WELMEC 2.3
Issue 2

WELMEC

European co-operation in legal metrology

Guide for Examining Software (Weighing Instruments)

Published June 2002

WELMEC

European cooperation in legal metrology

WELMEC is a cooperation between the legal metrology authorities of the Member States of the European Union and EFTA. This document is one of a number of Guides published by WELMEC to provide guidance to manufacturers of measuring instruments and to notified bodies responsible for conformity assessment of their products. The Guides are purely advisory and do not themselves impose any restrictions or additional technical requirements beyond those contained in relevant EC Directives. Alternative approaches may be acceptable, but the guidance provided in this document represents the considered view of WELMEC as to the best practice to be followed.

Published by:
WELMEC Secretariat
BEV
Arltgasse 35
A-1160 Vienna
Austria

Tel: +43 1 21176 3608
Fax: +43 1 49 20 875
Email: welmec@metrologie.at
Website: www.welmec.org

Contents

1. Introduction 4

1.1 Background 4

1.2 General considerations 4

1.3 Scope 5

1.4 Conception 7

2. Terminology 8

2.1 Legally relevant software 8

2.2 Changes of software 10

2.3 Protection of software 10

3. Software Requirements 10

3.1 Protection of the legally relevant software 10

3.2 Software interfaces 11

3.3 Software identification 12

3.4 Documentation 13

4. Report on the Software Examination 13

5. Required Specifications in Certificates 13

6. Preliminary Procedure 14

Annex I Checklist to Report on the Software Examination 15

Annex II Examples of Legally Relevant Functions and Data for AWIs 17

Annex III Software Download on Weighing Instruments 18

1. Introduction

1.1 Background

The EC Directive 90/384/EEC states some essential requirements for the protection against changes, manipulation or fraudulent use of non-automatic weighing instruments (NAWIs) which, in principle, have to be applied also to the software controlling these instruments:

(i) Annex I, No 8.1, Directive 90/384/EEC:
Design and construction of the instruments shall be such that the instruments will preserve their metrological qualities when properly used and installed, and when used in an environment for which they are intended...

(ii) Annex I, No 8.5, Directive 90/384/EEC:
The instruments shall have no characteristics likely to facilitate fraudulent use, whereas possibilities for unintentional misuse shall be minimal. Components that may not be dismantled or adjusted by the user shall be secured against such actions.

(iii) Annex II, No. 1.7, Directive 90/384/EEC:
The applicant shall keep the notified body that has issued the EC type-approval certificate informed of any modification to the approved type...

In the practice of type examination of NAWIs by the various European Notified Bodies, it has become apparent that the above essential requirements very urgently need a uniform interpretation with regard to intelligent, user-accessible (freeprogrammable) peripheral devices or modules of NAWIs, such as PC-based indicators, data storage devices or point of sales devices (POS).

The item of ′Software Requirements for NAWIs’ was raised at the 7th WG2 meeting on 23 February 1994 where a respective discussion paper and questionnaire of the PTB was circulated. The results were discussed at the 8th WG2 meeting at SP in Borås on 6/7 June 1994, where it was decided to cooperate with CECIP (the European Committee of manufacturers of weighing instruments) on this matter.

A WG2 subgroup was constituted, consisting of CECIP, DADTI (Denmark), DELTA (Denmark), NMi (the Netherlands), NWML (UK), PTB (Germany), SDM (France) and SP (Sweden).

On the occasion of a subgroup meeting in Berlin on 5/6 September 1994, a consensus of all participants - including CECIP - was achieved about a ′5 point catalogue′ of software requirements for freeprogrammable, PC-based modules or peripheral devices which are linked to, or form part of, NAWIs subject to legal control.

On the basis of this catalogue, a draft of ′Requirements on software for NAWIs subject to legal control’ was worked out which was circulated among all subgroup members and finally discussed and its principles agreed upon at the 9th WELMEC WG2 meeting in Brussels, 22/24 November 1994. Both sides, the representatives of the Notified Bodies responsible for type examinations of NAWIs and the representatives of CECIP fully agreed that there is a very urgent need for a ′Guide for examining software for non-automatic weighing instruments (NAWI)′, and that such a document should be issued as soon as possible in order to gain experience and knowledge with the approach presented hereafter.

1.2 General considerations

The European Standard on non-automatic weighing instruments, EN 45501, specifies the metrological and technical requirements for non-automatic weighing instruments subject to legal metrological control in order to meet the essential requirements of EC Directive 90/384/EEC. The requirements of this European Standard apply to all devices performing the relevant functions, whether integrated in an instrument or manufactured as a separate unit (see EN 45501, point 2.4).

A problem with the software of weighing instruments, modules or peripheral devices is that this standard does not describe the relevant requirements and examinations to be applied to the software of these instruments or modules and how the result of the examination is to be documented.

This guide tries to fill this gap with regard to software for freeprogrammable, PC-based devices which are linked to, or form part of, NAWIs subject to legal control.

The basic intention of this Guide is to:

- ***Describe essential properties*** of the software rather than technical solutions.
- ***Offer an effective***, but not an ***extensive protection against manipulation and simulation*** of the software performing legally relevant functions.
- ***Harmonise software examination and documentation*** by the Notified Bodies as part of the type approval and testing procedures for NAWIs and related modules or peripheral devices.

This approach takes into consideration the interests and responsibilities of both the manufacturer and the Notified Body. The manufacturer has a vital interest not only in the flexibility of his instrument but also in its protection against any misuse as far as he is liable for his product; this includes his responsibility for the conformity of the individual instrument to the approved type. The Notified Body by law is forced to examine thoroughly the conformity of a type with EC regulations and the measures taken to protect the customer of an instrument against wrong measurement, unintentional misuse and fraudulent use.

1.3 Scope

This guideline specifies ***basic requirements*** to be applied to software for freeprogrammable, PC-based modules or peripheral devices which are linked to, or form part of, NAWIs subject to legal control.

The Figures 1 and 2 schematically illustrate the structures of the hardware and software of a PC-based weighing system comprising devices and functions subject to legal control (inside the circles) and others not subject to legal control (outside the circles). Both figures are intended to serve as examples in order to demonstrate the basic principles of this guideline rather than as sophisticated models that cover all possible technical solutions. Therefore, they have to be interpreted with close regard to the requirements of the Directive 90/384/EEC and the European Standard EN 45501, respectively.

