configuration information can be recalled by an inspector using the Help/About menu in the application program.

Protection of active data
Data from the scale terminal is wholly owned by the scale server metrological interface. No other agent can acquire that data when the scale server is running, and the application program will not accept data except from the scale server.
Transactional information is stored in an encrypted Alibi Memory log. No access is permitted to this data except via the supplied application program. Data can be exported via the application program for external use, but no user modifications are permitted to the original transaction data.

Protection of operating system user interface
There are no special restrictions to the operating system. The application program runs as any other on the PC and can be started, stopped, or minimized.

In Europe, there are things like, safety, highest level security etc. First modification there would be a limit to the risk classes.

P5: Protection against accidental or unintentional changes
Legally relevant software and measurement data shall be protected against accidental or unintentional changes.

Specifying Notes:
Possible reasons for accidental changes and faults are: unpredictable physical influences, effects caused by user functions and residual defects of the software even though state of the art of development techniques have been applied.

This requirement includes:
a) Physical influences: Stored measurement data shall be protected against corruption or deletion when a fault occurs or, alternatively, the fault shall be detectable.
b) User functions: Confirmation shall be demanded before deleting or changing data.
c) Software defects: Appropriate measures shall be taken to protect data from unintentional changes that could occur through incorrect program design or programming errors, e.g. plausibility checks.

Required Documentation:
The documentation should show the measures that have been taken to protect the software and data against unintentional changes.

Validation Guidance: Typical Examples

Checks based on documentation:
□ Check that a checksum of the program code and the relevant parameters is generated and verified automatically.
□ Check that overwriting of data cannot occur before the end of the data storage period that is foreseen and documented by the manufacturer.
□ Check that a warning is issued to the user if he is about to delete measurement data files.
Functional checks:
□ Check by practical spot checks that before deleting measurement data a warning is given, if deleting is possible at all.

Example of an Acceptable Solution:
□ The accidental modification of software and measurement data may be checked by calculating a checksum over the relevant parts, comparing it with the nominal value and stopping if anything has been modified.
□ Measurement data are not deleted without prior authorization, e.g. a dialogue statement or window asking for confirmation of deletion.
□ For fault detection see also Extension I.

Discussion: At this point around the room there was a great deal of discussion. It was pointed out, that it would be difficult, if not impossible for the NTEP evaluated software to identify if unauthorized software was "added" to the device. It is not possible to identify all unapproved software (e.g. add on software, pirated software).

There was general agreement that this may be a field enforcement issue and that it was not appropriate to continue discussion on this item at this time.

From Previous Meeting:

Recommendation: The sector recommended moving this item under agenda item 7, as a sub-item, for discussion at a future meeting.

5. Software Protection / Security (Need input from Jim P)

Source: NTETC Software Sector

Background:

Discussion: The discussion from the last meeting on this issue is mingled in item 4. Appropriate sections need to be pulled out by the sector.

The sector reviewed the applicable items, line by line in the MID Software Work Package 2 and the OIML TC9/SC1 R-76-1 Draft Recommendation to determine items appropriate for the evaluation checklist.

Recommendation: Jim Pettinato from FMC Technologies, agreed to pull together additional information regarding the checklists that we have just developed for this section.

6. Software Maintenance and Reconfiguration (Sector needs to work out)

Source: NTETC Software Sector

Background: After discussion during the 10/06 meeting, it appeared these issues may go beyond the scope of current NTEP procedures, and possibly NTEP resources. The question was asked, does the sector need to address this issue? There was a split vote, no consensus, so it remains on the agenda.

OIML D-SW 5.2.6. was discussed. Comments included:

Only versions of legally relevant software that conform with the approved type are allowed for use (see OIML D-SW 5.2.5). Applicability of the following requirements depends on the kind of instrument and is to be worked out in the relevant OIML Recommendation.

It may differ also on the kind of instrument under consideration. The following options OIML D-SW 5.2.6.1 and 5.2.6.2 are equivalent alternatives. This issue concerns verification in the field. Refer to OIML D-SW chapter 7 for additional constraints.

