243. PTB-Seminar
Anwendung der MID bei Herstellern

Grundlegende Anforderungen an die Software von Messgeräten

Ulrich Grottker
PTB-8.53

- **WELMEC Leitfaden 7.2 „Software“**
  - Risikoklassen
  - Modulares Anforderungssystem
- **Prüfungen**
  - Modul B / Entwurfsprüfung H1
  - Module F, D, H1
- **Zusammenfassung**

- **WELMEC Working Group 7 “Software”**

  Gegründet November 1996

  – 15 Mitglieder (Benannte Stellen)
  – 5 EU-Organisationen
    (Hersteller und Anwender von Messgeräten)
  – 1 Beobachter

- **Sicherheit und Software-Identifikation**

  8.3 Software, die für die messtechnischen Merkmale entscheidend ist, ist entsprechend zu kennzeichnen und zu sichern. Die **Identifikation** der Software muss auf **einfache Weise** vom Messgerät zur Verfügung gestellt werden. Eventuelle **Eingriffe** müssen über einen angemessenen Zeitraum **nachweisbar** sein.

- **Datenübertragung und Datenspeicherung**

  8.4 **Messdaten**, **Software**, die für die messtechnischen Merkmale entscheidend sind und messtechnisch wichtige **Parameter**, die gespeichert oder übertragen werden, sind angemessen **gegen** versehentliche oder vorsätzliche **Verfälschung zu schützen**.

- **Schnittstellen**

  8.1 Die messtechnischen **Merkmale** eines Messgerätes dürfen durch das Anschließen eines anderen Gerätes, durch die Merkmale des angeschlossenen Geräts oder die Merkmale eines abgesetzten Geräts, das mit dem Messgerät in Kommunikationsverbindung steht, **nicht in unzulässiger Weise beeinflusst werden**.