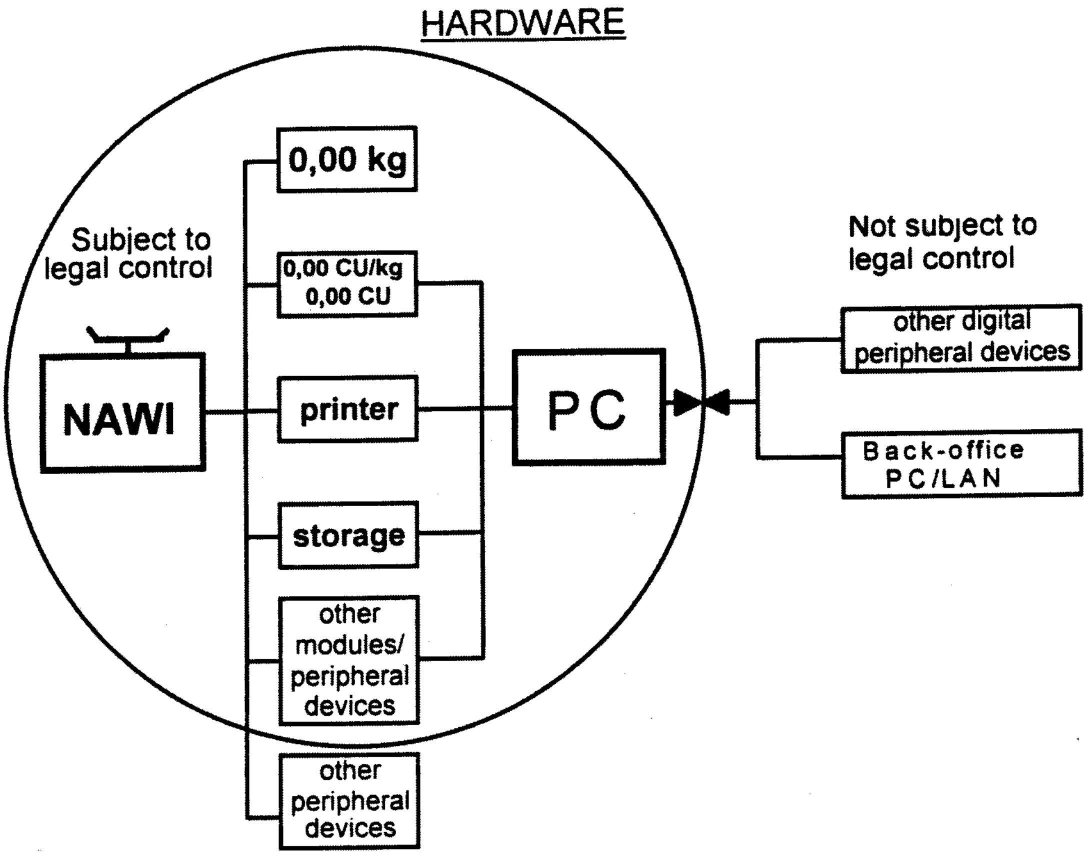

Figure 1: Example of a hardware structure of a PC-based weighing system; CU currency unit

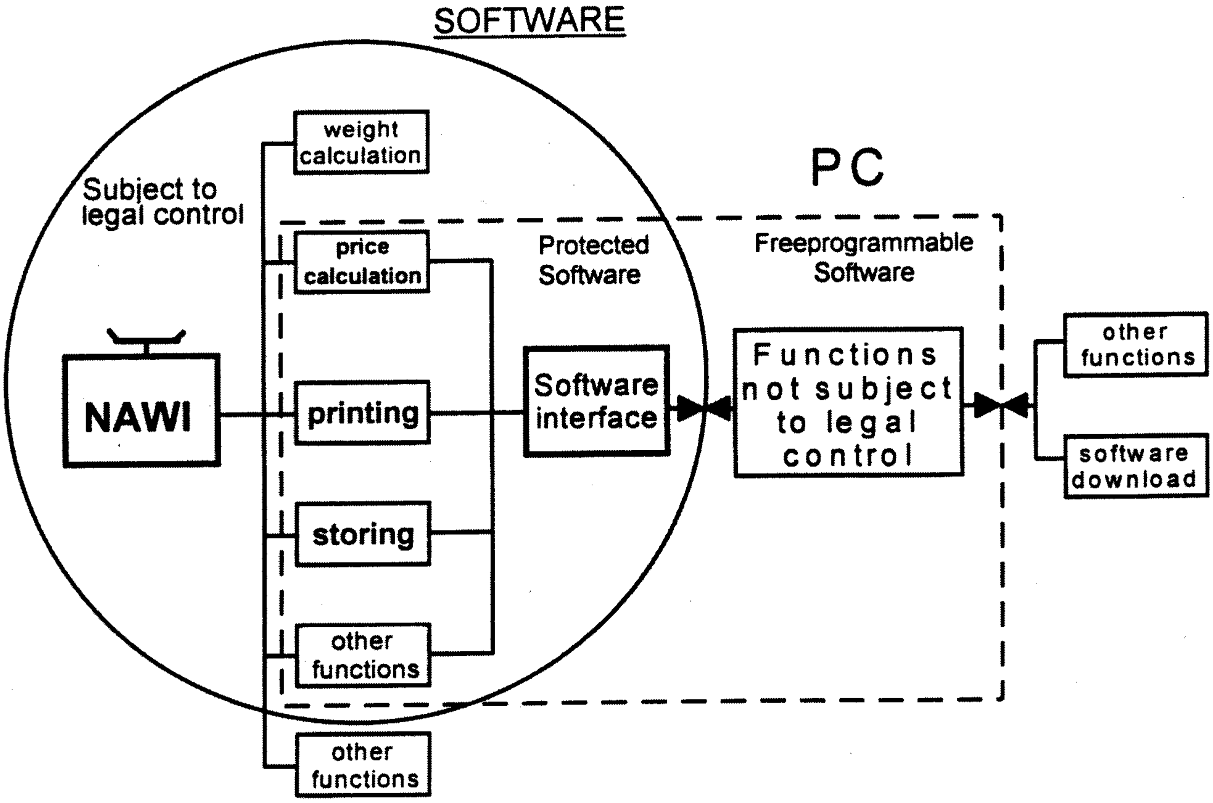

Figure 2: Example of a software structure of a PC-based weighing system

The basic instrument is the NAWI comprising at least a load cell, a load receptor, a microprocessor system including an A/D converter and a weight display. The basic instrument, if need be in combination with separate modules or peripheral devices, may perform further functions subject to legal control, such as price calculation, price indication, printing or storing of weighing results and other functions, eg. tare balancing, preset tare. Other peripheral devices not subject to legal control may be connected to the NAWI if the respective hardware interfaces are protective in the sense of EN 45501, Section 5.3.6.1.

