

How to judge whether or not weighing instruments under examination confirm software test results

Oliver Mack

Physikalisch-Technische Bundesanstalt (PTB)

Braunschweig

www.ptb.de

Introduction

Background

Requirements

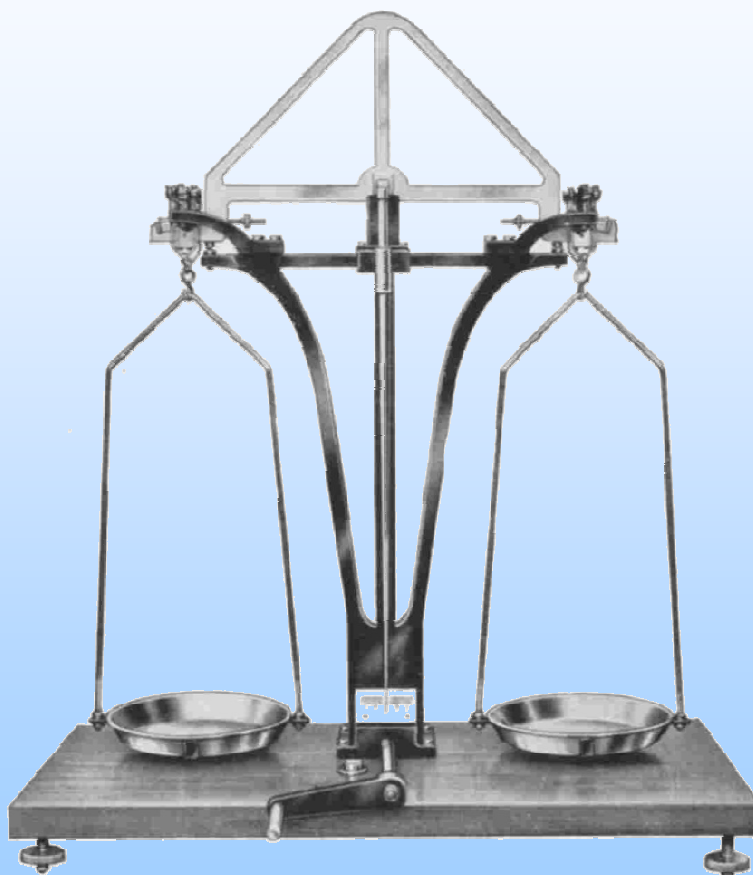
Software
Security

Interfaces

Software
Identification

Application

Software
Download



For type approval:

Documentation:

- General description of the weighing instrument
- Constructional drawings and schemes of components (load receptor, lever system, blade, socket,...)

Examination:

- Functional tests
- Accuracy tests

Introduction

Background

Requirements

Software
Security

Interfaces

Software
Identification

Application

Software
Download



Modern NAWI:

- Embedded systems controlled microprocessors
- PCs with programmable and/or loadable software
- Software is an essential part of the measuring instrument
→ Parts are under legal control

Resulting Problems:

- Software separation
- Software security

Non-automatic Weighing Instrument

Risk classification according to WELMEC 7.2

Introduction

Background

Requirements

Software
Security

Interfaces

Software
Identification

Application

Software
Download



Class B

- Conformity level: **low**
 - functions identical
- Protection against manipulation: **middle**
 - means against use of wide-spread simple tools (text editor, hex-editor, etc.)
- Examination level: **middle**
 - functional test of the instrument and software
 - examination based on functional description of the software
 - Documentation tests
 - Selected practical test

Non-automatic Weighing Instrument Software requirements (R76, 5.5.2.2)

Introduction

Background

Requirements

Software
Security

Interfaces

Software
Identification

Application

Software
Download

1. The legally relevant software shall be adequately protected against accidental or intentional changes.

Evidence of an intervention such as changing, uploading or circumventing the legally relevant software shall be available until the next verification or comparable official inspection.

2. When there is associated software which provides other functions besides the measuring function(s), the legally relevant software shall be identifiable and shall not be inadmissibly influenced by the associated software.
3. Legally relevant software shall be identified as such and shall be secured. The identification shall be easily provided by the device for metrological controls or inspections.

Software requirement

1. Protection against unnoticeable changes

Introduction

Background

Requirements

Software
Security

Interfaces

Software
Identification

Application

Software
Download

Assumption: It is not possible to influence legally relevant parameters and data, as long as they are processed by a program.

