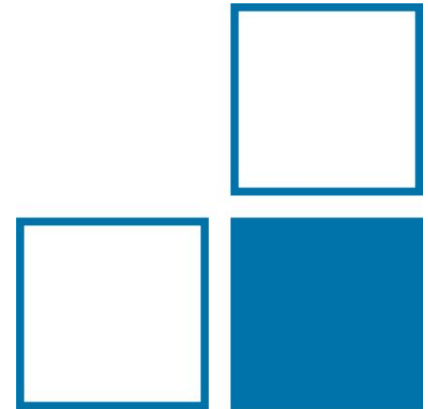


WELMEC 7.2 Software Testing and its Challenges

Daniel Peters, Ulrich Grottke





Braunschweig

1

Mechanics
and
Acoustics

2

Electricity

3

Chemical Physics
and
Explosion Protection

4

Optics

5

Precision
Engineering

6

Ionizing
Radiation

Q

Scientific-technical
Cross-sectional
Tasks

Z

Admini-
strative
Services

Berlin

7

Temperature and
Synchrotron Radiation

8

Medical Physics and
Metrological Information
Technology



Working Fields

- Software testing and quality assurance
- Data communication and security
- IT in legal metrology
- Gaming machines
- Research in Operating Systems and Cloud Computing

Type of activities

- Research and development in metrology
- Testing and type approval
- Advisory activities for industry, associations and government

- Founded November 1990
- European legal metrology
- establish a harmonized and consistent approach
- 37 members
- 8 Working Groups
- WELMEC Working Group 7 “Software”

95-99 % of Measuring Instruments are Software Controlled

■ Advantages:

- Easy to adapt to the needs
- More complex measuring algorithms possible than in hardware
- Robust against physical effects (drift, EMC, ...)
- Easy exchange of data (measurement values) over large distances

■ Disadvantages (from the notified body point of view):

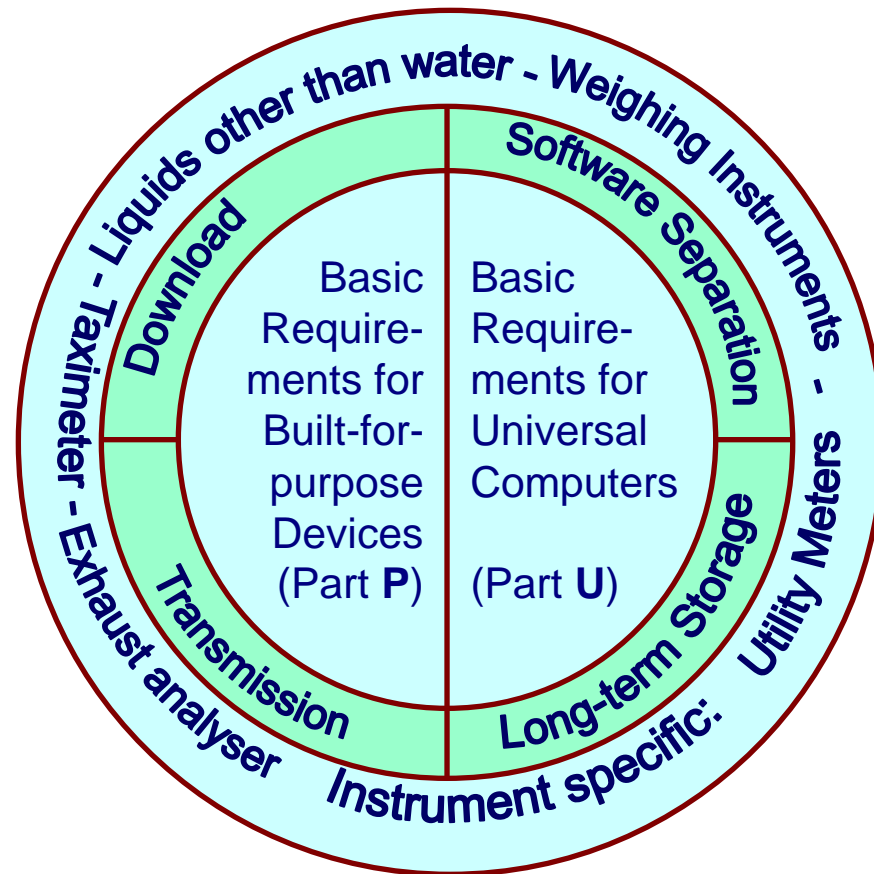
- Specific knowledge besides metrological skills necessary for examination (or at least helpful)
- Because of increased complexity: more effort for examination
- Fraud on measurement values often not obvious: software securing techniques necessary