A freeprogrammable PC-based module or peripheral device will ***not*** be subject to legal control if it communicates with the NAWI via a protective ***hardware interface*** and if it does not carry out ***any*** legally relevant function.

But today, freeprogrammable modules and peripheral devices - for example POS devices - take over more and more legally relevant functions from the NAWI, eg. printing of weighing results or price calculation. In this case, the ***hardware*** of the PC-based device is subject to legal control (see Figure 1). The ***software*** of such a device performs both functions subject to legal control and others not subject to legal control (see Figure 2).

The scope of this guide is to define the basic requirements to be met by the software of a PC-based device in order to have a ***freeprogrammable*** software part which can be adapted to the special needs of a customer and a ***protected and approved*** software part realising legally relevant functions which can only be changed with the knowledge and consent of the responsible Notified Body. This can be achieved by realising a ***software interface*** between the protected software part and the freeprogrammable part (see Figure 2 and Section 3.2) which itself is protective in the sense of EN 45501, Section 5.3.6.1. The software download for the PC-based device may then even be performed from a back-office PC within a local area network (LAN); also any other digital peripheral device not subject to legal control may be connected to the PC via an arbitrary (not necessarily protective) hardware interface.

Of course, the manufacturer of the instrument is free to declare the entire software to be subject to legal control. In this case the complete PC-based device including the software will be subject to legal control (ie. hardware and software of the device are completely inside the circle, see Figures 1 and 2) and ***any*** change of the software would have to be announced to the responsible Notified Body according to Annex II, No 1.7, Directive 90/384/EEC (see Note 2 under Section 3.2). In this case, of course, all hardware interfaces of the PC-based device to other digital peripheral devices would have to be protective in the sense of EN 45501, Section 5.3.6.1.

1.4 Conception

The conception of this guideline is the following:

- Definition of the most important terms in Section 2 ***'Terminology'***.
- Formulation of four essential requirements for the software of freeprogrammable modules or devices connected to NAWIs subject to legal control in Section 3 ***`Software requirements'***.
- ***Notes*** to the essential requirements to support their uniform interpretation.
- Suggestion of ***acceptable solutions*** to the manufacturer to demonstrate how he can meet the essential requirements. The manufacturer is free to choose different solutions if he can prove that with his solutions the essential requirements are met as well.
- Proposals to the Notified Bodies concerning a ***report*** on the software examination, see Section 4, and the ***specifications*** required in the type approval certificate (TAC) of the complete instrument or in the test certificate (TC) of the freeprogrammable module or peripheral device, see Section 5.

  The acceptance of certificates issued by other Notified Bodies is greatly enhanced if the results of the software examination are documented properly.
- This guideline is intended to serve as a ***preliminary document*** stating ***basic software requirements*** for a special type of measuring instrument, see Section 6. On the one

hand, it surely needs to be revised after some time (eg. after one year), when enough experience and knowledge have been gained by the responsible Notified Bodies; on the other hand it shall not anticipate general software requirements for all classes of measuring instruments which will be worked out by WELMEC WG7 or other WELMEC working groups.

2 Terminology

2.1 Legally relevant software

Program parts and data that form, by declaration of the manufacturer and by approval of the notified body, the software subject to legal control, see Figures 2 and 3.

Legally relevant program parts

Parts of the legally relevant software which realise functions subject to legal control, see Figure 3.

Legally relevant data

Parameters and data subject to legal control; according to Figure 3, the following types of legally relevant data can be distinguished:

- ***Type-specific parameters*** which depend on the special type of instrument only. Type-specific parameters are fixed at the type approval of the instrument.
- ***Device-specific parameters*** which depend on the individual device or instrument; device-specific parameters comprise ***calibration parameters*** (eg. of span adjustment, other adjustments or corrections) and ***configuration parameters*** (eg. Max, Min, e, d, units of measurement). Device-specific parameters are adjustable or selectable only in a special operational mode of the instrument. Some device-specific parameters may also be type-specific.
- ***Variable values*** which depend on the measurement (weighing) process itself. Variable values comprise ***processed variable values*** which are still under process of the legally relevant program parts and ***final variable values*** which are the final results of the measurement (weighing) process.

Examples of legally relevant functions and data are given in Table 1.

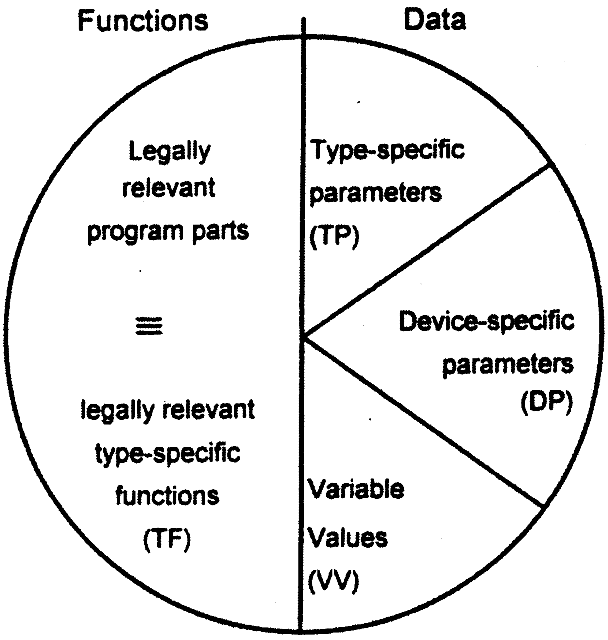
Functions
Data
Legally relevant program parts
≡
legally relevant type-specific functions (TF)
Type-specific parameters (TP)
Device-specific parameters (DP)
Variable Values (VV)

Figure 3: Schematic representation of the legally relevant software comprising legally relevant program parts (functions) and data

Table 1: Examples of legally relevant functions and data

Functions / data	**Type**
weight calculation	TF, TP
stability analysis	TF, TP
price calculation	TF, TP
rounding algorithm for price	TF, TP
span (sensitivity)	DP
corrections for non-linearity	DP (TP)
Max, Min, e, d	DP (TP)
units of measurement (eg. g, kg)	DP (TP)
weight value as displayed (rounded to multiples of e)	VV
tare, preset tare	VV
unit price, price to pay	VV
weight value in internal resolution	VV
status signals (eg. zero indication, stability of equilibrium)	VV

2.2 Changes of software

Unintentional changes
Changes of program parts or data subject to legal control that are unintentionally performed *by the user* of the instrument.

Intentional changes with common software tools
Changes of the legally relevant software that are performed using functions of its own or software tools and know-how commonly available to the general public.