Discussion points and questions:

This appears to be covered by Cat 3 and enforcement.
This may appear to be covered by other sections or security.
This section should not include eproms.
Is there a security key?
Does it download correctly?
OIML says that the audit trail needs to be updated.

The following flow chart, developed to assist the manufacturer/designer was discussed in depth.

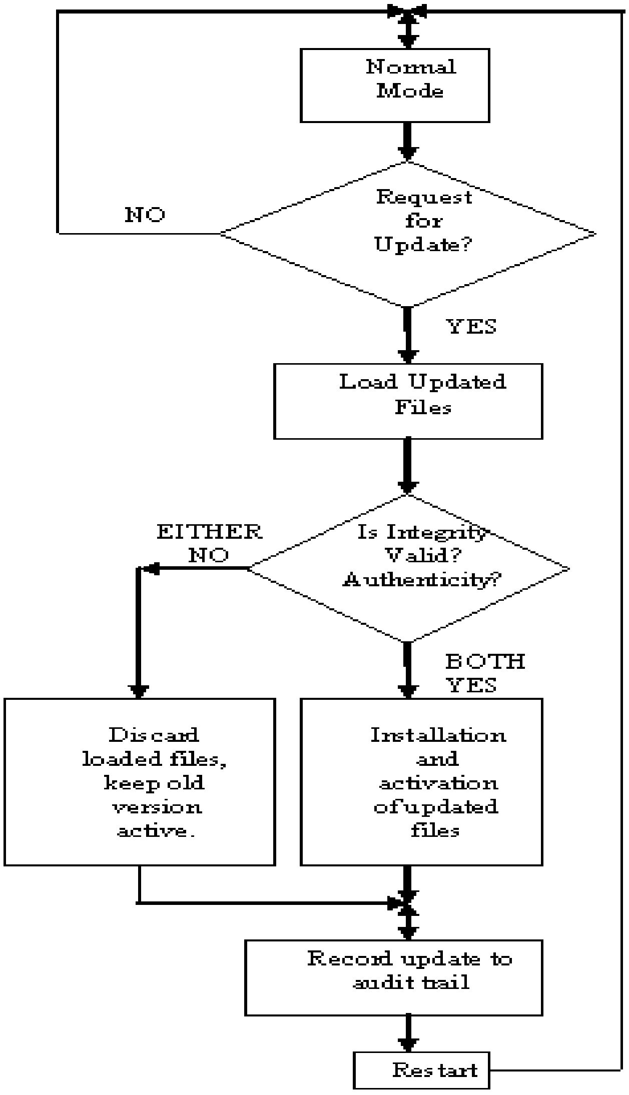
Normal Mode
Request for Update?
NO
YES
Load Updated Files
Is Integrity Valid? Authenticity?
EITHER NO
BOTH YES
Discard loaded files, keep old version active.
Installation and activation of updated files
Record update to audit trail
Restart