Protection: The legally relevant software with all data, parameters, variable values etc. cannot be changed with common software tools.

Common solution:

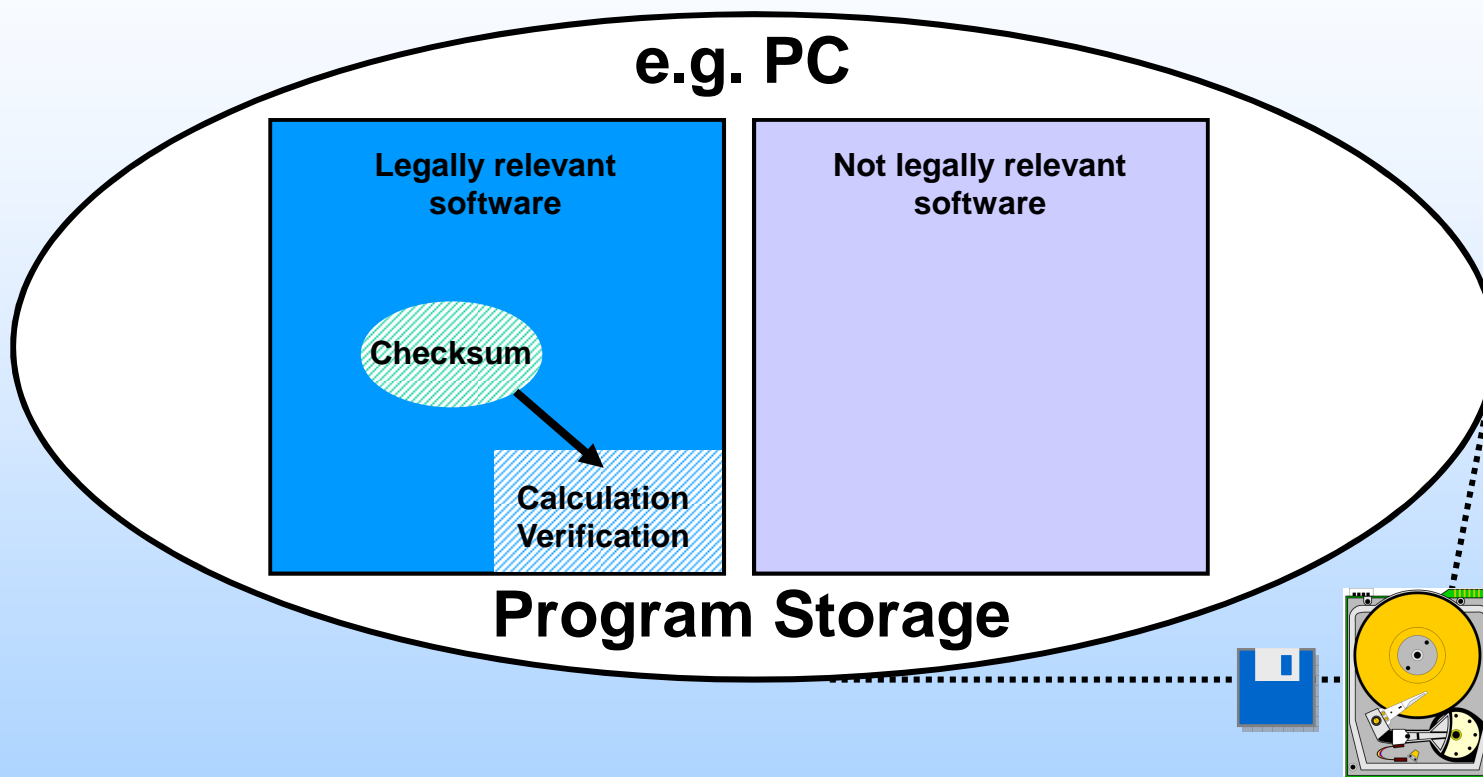
Automatic calculation of a secret checksum for the machine code of the complete legally relevant software.