Intentional changes with special software tools
Manipulation or simulation of the legally relevant software that is performed using software tools and know-how not commonly available to the general public.

2.3 Protection of software

Protected software
Software, including type- and device-specific parameters, a change of which either is not possible or is detected and made evident, e.g by an audit trail.

Audit trail („Footprint“)
An electronic count and/or information record of the changes to the device-specific parameters. An audit trail can be realised eg. as an ‘Event counter’ or as an ‘Event logger’.

Event counter
A non-resettable counter that increments once each time a special operational mode of the instrument is entered and one or more changes are made to device-specific parameters.

Event logger
A file containing a series of records where each record contains the number from the event counter corresponding to the change to a device-specific 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.

3 Software requirements

3.1 Protection of the legally relevant software

The legally relevant software shall be protected against intentional changes with common software tools.

Note 1
The program parts and data of the legally relevant software will be regarded as sufficiently protected against *unintentional changes* if the above requirement is met.

Note 2
The protection against *intentional changes with special software tools* is not the object of these requirements, as those changes are considered as criminal actions which are covered by existing laws.

Note 3
It can normally be assumed that it is not possible to influence legally relevant data - especially processed variable values - as long as they are processed by a program which fulfils the requirements under Sections 3.1 and 3.2. However, if legally relevant data - especially final variable values - will be transmitted out of the protected software part for applications or functions subject to legal control, see Figure 2, they shall be secured in order to meet EN 45501, Section 5.3.6.3.

Note 4
The part of the legally relevant software exclusively dealing with final variable values will be regarded as sufficiently protected, if these variable values cannot be changed with common software tools.

Note 5
At the moment, for example, all kinds of text editors are regarded as common software tools.

Example of an acceptable solution

Objective	*Acceptable solution for legally relevant software*	*Documentation for type approval*	*Examples for checking at type approval*
Protection of the relevant functions of the measuring instrument while measurement is active. Protection against circumventing of software interfaces (see Section 3.2).	° closed shell of the programs subject to legal control, only controlled access to the operating system for the user ° communication between programs subject to legal control and others via software interfaces according Section 3.2	° complete set of commands (from keyboard or any interface) and the meaning of each command ° declaration of the completeness of the documented command set	° practical test of the shell by checking, whether all commands operate as documented ° check, whether the declaration for completeness is given ° verify the protection means by using a text editor
Protection against intended changes of the legally relevant program and the type-specific and device-specific parameters	° checksum and audit trail over machine code of legally relevant program parts and type-specific parameters ° checksum and audit trail over device-specific parameters ° no start if code is falsified	° declaration that checksum(s) are generated ° documentation of the manufacturers selected solution	° check, whether checksum(s) are generated and comply with the documentation ° verify the protection means by using a text editor

3.2 Software interfaces

Interfaces between the legally relevant software and the software parts not subject to legal control shall be protective.

Note 1
If parts of software exist besides the legally relevant parts, these parts shall be separated in a sense that they communicate via a software interface, see Figure 2. A software interface is defined as being protective:

- if in accordance with EN 45501, Section 5.3.6.1, only a defined set of parameters and functions of the legally relevant software part can be influenced via this interface and
- if both parts do not exchange information via any other link.

Software interfaces are part of the legally relevant software. They comprise program modules and data structures.

Note 2
Software interfaces need not be protective if the manufacturer will announce ***any*** change of the software (including the legally irrelevant part) of an EC type-approved instrument to the notified body according to EC directive 90/384/EEC, Annex II, No 1.7. In this case, the software identification, cf. Section 3.3, must comprise the entire program.

Note 3

Circumventing the protective interface ***by the user*** is considered as a criminal action if the software is protected in the sense of Section 3.1.

Example of an acceptable solution

Acceptable solution for legally relevant software	*Documentation for type approval*	*Examples for checking at type approval*
° definition of program modules used to handle legally relevant functions and data ° definition of functions which may be released via the protective interface ° definition of data which may be exchanged via the protective interface	° short functional description of the legally relevant program modules ° complete list of the legally relevant functions and data ° declaration of completeness of these lists	° check, whether the functional description is conclusive ° check, whether all documented functions or data released or exchanged via the protective interface are allowed ° check, whether the declaration for completeness is given

3.3 Software identification

There must be a software identification, comprising the legally relevant program parts and parameters, which is capable of being confirmed at verification.

Note 1

The software identification may be split into two parts, one comprising the non-adjustable, type-specific functions and parameters, the other one comprising the device-specific parameters, see Figure 3.

Note 2

The operating system of the PC and auxiliary software, such as video drivers, printer drivers or hard disk drivers, need not be included in the software identification. However, special application software made by or by order of the manufacturer of the instrument shall be included in the software identification if those program parts affect the printer or display subject to legal control (eg. software parts realising the layout and printing of a receipt, see Figure 2).

Example of an acceptable solution

Acceptable solution for legally relevant software	*Documentation for type approval*	*Examples for checking at type approval*
° checksum (or other signature) over machine code which represents the legally relevant program parts and type-specific parameters	° documentation of the manufacturers selected solution	° check, whether the checksum(s) or other signature(s) are generated and may be confirmed at verification
° checksum (or other signature) over device-specific parameters	° documentation of the manufacturers selected solution	° check, whether the checksum(s) or other signature(s) are generated and may be confirmed at verification, eg. by an audit trail

3.4 Documentation

The documentation shall describe:

- All legally relevant parts and parameters of the software.
- The functions of these parts.
- The complete set of commands to be exchanged via the protective software interface.
- A written declaration of completeness of the list of the legally relevant functions and parameters and the documented set of commands.
- The securing measures (eg. checksum, software identification, audit trail).
- The instructions in order to check the legally relevant software at verification.
- A written declaration that the standard EN 45501:1992/AC 1993 has been adopted.

4 Report on the software examination

The software examination by the Notified Body is to be documented in a *short* report which can be made available to other Notified Bodies on their request.

The report shall contain:

- A reference to the type of PC-based, freeprogrammable instrument, module or peripheral device used for the examination of the software. If a certificate (TAC or TC) was issued for that device, the respective certificate number should also be referred to.
- A list of the documents concerning the software supplied by the manufacturer and examined by the Notified Body (including date and identification No).
- A list of programs and program modules, including their identification numbers, which form the legally relevant software.
- A checklist containing the examinations performed in order to verify that the requirements under Sections 3.1 to 3.4 are met. The checklist shall comprise all checks mentioned under 'Examples for checking at type approval' in the tables under Sections 3.1 to 3.3 and all points mentioned under Section 3.4. If the manufacturer offers a solution differing from the given 'Examples of an acceptable solution', the reasons for accepting this solution shall be given.