- **Security and software identification** (MID Annex I, 8.3)
- **Data transmission and data storage** (MID Annex I, 8.4)
- **Interfaces** (MID Annex I, 8.1)
- **Software separation** (MID Annex I, 7.6)

- Structure of the Guide



Risk Classes



Conformity

low: functions identical
middle: selected parts of the software identical
high: whole software identical

		Conformity		
		low	middle	high
Software Protection		A	-	-
	middle	B	C	-
	high	-	D	E
				F

Risk Classes A - F

Protection against manipulation

low: no specific protection means
middle: means against use of wide-spread simple tools (text editors, etc.)
high: state of the art in e-commerce.

amination level

low
middle
high

Examination

low: functional test of the instrument
middle: examination based on functional description of the software (documentation + selected practical tests)
high: examination based on the source code

Conformity:

low: functions identical

Protection against manipulation:

middle: means against use of wide-spread simple tools

Examination:

middle: examination based on functional description of the software (documentation + selected practical tests)

Conformity			
low	middle		high
A	-		-
B	C		-
-	D	E	F

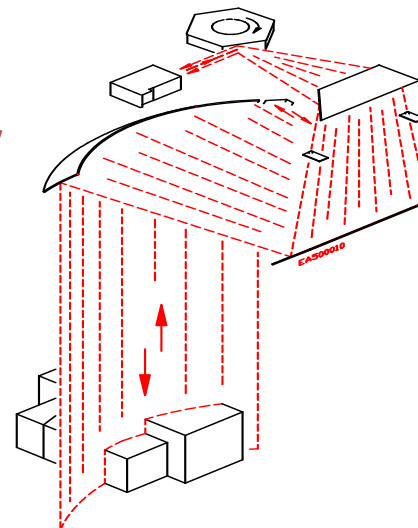
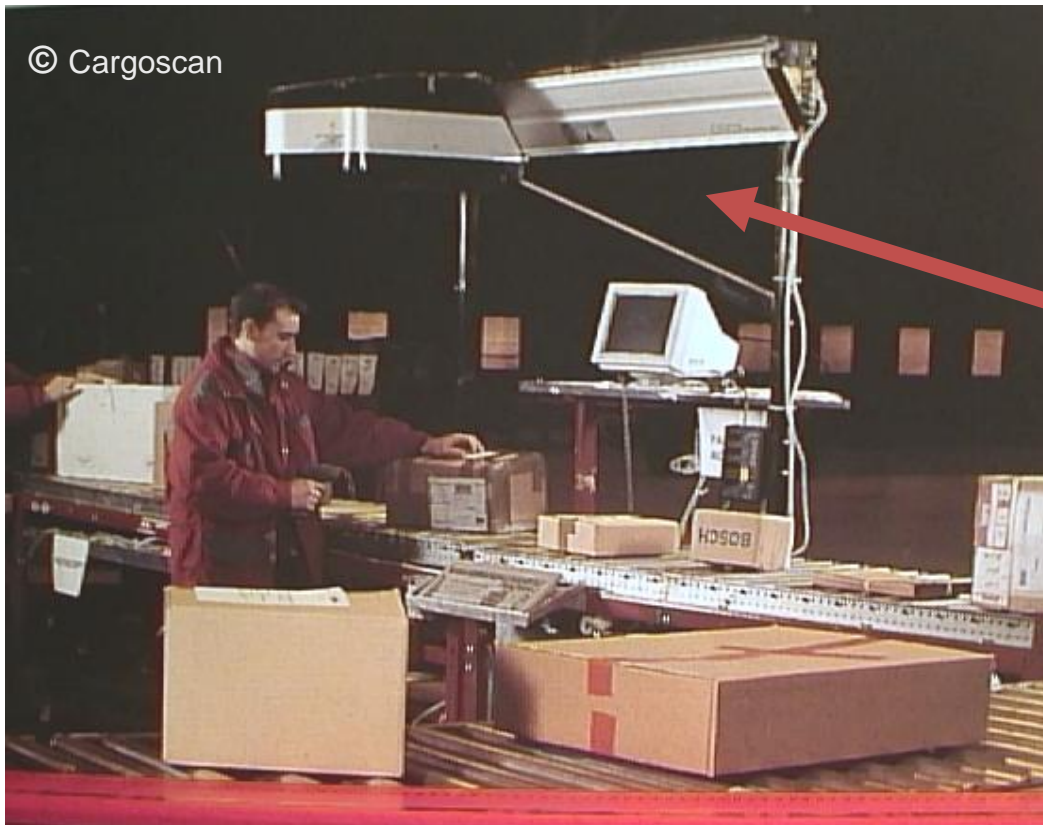
Risk Classes A - F