- Calculation at least after start of the program or in fixed time intervals
- Security level at least CRC-16 with hidden polynomial and start value

Software requirement

1. Protection against unnoticeable changes

- Introduction
- Background
- Requirements
- Software Security**
- Interfaces
- Software Identification
- Application
- Software Download



- Examination:**
- Functional test (with Hex-Editor)
 - Check of the description in the documentation
- Criterion:**
- No start if the machine code is falsified

Software requirement

2. No influence of legally non-relevant software parts

Introduction

Background

Requirements

Software
Security

Interfaces

Software
Identification

Application

Software
Download

Assumption: Associated software is separated from the legally relevant software in the sense that they communicate via software interfaces.

Protection: The legally relevant software with all data, parameters, variable values etc. cannot be changed with common software tools.

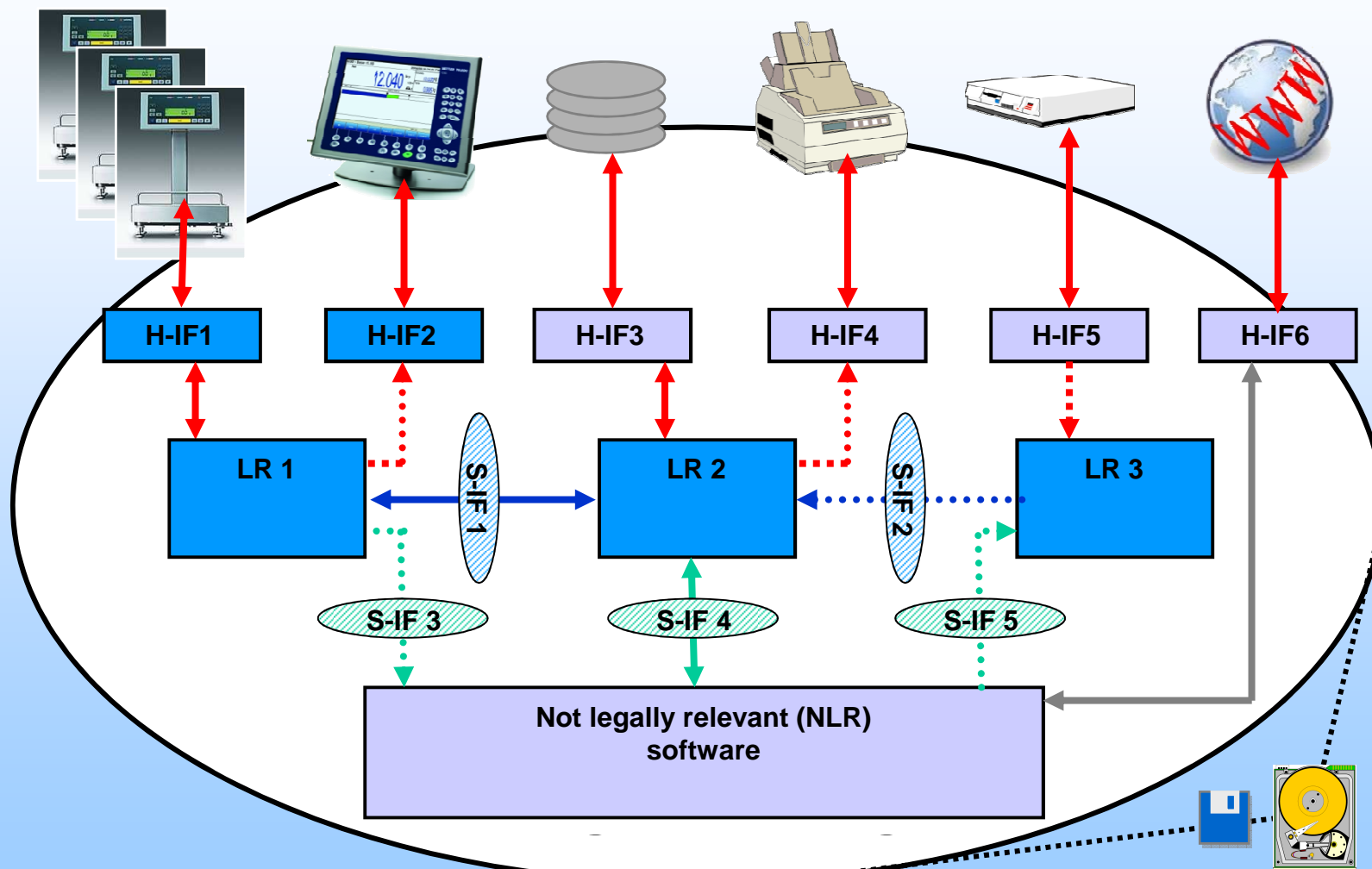
Common solution:

Definition of all functions, commands, data, etc. which are exchanged via the protective interface from the legally relevant software to all other connected software or hardware parts.