5 Required specifications in certificates

The type-approval certificate (TAC) of the complete, freeprogrammable NAWI or the test certificate (TC) of the freeprogrammable module or peripheral device of a NAWI shall contain the following specifications:

- A statement that there exist two separate software parts, one part representing the legally relevant software and the other one realising functions not subject to legal control.
- A statement that the legally relevant software meets the requirements of Sections 3.1 to 3.4 of the 'WELMEC Guide for examining software of non-automatic weighing instruments (NAWI)
- A *short* functional description of the legally relevant software, including eg. keyboard interfaces, terminal interfaces, hard disk interfaces and the software interface (mentioning the different interfaces and their functions is sufficient).
- The identification number(s) of the legally relevant software
- A list or a summary of the software documents of the manufacturer
  (reference to the report on the software examination, cf. Section 4)

- Information for verification:
  - How to verify the software identification
  - How to get access to detected software changes, made evident eg. by an audit trail

6 Preliminary procedure

These requirements are valid until general software requirements for measuring instruments under legal control will be elaborated by WELMEC Working Group 7. For the time being, only the functional description of the software is examined according to the requirements under Sections 3.1 to 3.4.

Annex I

CHECKLIST

to Report on the Software Examination (Section 4)

This checklist essentially refers to the examples of acceptable solutions given under Sections 3.1 to 3.4 of the WELMEC Guide 2.3. Other solutions may be chosen by the manufacturer which should then be explained in the documentation and in the report on the software examination.

The abbreviations used in the following mean:

y	=	The respective requirement / documentation is met / existing	
n	=	Requirement is not met or documentation is not (completely) existing	
n/a	=	Requirement is not applicable (shall be explained in the report)	
DP	=	Device-specific parameter (eg span)	
PM	=	Program module subject to legal control	see Section 2.1
TP	=	Type-specific parameter	
VV	=	Variable value	
PSI	=	Protective software interface	

1 Protection of the legally relevant software (Section 3.1)

1.1/A Closed shell of the programs subject to legal control:

- Automatic booting of the PMs: y □ n □ n/a □
- User has no access to the operating system of the PC: y □ n □ n/a □
- User has no access to other programs than the approved ones: y □ n □ n/a □
- The complete set of commands (eg function keys or commands via external interfaces) is given and shortly described: y □ n □ n/a □
- A written declaration of the completeness is given: y □ n □ n/a □

or:

1.1/B User-accessible operating system and/or programs:

- Description of the commands and functions available to the user: y □ n □ n/a □
- Checksum over machine code of the PMs and TPs is generated: y □ n □ n/a □
- Legally relevant program cannot be started if code is falsified: y □ n □ n/a □

1.2 Checksum over the DPs is generated: y □ n □ n/a □

1.3 Audit trail for the protection of the DPs is described: y □ n □ n/a □

1.4 Practical test of the performance of some documented functions with the following commands: ... y □ n □ n/a □

2 Software interfaces (Section 3.2)

2.1 PMs are defined and separated from the modules not subject to legal control by a defined PSI: y □ n □ n/a □

2.2 PSI itself is defined as part of the PMs: y □ n □ n/a □

2.3 The *functions* of the PMs that may be released via the PSI are defined and described: y □ n □ n/a □

2.4 The *parameters* that may be exchanged via the PSI are defined and described: y □ n □ n/a □

2.5 The description of the functions and parameters is conclusive and complete: y □ n □ n/a □

2.6 Each documented function and parameter does not contradict EN 45501:1992/AC 1993: y □ n □ n/a □

2.7 The application programmer is instructed by appropriate means (eg in the software documentation) about the requirements concerning the PSI: y □ n □ n/a □

3 Software identification (Section 3.3)

3.1 Checksum over the PMs and the TPs is generated: y □ n □ n/a □

3.2 Every PM and TP is included in this checksum: y □ n □ n/a □

3.3 Checksum over the DPs is generated: y □ n □ n/a □

3.4 Every DP is included in this checksum: y □ n □ n/a □

3.5 The checksums (or other signatures) are generated as documented and may be confirmed at verification: y □ n □ n/a □

3.6 Audit trail does exist and may be checked at verification: y □ n □ n/a □

4 Software documentation (Section 3.4)

4.1 A complete list of PMs with a description of each PM is supplied: y □ n □ n/a □

4.2 A complete list of the legally relevant parameters and a short description of each parameter is supplied separately for:

- TPs: y □ n □ n/a □
- DPs: y □ n □ n/a □
- VVs: □ n □ n/a □

4.3 A complete set of commands to be exchanged via the PSI is supplied: y □ n □ n/a □

4.4 A written declaration of the completeness of the lists under 4.1, 4.2 and 4.3 is given: y □ n □ n/a □

4.5 A description of the following securing measures is given:

- checksums y □ n □ n/a □
- software identification y □ n □ n/a □
- audit trail (eg event counter, event logger) y □ n □ n/a

4.6 Instructions for checking the software identification number(s) at verification are given: y □ n □ n/a □

4.7 A written declaration is given that the freeprogrammable system, including its software, does meet the requirements of EN 45501:1992/AC 1993, Section 5.3.6: y □ n □ n/a □

Annex II

Examples of Legally Relevant Functions and Data for Automatic Weighing Instruments (AWIs)

The following table is intended to amend Table 1 of this Guide with respect to AWIs subject to pattern examination under the relevant OIML Recommendation.

Table 2: *Examples of legally relevant functions and data for AWIs in comparison with those of non-automatic weighing instruments (R76).*

The marked functions and parameters are likely to occur on the various types of weighing instruments. If one of them is present, it has then to be treated as "legally relevant". The table is however not meant as an obligatory list indicating that any function or parameter mentioned has to be realised in each instrument. (The abbreviations under "Type" are explained in Figure 3.)