Examination level	low
	middle
	high

Automatic Balance for the control and surveillance of automatic filling processes



Dimensional Measuring System for Cargo (Laser Scanner)



Conformity:

middle:

selected parts of the software
identical

Protection against manipulation:

middle:

means against use of wide-
spread simple tools

Examination:

middle:

examination based on functional
description of the software
(documentation + selected
practical tests)

Conformity		
low	middle	high
A	-	-
B	C	-
-	D	E
		F

Risk Classes A - F

Examination
level

low
middle
high

Utility Meters



Volume Measurement of Liquids other than Water on Road Tankers



Conformity:

middle:

selected parts of the software identical

Protection against manipulation:

high:

state of the art in e-commerce

Examination:

middle:

examination based on functional description of the software (documentation + selected practical tests)

Conformity		
low	middle	high
A	-	-
B	C	-
-	D	E
		F

Risk Classes A - F

Examination level	low
	middle
	high

Taxameters



© HaLe



© Kienzle Argo



Built-for-Purpose Computer

P1 - Documentation

P2 - Software identification

P3 - Influence via user interfaces

P4 - Influence via communication interface

P5 - Protection against accidental or unintentional changes

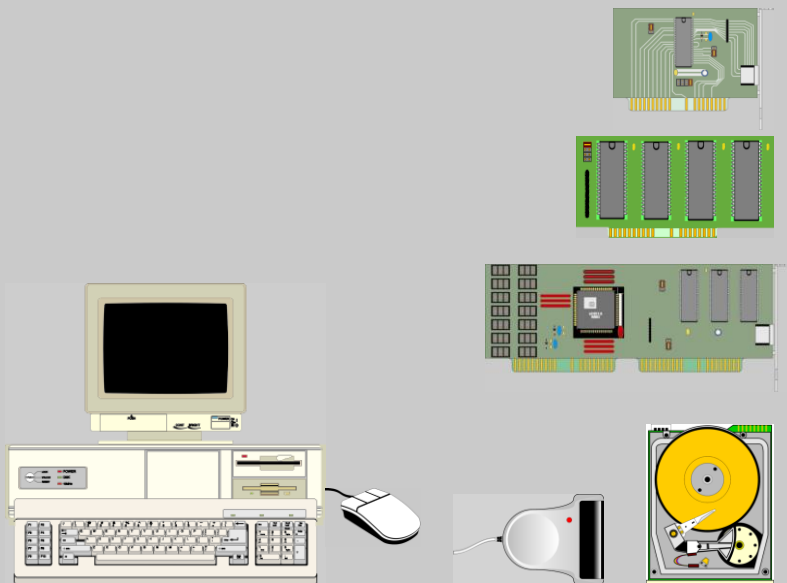
P6 - Program protection against intentional changes

P7 - Parameter protection

- Devices designed for the measuring purpose
- IT components only realise functions for measuring, indication and supporting tasks
- No option of loading software, programming or starting of other software when instrument is in use