Software requirement

2. No influence of legally non-relevant software parts

Introduction
Background
Requirements
Software Security
Interfaces
Software Identification
Application
Software Download



Introduction

Background

Requirements

Software
Security

Interfaces

Software
Identification

Application

Software
Download

Examination: Documentation with
Soft- and Hardware description

- 1.) Hardware requirements of the software
- 2.) Functional description of all
legally relevant software components e.g.
 - LR 1: bill.dll: Realises the layout of the printing
 - LR 2: Programm X.exe of the data storage device
 - H-IF1: Nawi.dll: Driver with following functions: ...
- 3.) Principle description of the non legally relevant software
 - e.g. the user manual
- 4.) Principle or detailed description of the hardware,
which can be connected, e.g.
 - standard printer and displays
 - NAWIs with standard data dialog (e.g. dialog 06 for POS)
 - weighing instrument Type XYZ TAC D08-09-021

Software requirement

2. No influence of legally non-relevant software parts

Introduction
Background
Requirements
Software Security
Interfaces
Software Identification
Application
Software Download

Examination: Documentation of the interfaces

Interface	Between	Command	Type	Remark

Introduction

Background

Requirements

Software
Security

Interfaces

Software
Identification

Application

Software
Download

Examination: Documentation

Written declarations of the manufacturer

- 1.) Declaration that the freely programmable device including its software complies with standard EN45501 / OIML R76
- 2.) Declaration that the list of documented modules, functions and procedures is complete.
- 3.) Declaration that the list of documented interfaces is complete and all interfaces are non-interactive according to EN45501 No. 5.3.6.1 / OIML R76 No. 5.3.6.1
- 4.) Certificate of the manufacturer that no legally relevant functions are imported or realised with non-legally relevant software parts.

3. Legally relevant software must be identifiable and secured

Introduction

Background

Requirements

Software
Security

Interfaces

Software
Identification

Application

Software
Download

Assumption: The operating system or similar auxiliary standard software, such as video drivers, printer drivers or hard disk drivers, need not be included in the software identification.

Protection: The identification shall be easily provided at run time by the device for metrological controls or inspections.

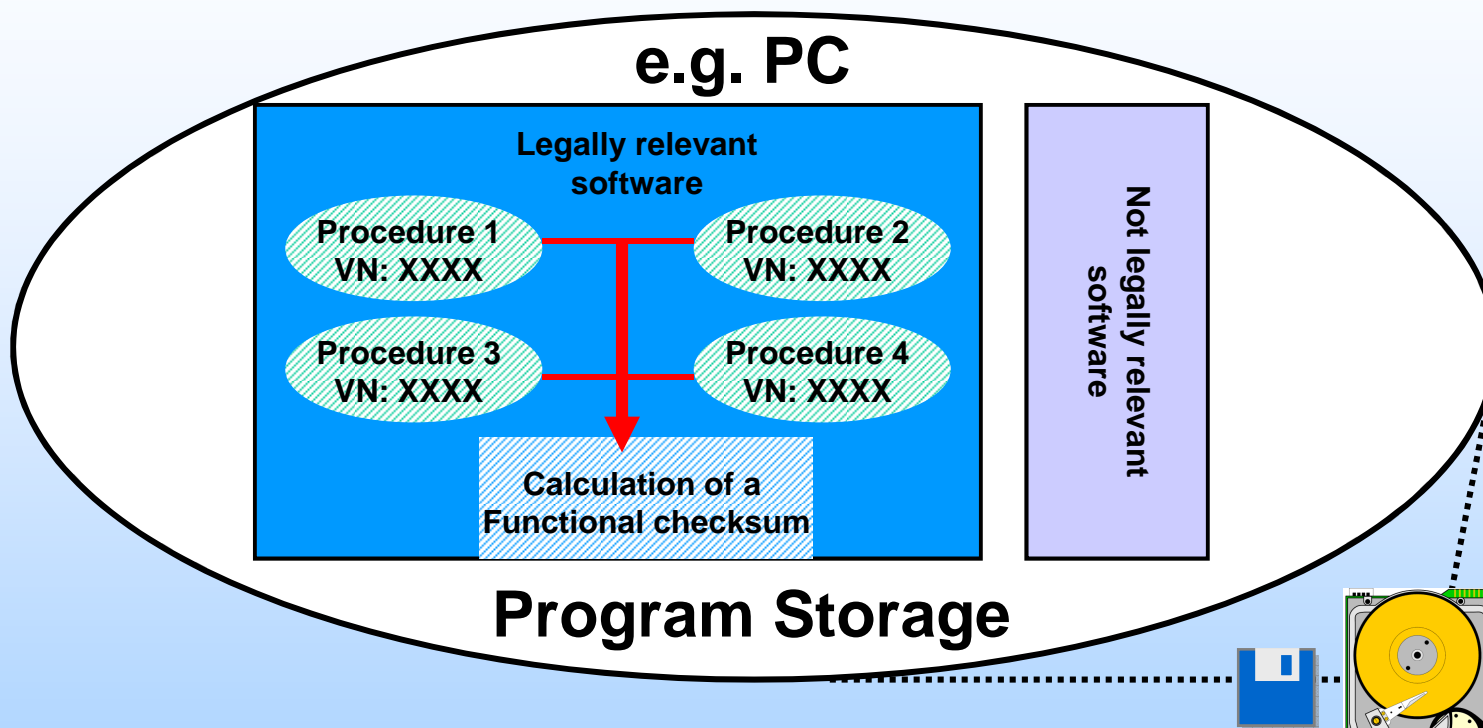
Common solution: Calculation of a checksum over the machine code of the legally relevant software at runtime and indication at any time on manual command.