Figure 1.0 Traced Update Requirements

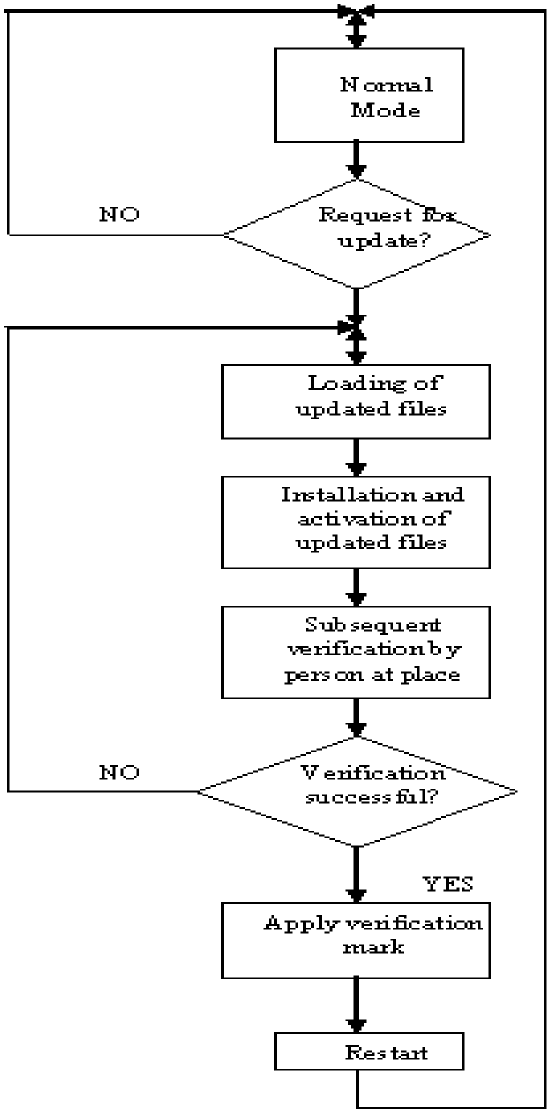

Figure 2.0 Verified Update Model

10/06 Conclusion: *It is apparent a lot more study and understanding of these complex issues are necessary. More discussion will need to take place during the next meeting. Sector members are encouraged to submit specific proposals for consideration.*

Discussion: Traced update provides the ability to update the software either remotely or with equipment that is not part of the device, Category 3 Method of Sealing, it is in line with current technology. It is a feature that currently is being asked for.

From Previous Meeting:

Recommendation: After lengthy discussion on this item the sector came to general consensus that the information in the recommendation below should be considered for further developing type evaluation checklists and field test procedures. It was pointed out that these isses are relevant to agenda item 8, the NTEP application.

Current Comment: Time to work out the final details on this item.

Traced means audit trail record - requires Category 3 audit trail.

Verified means evaluator verified - requires breaking a seal and placing back into service by registered agent or W&M official. D-SW requires agent to be present to verify the update. It was noted that in some jurisdiction, this role may be performed by a registered service agent.

There was discussion on procedures for verifying the versions of software and it was discussed that these procedures should be part of the NTEP CC.

The sector will continue to develop this area.

This section taken from Document OIML D-SW Working Draft 1 WD

5.2.5 Conformity of production-line devices with the approved type

Requirement: The manufacturer shall produce devices and the legally relevant *(is this term correct?? sap)* software that conform to the approved type and the documentation submitted. There are different levels of conformity demands:

(a) identity of the *legally relevant functions* described in the documentation (6.1) of each device with those of the type (the executable code may differ),

(b) identity of *parts of the legally relevant source code*, and the rest of the legally relevant software complying with (a),

(c) identity of the *whole legally relevant source code*, and

(d) identity of the *whole executable code*.

It has to be defined for each kind of instrument or area of application by the responsible TCs which degree of conformity is suitable. The TCs could define a subset from these conformity degrees for a particular kind of instrument and leave the decision what degree of conformity is to be applied to the approving body.

Except for (d) there may be a software part with no conformity requirements, if it is separated from the legally relevant part according to.5.2.1.2.

Means described in 5.1.1 and 5.2.1 shall be provided to make the conformity evident.

5.2.6. Maintenance and re-configuration

Requirement: Only versions of legally relevant software that conform with the approved type are allowed for use (see 5.2.5). Applicability of the following requirements depends on the kind of instrument and is to be worked out in the relevant OIML Recommendation. It may differ also on the kind of instrument under consideration. The following options 5.2.6.1 and 5.2.6.2 are equivalent alternatives. This issue concerns verification in the field. Refer to chapter 7 for additional constraints.

5.2.6.1 Verified update

The software to be updated can be loaded locally ie. directly on the measuring device or remotely via a network. Loading and installation may be two different steps (as shown in Fig. 5-1) or combined to one, depending on the needs of the technical solution. After update of the legally relevant software of a measuring instrument (exchange with another approved version or re-installation) the measuring instrument is not allowed to be used for legal purposes before a (subsequent) verification of the instrument as described in chapter 7 has been performed and the securing means have been renewed (if not otherwise stated in the relevant OIML Recommendation or in the approval certificate). A person responsible for verification must be at place.