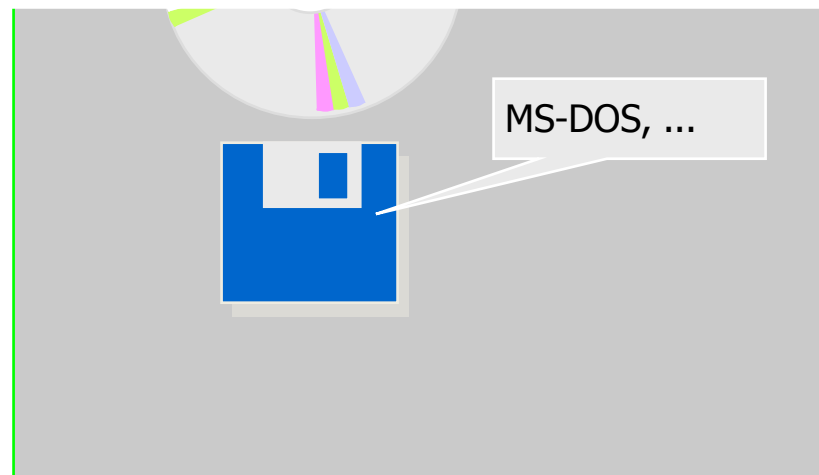
Universal Computer (1990)

Hardware Components



Universal Computer

- U1 - Documentation
- U2 - Software identification
- U3 - Influence via user interfaces
- U4 - Influence via Electronic interface
- U5 - Protection against accidental or unintentional changes
- U6 - Protection against intentional changes
- U7 - Parameter protection
- U8 - Software authenticity and presentation of results
- U9 - Influence of other software

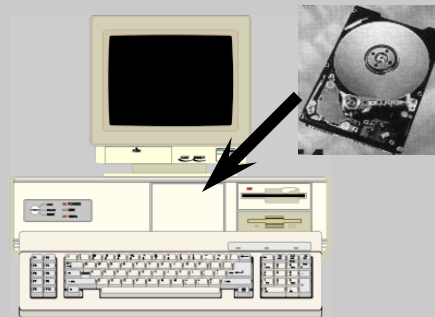


Long-term storages

Integrated storage



Storages in universal computers



Long-term Storage

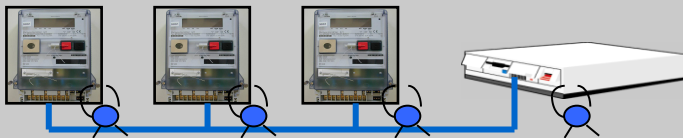
- L1 - Completeness of stored data
- L2 - Protection against accidental or unintentional changes
- L3 - Integrity of data
- L4 - Authenticity of stored data
- L5 - Confidentiality of keys
- L6 - Retrieval of stored data
- L7 - Automatic storing
- L8 - Storage capacity and continuity