Not acceptable: version number

→ Functional checksum as identification

3. Legally relevant software must be identifiable and secured

- Introduction
- Background
- Requirements
- Software Security
- Interfaces
- Software Identification
- Application
- Software Download



Intension: Each legally relevant software module or procedure bears a release number which is incremented whenever there are significant modifications of the software

3. Legally relevant software must be identifiable and secured

Introduction

Background

Requirements

Software
Security

Interfaces

Software
Identification

Application

Software
Download

- Examination:**
- Functional test
 - Description of the function and how the functional checksum is calculated
 - Description of the modules and procedures
 - Exemplary header printout with a remark for the software engineer:
„This is a legally relevant software module or procedure which requires an increase of the release number whenever there are significant modifications of the software“

- Criterion:**
- Indication of the functional checksum at any time on manual command

Non-automatic Weighing Instrument in combination with peripheral devices

Introduction

Background

Requirements

Software
Security

Interfaces

Software
Identification

Application

Software
Download



Peripheral devices based on PC software:

- Data storage devices
- Non-price-computing
Point of Sale Devices

Protection level:

- The mentioned software requirements are sufficient
- No additional security actions for PC interfaces necessary

Essential functions of the NAWI realised by PC Software

Introduction

Background

Requirements

Software Security

Interfaces

Software Identification

Application

Software Download



Essential functions

- Price Computing
- Realisation of the primary display
- Calculation of the weighing values

Software requirement (R76, 5.5.2.2)