Functions/data	**Type**	**OIML Recommendation No**						
		50	**51 (X)**	**51 (Y)**	**61**	**76**	**106**	**107**
Weight calculation	TF, TP	X	X	X	X	X	X	X
Stability analysis	TF, TP		X	X		X	X	X
Price calculation	TF, TP			X		X		
Rounding algorithm for price	TF, TP			X		X		
Span (sensitivity)	DP	X	X	X	X	X	X	X
Corrections for non-linearity	DP (TP)	X	X	X	X	X	X	X
Max, Min, e, d	DP (TP)	X	X	X	X	X	X	X
Units of measurement (eg. g, kg)	DP (TP)	X	X	X	X	X	X	X
Weight value as displayed (rounded to multiples of e or d)	VV	X		X		X	X	X
Tare, preset tare	VV		X	X	X	X	X	
Unit price, price to pay	VV			X		X		
Weight value in internal resolution	VV	X	X	X	X	X	X	X
Status signals (eg zero indication, stability of equilibrium)	TF	X				X		
Comparison of actual weight vs. present value	TF		X		X			
Automatic printout release, eg at interruption of automatic operation	TF							X
Warm-up time	TF (TP)	X	X	X	X	X	X	X
Interlock between functions	TF							
eg zero setting/tare						X		
automatic/non-automatic operation,							X	
zero-setting/totalising		X						X
Record of access to dynamic setting	TF (VV)		X	X				
Maximum rate of operation/range of operating speeds (dynamic weighing)	DP (TP)		X	X			X	
(Product)-Parameters for dynamic weight calculation	VV		X	X			X	
Preset weight value	VV		X		X			
Width of adjustment range	DP (TP)		X	X				
Criterion for automatic zero-setting (eg. time interval, end of weighing cycle)	DP (TP)		X	X	X		X	
Minimum discharge, rated minimum fill	DP							X
Limiting value of significant fault (if not 1e or 1d)	DP (TP)	X			X			
Limiting value of battery power	DP (TP)	X	X	X	X	X	X	X

Annex III

Software Download on Weighing Instruments

1 Scope

Modern weighing instruments, as well as other measuring instruments, are almost exclusively controlled by microprocessors. Up to now the software has been stored in non-erasable media or in media which could not be erased within the device (eg. PROM, EPROM). Exchanging software is only possible by changing the storage media which in most cases requires interference in hardware.

New data storage technologies (eg. EEPROM, Flash Memory) and new concepts of instruments admit an exchange of software via communication interfaces without interfering in hardware. In this case an in situ access to the program code and data shall be distinguished from a remote access. When performing an in situ access the download of software (eg. via floppy disk, CD or modem) is performed manually controlled, while during remote download the control is remote (eg. via modem or Internet). From the manufacturer's point of view the advantages are obvious since maintenance and service of the normally complicated software may be accomplished without service technicians at the face and thus costs can be reduced. For applications under legal control, up to now, only in situ access to the legally relevant (LR) software (see WELMEC 2.3, Chapter 2.1 "Program parts and data that form, by declaration of the manufacturer and by approval of the notified body, the software subject to legal control") is permitted and it is permitted only to authorised staff (eg. authorised service personal or field inspectors).

With non-automatic weighing instruments (NAWIs) a download by the manufacturer is already allowed, provided that it is covered by a conformity assessment procedure and that it is performed before the respective instrument is put into service. After putting into service ***national legislation*** is relevant and legal procedures have to be followed. Software normally has to be secured so that an exchange is either impossible or made evident. This is normally still done by using conventional (mechanical) sealing/securing methods such as securing stamps or the like.

From the technical point of view, however, a download of LR software (by remote or in situ access) could be performed if certain technical conditions (see Chapter 2 of this annex) are met.

New technical means of remote service basically offer the same advantages to the surveillance authorities as to the manufacturers. Suitable conditions have to be established under which a download by the manufacturer could be performed on an instrument in service, as long as the metrological characteristics remain unchanged and the declaration of conformity is still valid. This paper shall be considered as a first approach towards that purpose. Chapter 2 provides essential requirements, whereas Chapter 3 gives some ideas about examples of acceptable technical solutions.

These requirements refer to software download on weighing instruments. However the intention is to feed these general rules in a document which will be elaborated by WELMEC Working Group 7 for other measuring instruments. Within the scope of the WELMEC agreement on mutual recognition of test results, however, in principle this guideline may already be applied to automatic weighing instruments.

2. Essential Requirements

A) With destroying a conventional means of securing

The conventional way of protecting legally relevant software against changes is to use conventional or physical securing means (hardware securing) and optionally a software securing method (see WELMEC 2, Issue 3, Chapter 3.4).

B) Without destroying a conventional means of securing

Alternative to A) downloading software could be performed if all the following technical requirements are met.

B.1 It shall be guaranteed by appropriate technical means that no other than the software approved for the respective instrument can be loaded.

Note 1:
Only approved software is allowed to be loaded. Thus, if a manufacturer intends to change or update the LR software he shall - in the sense of Directive 90/384/EEC, Annex II, No 1.7 - announce the intended changes to the responsible notified body. The notified body decides whether an addition to the existing type approval is necessary or not. For software download it is indispensable that there is a software identification (for the LR software) which is unambiguously assigned to the approved software version.

Note 2:
The loadable software components and the securing means are described in the documentation supplied by the manufacturer and are laid down in the descriptive annex to the type approval document.

Note 3:
For download of LR software it is indispensable that inside the respective weighing instrument there is a fixed and specially protected software (stored eg. in a non-erasable hardware which is secured against exchange) which can neither be modified (ie. which is not downloadable, remains bit-to-bit identical) nor be influenced (eg. made inoperative). This fixed software comprises at least all device specific parameters (in the meaning of WELMEC 2.3; including the parameters and data for the checking functions) as well as all checking functions necessary for fulfilling requirements B.1 to B.3. This fixed part shall be described in the documentation supplied by the manufacturer and is laid down in descriptive annex to the approval document.

B.2 It shall be possible for the weighing instrument itself to check the authenticity and integrity of the loaded software by appropriate technical means at every download procedure.

Note:
This requirement implies an automatic checking mechanism implemented in the fixed software part of the weighing instrument itself. This does not, however, exclude the ***additional*** possibility for the user to check the integrity and authenticity of the loaded software in case of need, eg. at the touch of a single button.

B.3 It shall be guaranteed by appropriate technical means that downloads of software are adequately traceable within the instrument for subsequent controls.

Note 1:
This requirement enables inspection authorities, who are responsible for the metrological surveillance of legally controlled instruments, to trace back downloads of LR software over an adequate period of time depending on national legislation.

Note 2:
For an effective control of downloaded LR software it is indispensable that the measuring instruments are equipped with an event-logger in the sense of WELMEC 2.3, Chapter 2.3, where the software identification of the loaded software (see B.1, Note 1) is part of the data record, or any equivalent solution.

Note 3:
After having reached the limit of the event logger it is ensured by technical means that further downloads are impossible. Data sets of the event-logger can only be erased by breaking the seal of the specially protected fixed software. While doing so national regulations concerning the traceability have to be observed.

B.4 It shall be guaranteed by technical means that software can only be loaded with the explicit consent of the user of the measuring instrument.