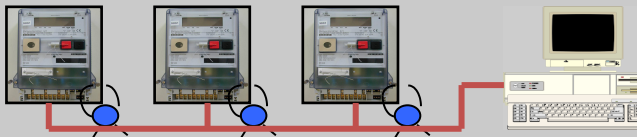
Removable or remote storage

Data transmission

Closed
Network



Network
participants
not subject to
Legal Control



Open
Network

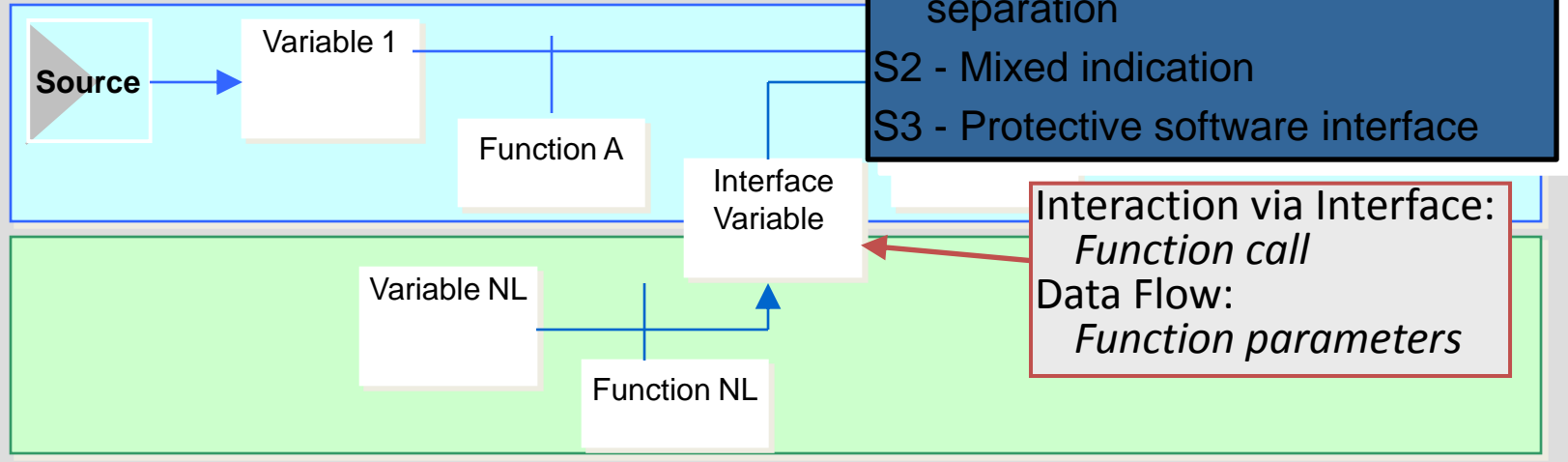


DataTransmission

- T1 - Completeness of transmitted data
- T2 - Protection against accidental or unintentional changes
- T3 - Integrity of data
- T4 - Authenticity of transmitted data
- T5 - Confidentiality of keys
- T6 - Handling of corrupted data
- T7 - Transmission delay
- T8 - Availability of transmission services