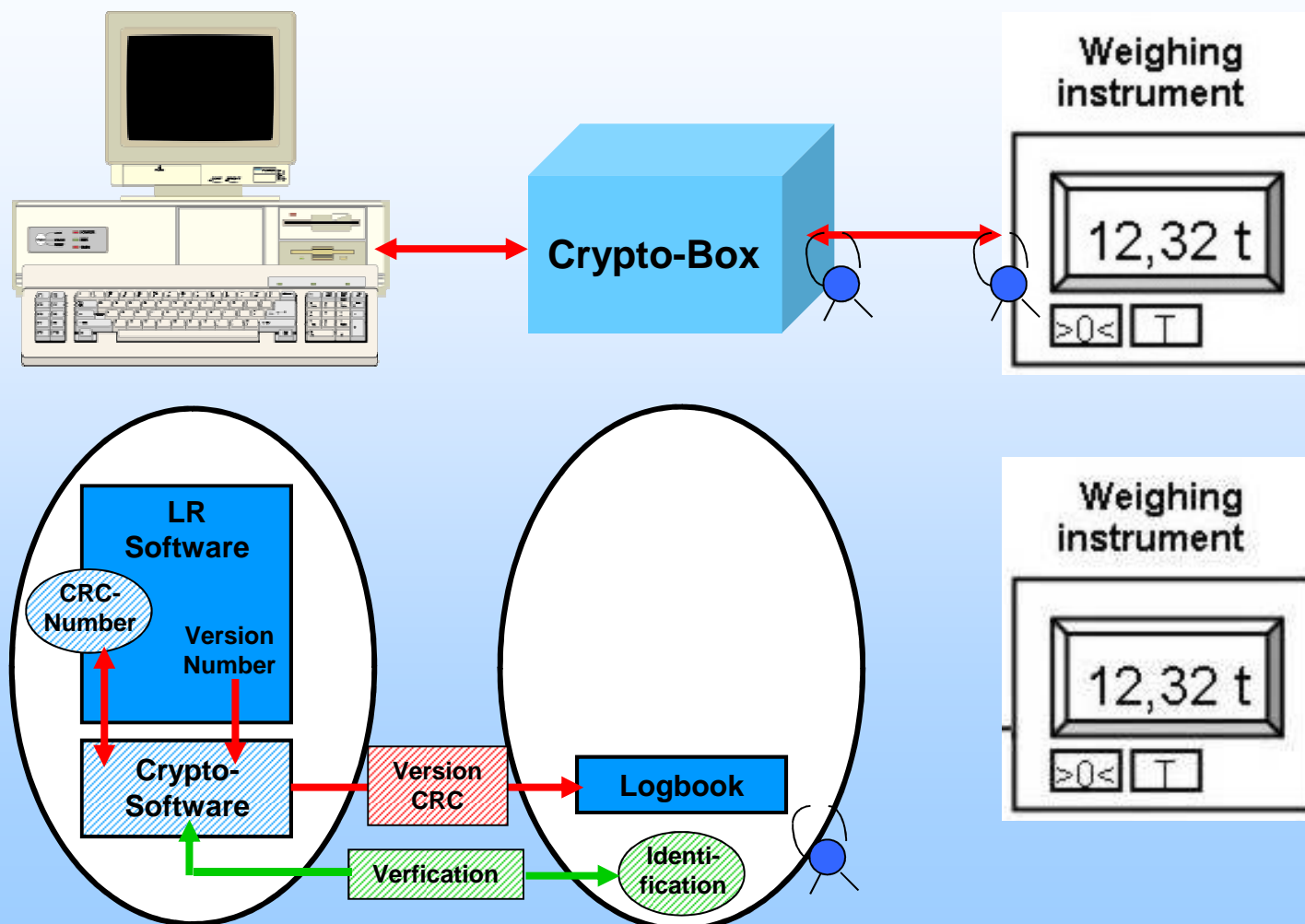
Evidence of an intervention such as changing, uploading or circumventing the legally relevant software shall be available until the next verification or comparable official inspection

Solution

- Secured PC interfaces
- Additional hardware with fixed software which controls legally relevant software