5.2.6.2 Traced update

The software is implemented into the instrument according to the requirements for traced update (**5.2.6.2.1** to **5.2.6.2.6**) if it is in compliance with the relevant OIML Recommendation. Traced update is the procedure of changing software in a verified instrument or device after which the subsequent verification by a responsible person at place is not necessary. The software to be updated can be loaded locally ie. directly on the measuring device or remotely via a network. The software update is recorded in an audit trail (see **5.2.6.2.5**). The procedure of a traced update comprises several steps: loading, integrity checking, checking of the origin (authentication), installation, logging and activation.

5.2.6.2.1 Traced update of software shall be automatic. On completion of the update procedure the software protection environment shall be at the same level as required by the type approval.

5.2.6.2.2 The target measuring instrument (device, sub-assembly) shall have a fixed legally relevant software that cannot be updated and that contains all of the checking functions necessary for fulfilling traced update requirements.

5.2.6.2.3 Technical means shall be employed to guarantee the authenticity of the loaded software ie. that it originates from the owner of the type approval certificate. This can be accomplished eg. by cryptographic means like signing. The signature is checked during loading. If the loaded software fails this test, the instrument shall discard it and use the previous version of the software **or become inoperative**.

5.2.6.2.4 Technical means shall be employed to guarantee the integrity of the loaded software ie. that it has not been inadmissibly changed before loading. This can be accomplished by adding a checksum or hash code of the loaded software and verifying it during the loading procedure. If the loaded software fails this test, the instrument shall discard it and use the previous version of the software **or become inoperative.**

5.2.6.2.5 **The manufacturer shall ensure** ~~**It shall be guaranteed**~~ by appropriate technical means eg. an audit trail 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 shall contain the following information: **notification** ~~**success / miscarriage**~~ of the update procedure, software identification of the installed version, time stamp of the event, identification of the downloading party. An entry is generated for each update ~~**attempt regardless of the success**~~.
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. ***Note: This needs to be discussed further due to some manufacturer concerns about where the software that displays the audit trail information is located and who has access if this feature is provided.***

5.2.6.2.6 It shall be guaranteed by technical means that software may only be updated with the explicit consent of the user or owner of the measuring instrument. ~~**Relevance of this requirement depends on national legislation.**~~

5.2.6.2.7 If the requirements **5.2.6.2.1** to **5.2.6.2.6** cannot be fulfilled, it is still possible to update the legally non-relevant software part. In this case the following requirements shall be met:

- There is a distinct separation between the legally relevant and non-relevant software according to 5.2.1.2.
- The whole legally relevant software part cannot be updated without breaking a seal.
- It is stated in the type approval certificate that updating of the legally non-relevant part is acceptable.