Software separation

Low level separation



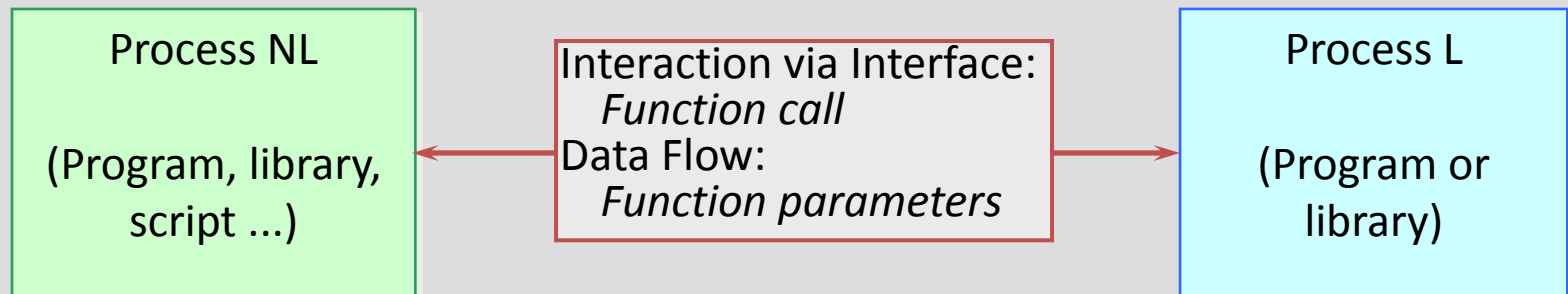
Software Separation

S1 - Realisation of software separation

S2 - Mixed indication

S3 - Protective software interface

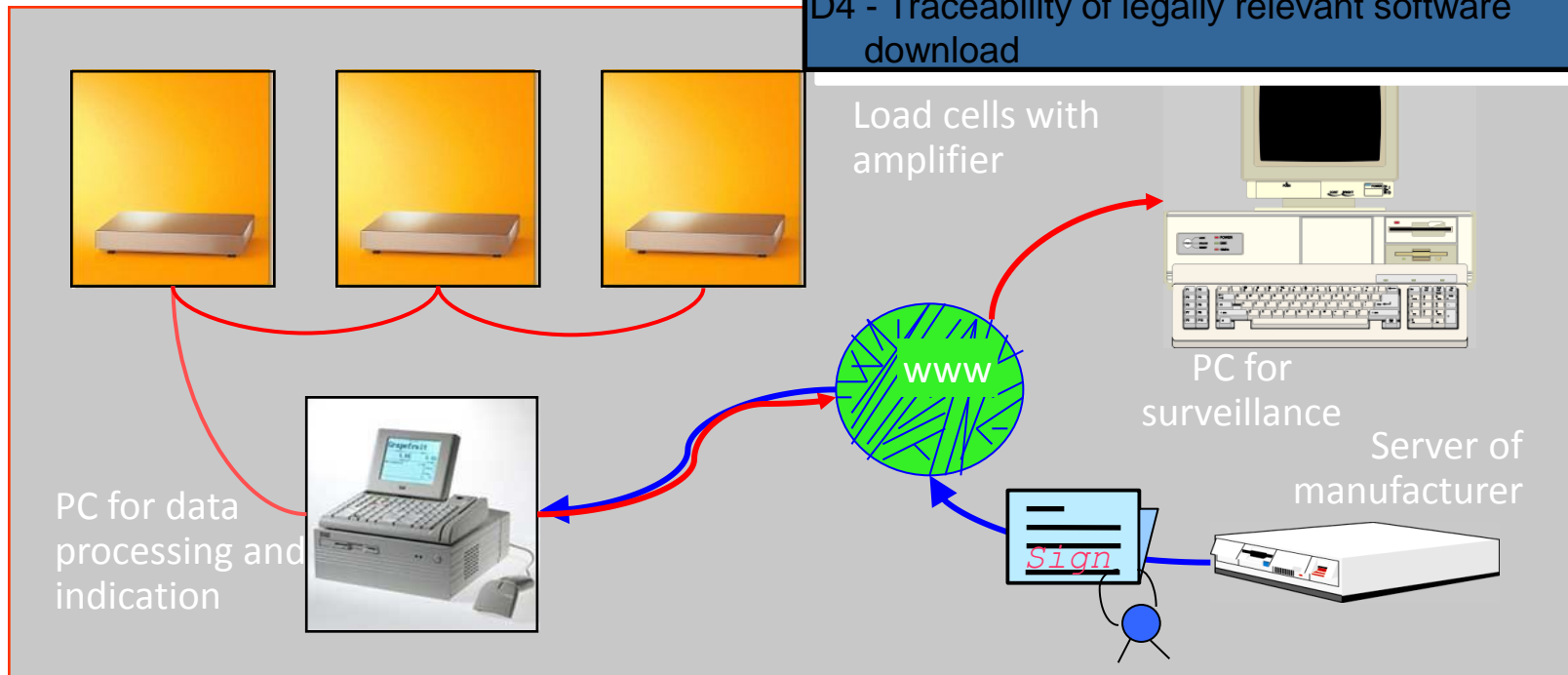
High level separation



Measuring system with download via open

Download

- D1 - Download mechanism
- D2 - Authentication of downloaded software
- D3 - Integrity of downloaded software
- D4 - Traceability of legally relevant software download



- Accent on security-oriented requirements
- No quality requirements for documents (consistency, plausibility, usability)
- Emphasis on simple reviews of documents
- Low quality of documents / software documentation (internal quality, correspondence with product / software implementation)
- Risk to ignore a mismatch between documents and product, especially between software documentation and implementation
- Appropriate risk analysis
- Cost-intensive validations
- software separation in case of using operating systems



**Physikalisch-Technische Bundesanstalt
Braunschweig and Berlin**

Abbestraße 2 - 12

10587 Berlin



Daniel Peters

Telefon: +49 30 3481-7916

E-Mail: daniel.peters@ptb.de

www.ptb.de



Stand: 09/15