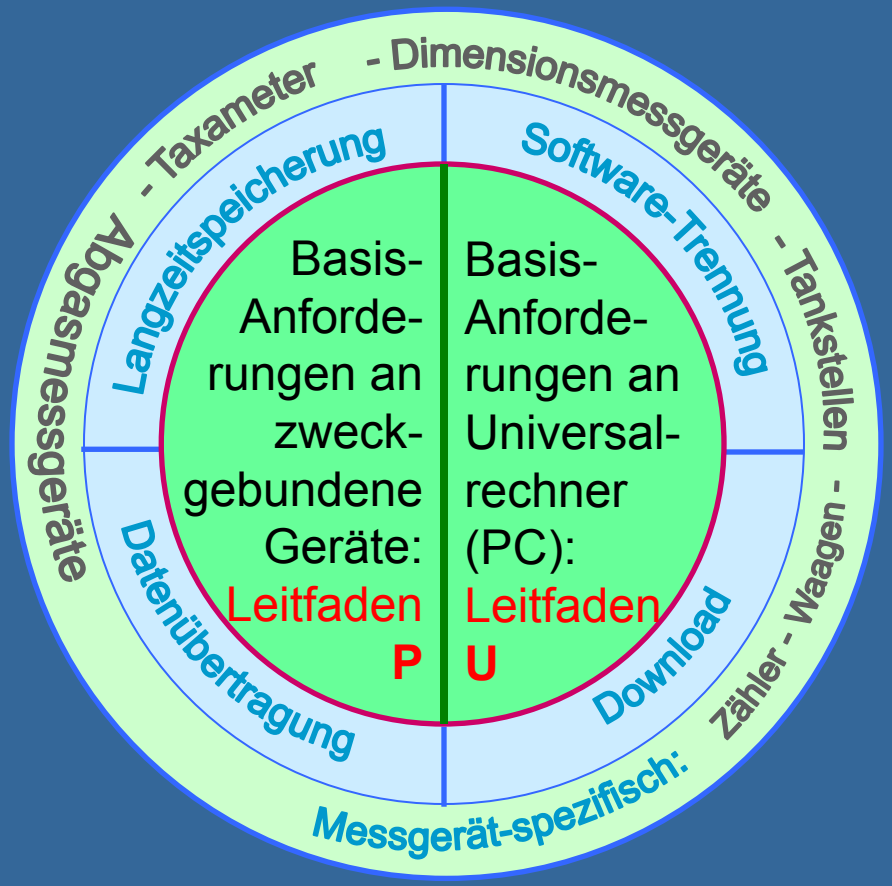
- **Software-Trennung**

  7.6 ... Wenn ein Messgerät über zugehörige **zusätzliche Software** verfügt, die neben der Messfunktion weitere Funktionen erfüllt, muss die für die messtechnischen Merkmale **entscheidende Software identifizierbar** sein; sie darf durch die zugehörige zusätzliche Software **nicht** in unzulässiger Weise **beeinflusst** werden.

Aufbau des Leitfadens

A
B
C
D
E
F

Risiko Klassen



Definition der Risikoklassen

WELMEC

PTB

Konformität

niedrig : Funktionen identisch

mittel: Ausgewählte Softwareteile identisch

hoch: Gesamte Software identisch

Konformität Seriengerät - Baumuster

Manipulationsschutz	niedrig	mittel	hoch
hoch	-	D	E	F
mittel	B	C	-
niedrig	A	-	-

Risikoklassen A - F

Manipulationsschutz

niedrig: keine besonderen Schutzmaßnahmen

mittel: Verwendung von verbreiteten einfachen Werkzeugen (Texteditoren, etc.)

hoch: Stand der Technik im e-Commerce.

üftiefe

niedrig
mittel
hoch

Prüftiefe

niedrig: Funktionaler Test des Gerätes

mittel: Prüfung auf der Basis von Funktionsbeschreibungen (Dokumentation) + ausgewählte praktische Tests

hoch: Prüfung auf der Basis des Quellcodes

Konformität

niedrig : Funktionen identisch

Manipulationsschutz

mittel: Verwendung von verbreiteten einfachen Werkzeugen (Texteditoren, etc.)

Prüftiefe

mittel: Prüfung auf der Basis von Funktionsbeschreibungen (Dokumentation) + ausgewählte praktische Tests

Konformität Seriengerät - Baumuster

Prüftiefe	niedrig	mittel	hoch
niedrig	A	-	-
mittel	B	C	-
hoch	-	D	E / F

Risikoklassen A - F

Beispiele

- Waagen (P), keine Förderbandwaagen
- Abgas (P)
- Dimensionsmessgeräte (P)
- Druck Flüssigkeiten, Gase (national)

PTB

Konformität

mittel: Ausgewählte Softwareteile identisch

Manipulationsschutz

mittel: Verwendung von verbreiteten einfachen Werkzeugen

Prüftiefe

mittel: Prüfung auf der Basis von Funktionsbeschreibungen (Dokumentation) + ausgewählte praktische Tests

Konformität Seriengerät - Baumuster

Prüftiefe	niedrig	mittel	hoch
niedrig	A	-	-
mittel	B	C	-
hoch	-	D	E / F

Risikoklassen A – F

Beispiele

- Zähler
- Waagen (U), Förderbandwaagen
- Flüssigkeiten außer Wasser (U)
- Taxameter (P)
- Dimensionsmessgeräte (U)
- Abgas (U)
- Getreidefeuchte (national)
- Kalorimeter (national)

Konformität

mittel: Ausgewählte Softwareteile identisch

Manipulationsschutz

hoch: Stand der Technik im e-Commerce.

Prüftiefe

mittel: Prüfung auf der Basis von Funktionsbeschreibungen (Dokumentation) + ausgewählte praktische Tests

Konformität Seriengerät - Baumuster

Prüftiefe	niedrig	mittel	hoch
niedrig	A	-	-
mittel	B	C	-
hoch	-	D	E	F

Risikoklassen A - F

Beispiele

- Taxameter (U)

National:

- Messsysteme mit Speicherung / Datenübertragung nach PTB-A50.7

Konformität

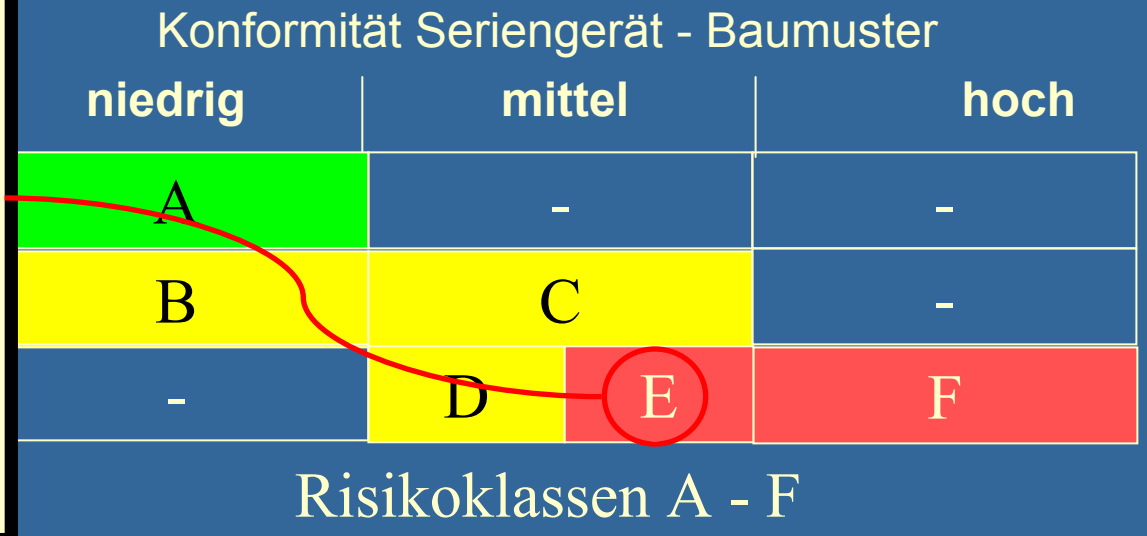
mittel: Ausgewählte Soft-wareteile identisch

Manipulationsschutz

hoch: Stand der Technik im e-Commerce.

Prüftiefe

hoch: Prüfung auf der Basis des Quellcodes



Beispiel

- Choirometer (national)

WELMEC

PTB

Konformität

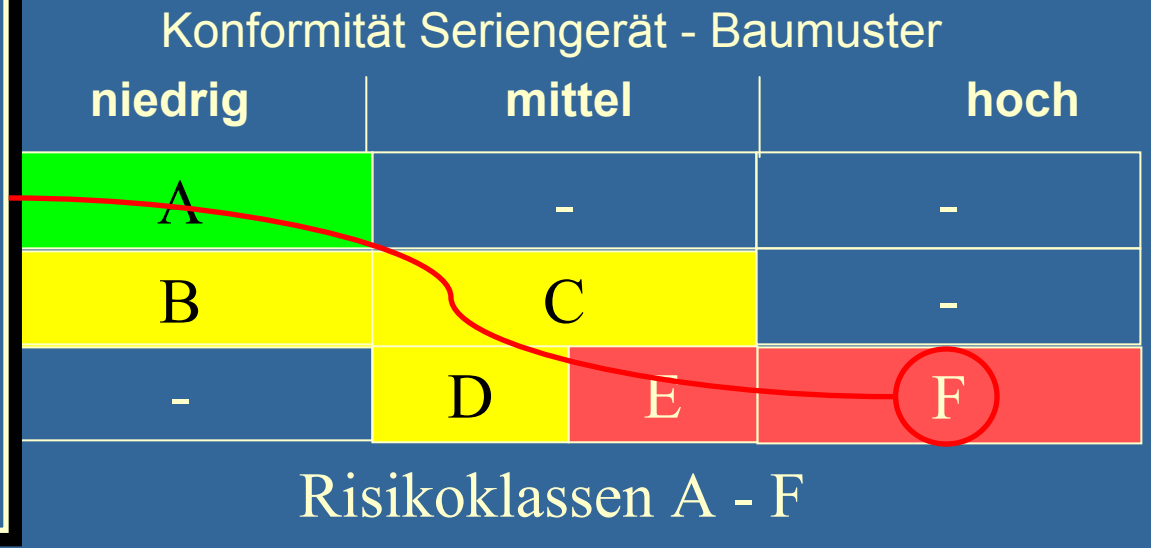
hoch: Gesamte Software identisch

Manipulationsschutz

hoch: Stand der Technik im e-Commerce.