Note 1:
After putting an instrument into service the user is responsible for it. Requirement B.4 ensures that the manufacturer cannot change the LR software of the instrument without the explicit consent of the responsible user.

Note 2:
The corresponding technical means are described in the documentation supplied by the manufacturer and are laid down in the descriptive annex to the approval document.

B.5 If there is no software separation realised in the sense of this WELMEC guide (2.3), requirements B.1 to B.4 apply to the entire software without any exception. If there is a distinct separation of the LR software and communication via a protective software interface the software not subject to legal control can be loaded without observation of requirements B.1 to B.3.

Note 1:
In the latter case the new software parts not subject to legal control shall not import new legally relevant functions.

Note 2:
During the type approval procedure it will be checked that the software separation is certain, ie. that there is no influence on the (verified) weighing instrument possible by the software not subject to legal control (see WELMEC 2.3, Chapter 3.2, examples for checking at type approval).

3. Examples of acceptable technical solutions

This section describes examples of different technical solutions by which the essential requirements according to Chapter 2 are considered being fulfilled.

3.1 Conventional Securing (requirement A)

Examples of diverse technical solutions:

- The housing of the device is sealed (secured),
- The (external) interface for downloading is sealed (secured),
- A switch physically or logically (by means of software) inhibiting the download is blocked and secured.

3.2 Software Download with Separation of Software (Example A, all requirements B.1 to B.5)

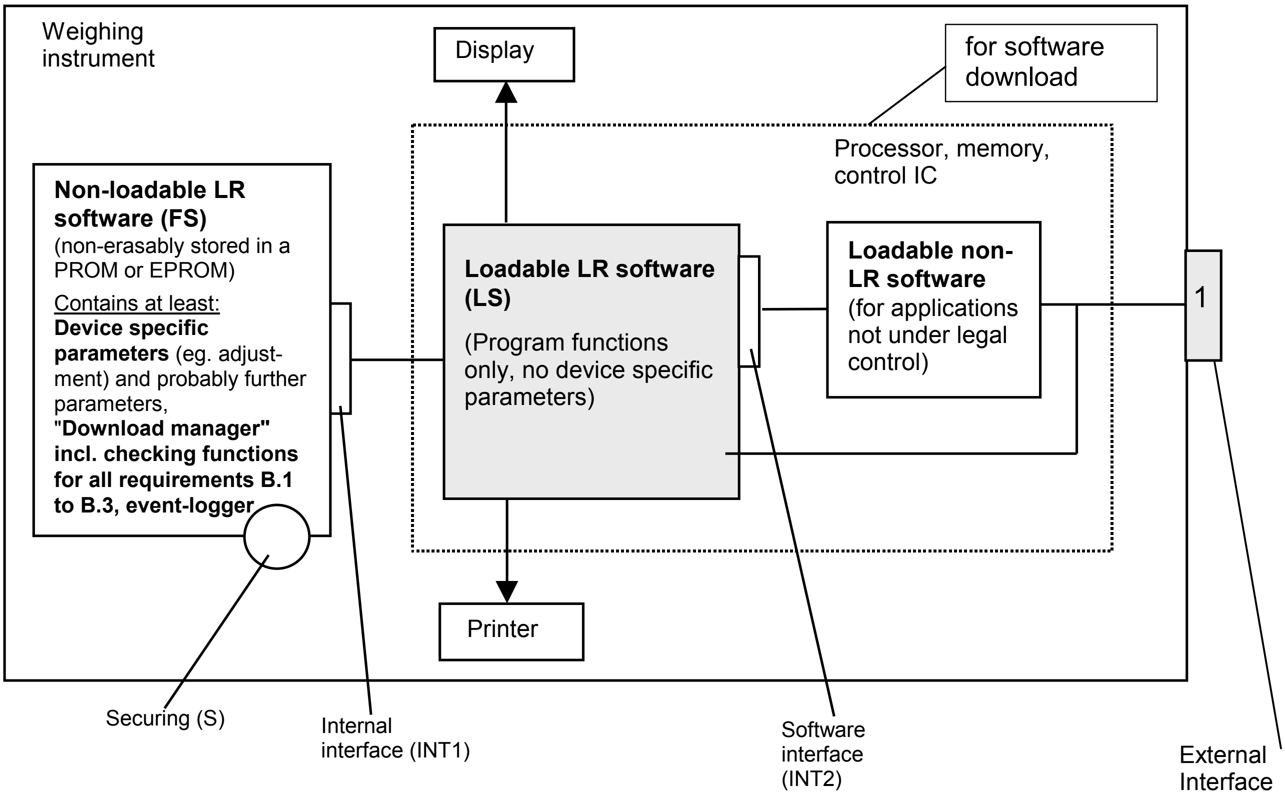
Weighing instrument
Display
for software download
Processor, memory, control IC
Non-loadable LR software (FS)
(non-erasably stored in a PROM or EPROM)
Contains at least:
Device specific parameters (eg. adjust-ment) and probably further parameters,
"Download manager" incl. checking functions for all requirements B.1 to B.3, event-logger
Loadable LR software (LS)
(Program functions only, no device specific parameters)
Loadable non-LR software
(for applications not under legal control)
1
Printer
Securing (S)
Internal interface (INT1)
Software interface (INT2)
External Interface

Figure 4: Software download into a weighing instrument with separation of the LR software from the non-LR software by a protective software interface (INT2) (see requirement B.5).

Explanations

a) The weighing software under legal control (LR software) is separated into a loadable software part (LS) and a fixed part (FS). The software separation is realised in the sense of WELMEC 2.3, ie. by a protective software interface.

b) The fixed part (FS) contains all device-specific parameters and eventually further data/ parameters and all control/ checking functions that are necessary to meet the essential requirements B.1 to B.3 (eg. "download manager", identification and authentification of the downloaded software, event-logger for tracing all download processes, display of software identification).

c) The fixed software (FS) is stored on a hardware that is access-protected and secured by a control (securing) mark (S) and cannot be influenced by the loadable software (LS). Modification of FS, except for modification (supplementation) of data in the event-logger (which are automatically modified after each downloading), is possible only after destruction of the securing mark (S).

d) The functions and parameters of the fixed software (FS) are described by the manufacturer, particularly concerning their interaction with the loadable software (LS).

e) The internal interfaces INT1 and INT2 are protective in the sense of Section. 5.3.6.1 of EN 45501 and WELMEC 2.3, Chapter 3.2. Instructions and data other than the permitted ones are not accepted.

f) A complete list of all instructions and parameters for the internal interfaces INT1 and INT2 along with a declaration of the completeness of this list is submitted by the manufacturer. In addition, the manufacturer declares that the download does not change any part of the FS (FS remains bit-to-bit identical) and does not import new legally relevant functions that are not covered by the declaration of conformity.

g) The external interface (1) is not permanently activated for software download, but will only be activated on demand of the user of the instrument (essential requirement B.4).

h) The internet connection via external interface to a specified URL (stored within the instrument, eg. as part of the device specific parameters) for downloading is initialised by the download manager that is part of the fixed software (see Figure 4).