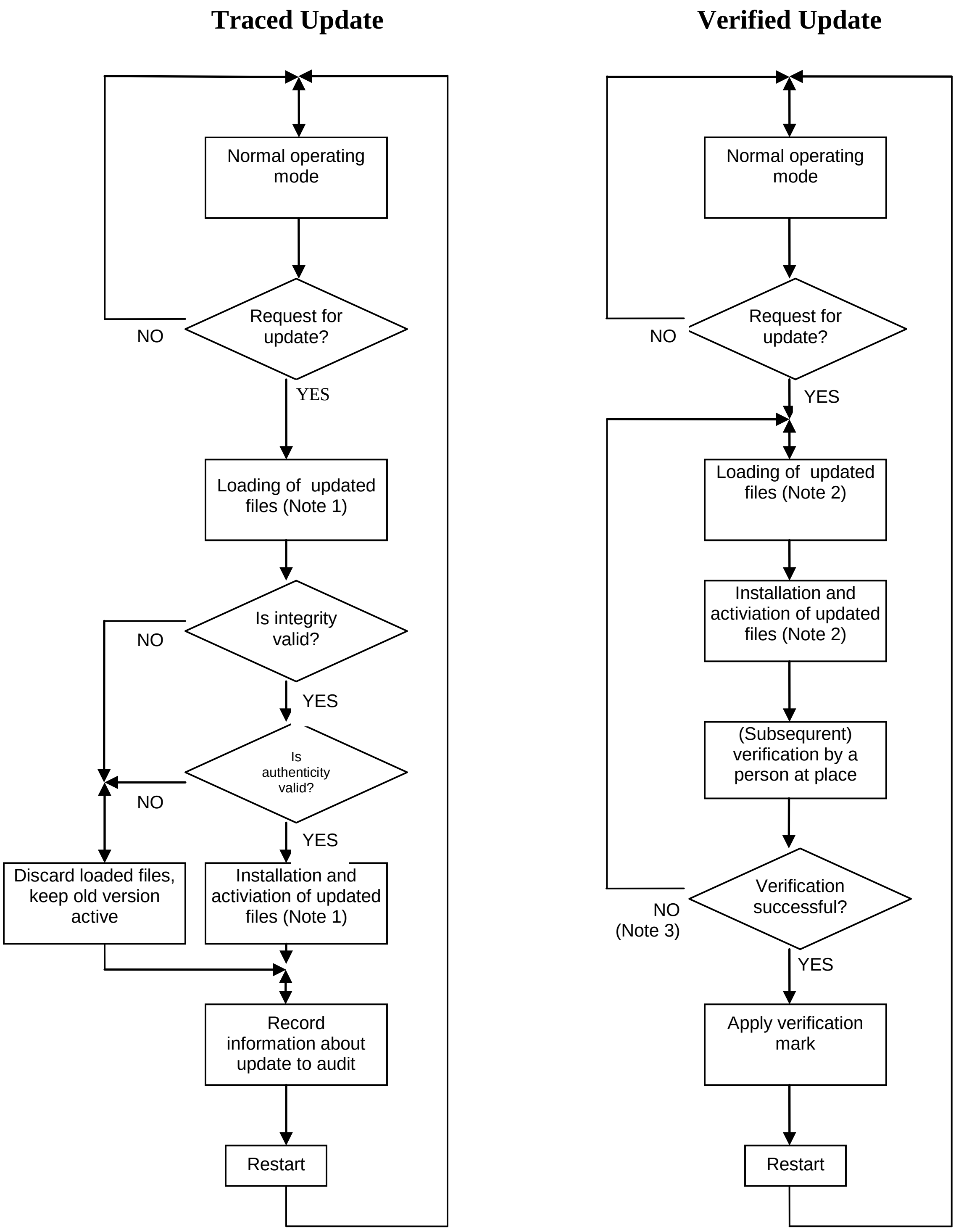
Traced Update
Verified Update
Normal operating mode
Request for update?
NO
YES
Loading of updated files (Note 1)
Is integrity valid?
NO
YES
Is authenticity valid?
NO
YES
Discard loaded files, keep old version active
Installation and activiation of updated files (Note 1)
Record information about update to audit
Restart
Normal operating mode
Request for update?
NO
YES
Loading of updated files (Note 2)
Installation and activiation of updated files (Note 2)
(Subsequrent) verification by a person at place
Verification successful?
NO
(Note 3)
YES
Apply verification mark
Restart

Figure 5-1: Software update procedures

Notes to

Figure 5-1:

1) In case of *Traced update* updating is separated into the steps: “loading” and “installing/activating”. This implies that the software is temporarily stored after loading without being activated because it must be

possible to discard the loaded software and fall back to the old version, if the checks fail **or become inoperative.**

2) In case of *Verified update* the software may also be loaded and temporarily stored before installation but depending on the technical solution loading and installation may also be accomplished in one step.
3) Here only failing of the verification because of the software update is considered. Failing because of other reasons doesn't require re-loading and re-installing of the software, symbolised by the NO-branch.

7. Verification in the Field, By the Inspector

Source: NTETC Software Sector

Time to work on this item.

8. NTEP Application – [mfg documentation to be submitted]

Source: NTETC Software Sector

Time to work on this item.

9. Next Meeting

Next Meeting could be scheduled in conjunction with the NTEP Lab Meeting which is planned for Ottawa, Canada toward the end of April. Details are now being worked out.