Prüftiefe

hoch: Prüfung auf der Basis des Quellcodes



Prüftiefe

niedrig
mittel
hoch

Beispiel

- Geschwindigkeits-messgeräte (national)

WELMEC

PTB

P-Gerät (Built-for-Purpose Device), “Gesamtgerät”

Elektrizitätszähler, Abgasmessgerät, Taxameter, Waage, ...

- Für den Messzweck konstruierte Geräte
- Eingebettete IT-Komponenten realisieren nur Mess- und Anzeigefunktionen
- Keine Möglichkeit für den Benutzer zum Programmieren oder Betreiben anderer Software

P-Gerät (Built-for-Purpose

Elektrizitätszähler, Abgasmessg

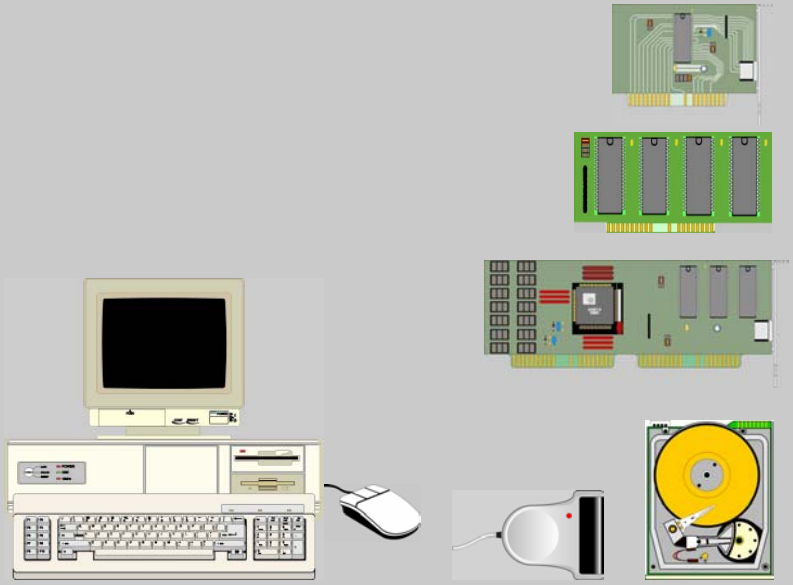
Anforderungen: Zweckgebundener Computer

P1 – Dokumentation
P2 – Software-Identifikation
P3 – Nutzer-Interface
P4 – Kommunikationsinterface
P5 – Schutz gegen zufällige Veränderungen
P6 – Schutz gegen beabsichtigte Software-änderungen
P7 – Parameterschutz

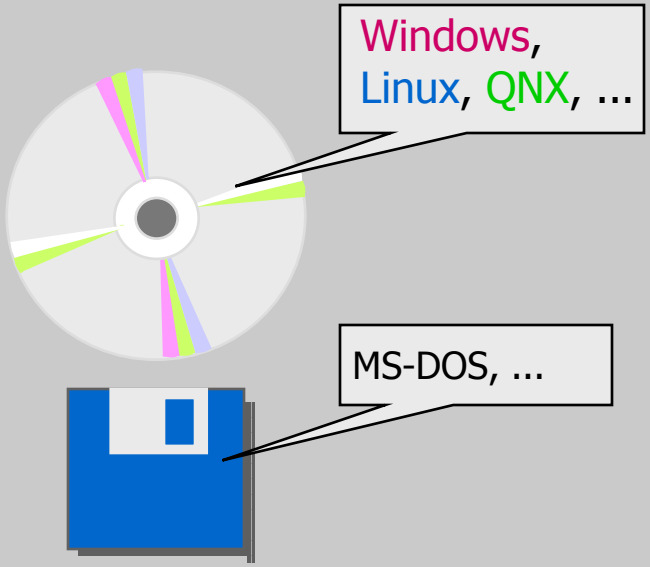
- Fü
- Ei
  nur Mess- und Anzeigefunktionen
- Keine Möglichkeit für den Benutzer zum Programmieren oder Betreiben anderer Software