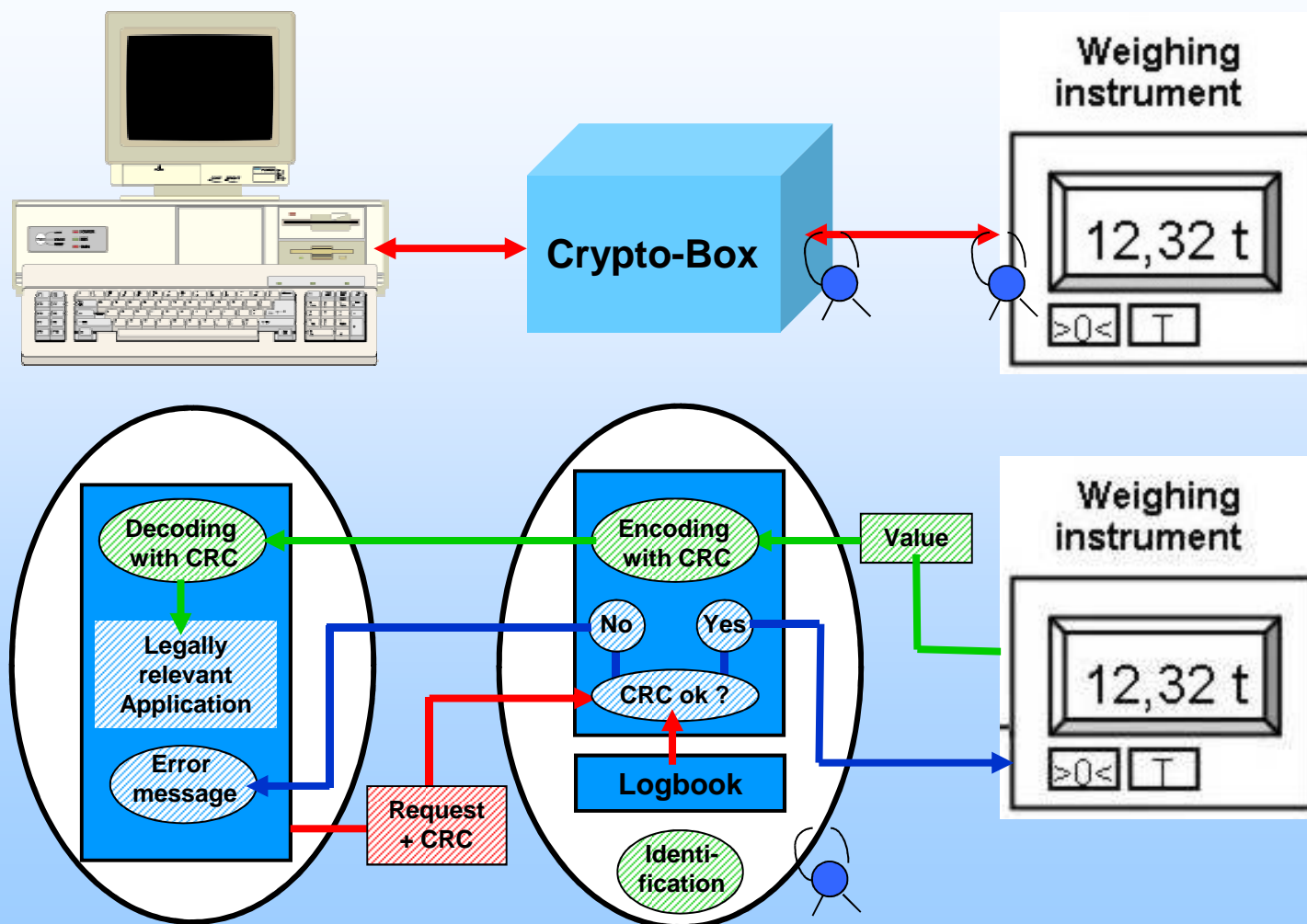
Acceptable Solution: “Cryptobox”

- Introduction
- Background
- Requirements
- Software Security
- Interfaces
- Software Identification
- Application
- Software Download



Acceptable Solution “Cryptobox”

- Introduction
- Background
- Requirements
- Software Security
- Interfaces
- Software Identification
- Application
- Software Download