3.3 Software Download with Separation of Software (Example B)

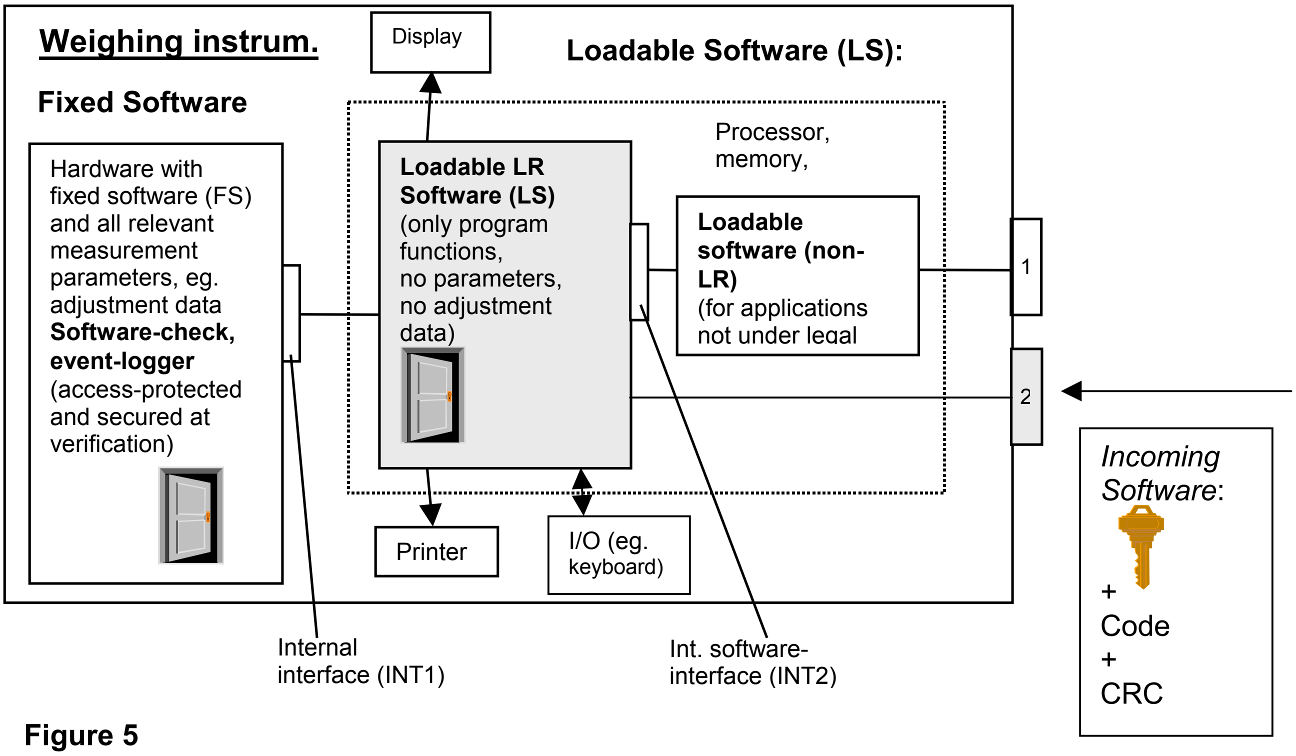
Weighing instrum.
Display
Loadable Software (LS):
Fixed Software
Processor, memory,
Hardware with fixed software (FS) and all relevant measurement parameters, eg. adjustment data **Software-check, event-logger** (access-protected and secured at verification)
Loadable LR Software (LS) (only program functions, no parameters, no adjustment data)
Loadable software (non-LR) (for applications not under legal
1
2
Incoming Software:
+ Code + CRC
Printer
I/O (eg. keyboard)
Internal interface (INT1)
Int. software-interface (INT2)

Figure 5

Explanations

a) Authenticity:
The software to be downloaded is identifying itself by means of a code (type specific, secured key). The fitting counterpart (door) is resident within the instrument as part of the device specific parameters within the legally relevant part of the fixed software (FS) that cannot be modified (see Figure 5). The checking (key - door) may be accomplished

- during the download procedure or
- after the download procedure, but not later than at the first start of the loaded software (eg. new PC program copied to the PC).

b) Integrity:
Is most simply made sure by at least a CRC16 checksum by which the program is being checked cyclically or at start.

c) Identification:
Output of a functional checksum, comparison with the checksum given in the type approval certificate. Functional checksum: each legally relevant software module bears a release number which is incremented whenever there are significant modifications as decided by the notified body responsible for type approval. The functional checksum is processed on the basis of all release numbers.

d) Automatic event-logger which cannot be deleted or modified without evidence for intervention (accomplished eg. by a data storage device and secured by a checksum of at least the level CRC-16, generated by the FS). The event-logger is registering each download (recording at least: consecutive number of the event / date / time / software identification of the loaded software / and the source of download eg. URL). The number of downloading processes is limited by physical properties of the instrument (maximum storage capacity). After having reached that limit it is ensured by technical means that further downloads are impossible. Data sets of the event-logger can only be erased by breaking the seal of the specially protected fixed software. However at least the last data set must be kept (depending on the national regulations).

e) Only releasable by the user of the instrument via a menu item on the instrument or by means of another function. This function allows a single download or repeatedly downloading over a certain period of time when being released according to rules yet to be determined (length of the period, event-logger etc.).

Revisions of this guide

Issue	Date	Significant changes
1	January 1995	Guide first issued.
Am1	August 1996	Amendment 1: Addition of Checklist to Report on the Software Examination.
Am2	August 1996	Amendment 2: Addition of Table 2 Extending Guide to Automatic Weighing Instruments (AWIs).
2	June 2002	Incorporation of Amendments 1 and 2, to form Annexes I and II. Addition of Annex III Software Download. Change to wording of Section 6. Change of title from “Guide for Examining Software (Non-automatic weighing instruments)” to “Guide for Examining Software (Weighing instruments)” Correction in Annex 1 Section 4.2 of “GP’s” to “DPs”. Addition of this Revisions table.