Introduction

Background

Requirements

Software
Security

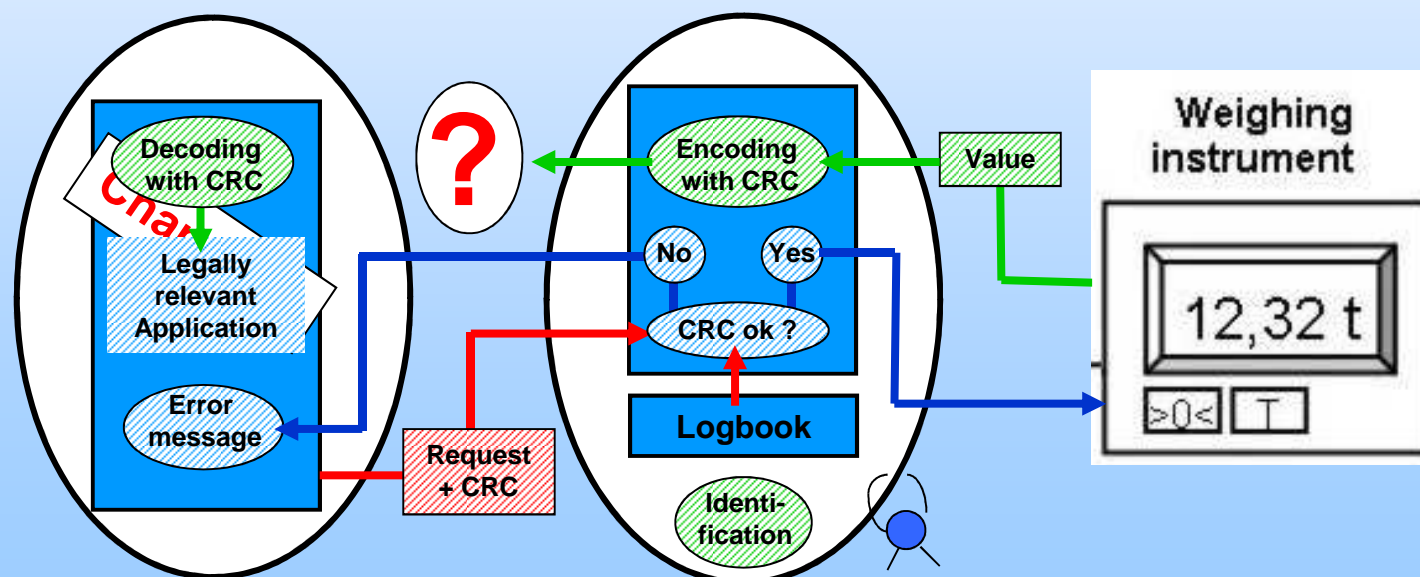
Interfaces

Software
Identification

Application

Software
Download**Software requirement:** (R76, 5.5.2.2)

Evidence of an intervention such as **changing**, uploading or **circumventing** the legally relevant software shall be available until the next verification or comparable official inspection



Introduction

Background

Requirements

Software
Security

Interfaces

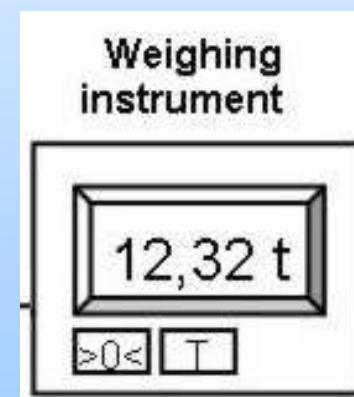
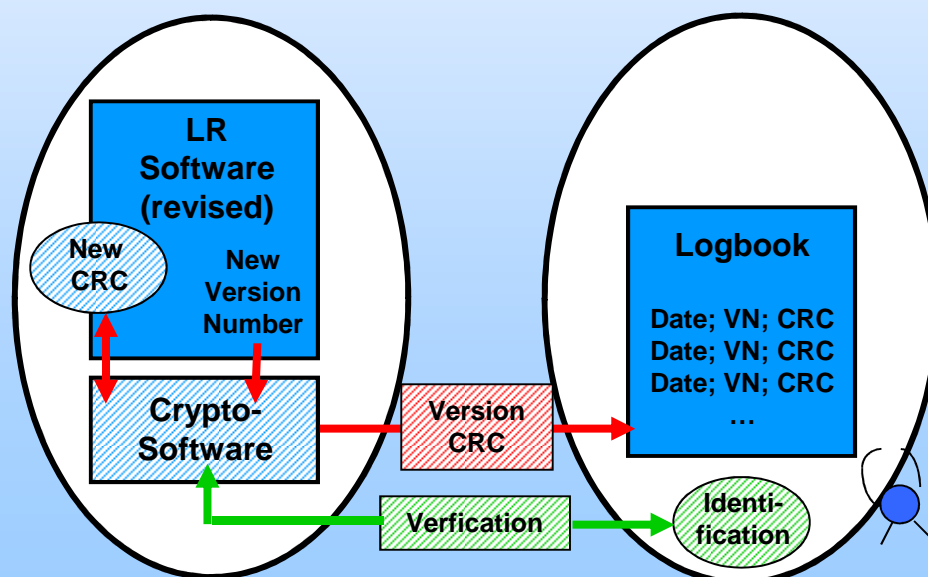
Software
Identification

Application

Software
Download

Software requirement: (R76, 5.5.2.2)

Evidence of an intervention such as changing, **uploading** or circumventing the legally relevant software shall be available until the next verification or comparable official inspection



Introduction

Background

Requirements

Software
Security

Interfaces

Software
Identification

Application

Software
Download



**Thank you very
much for your attention !**