Universal Computer als Bestandteil des Messsystems

Hardware Komponenten

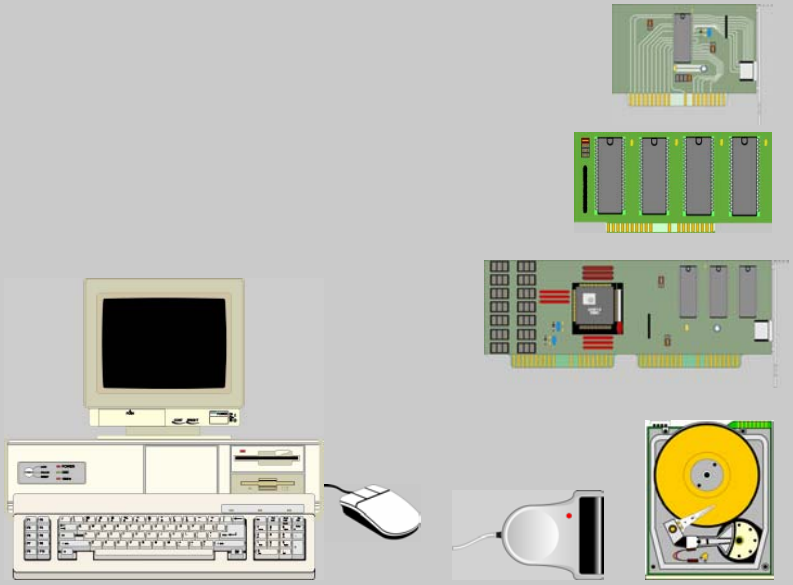


Software Komponenten



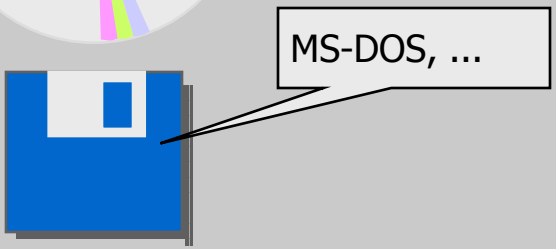
Universal Computer als Bestar

Hardware Komponenten



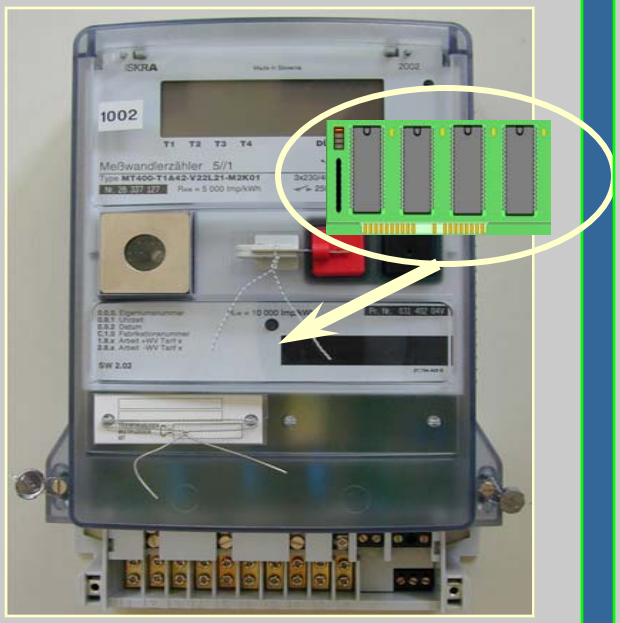
Anforderungen: Universal Computer

U1 – Dokumentation
U2 – Software Identifikation
U3 – Nutzerinterfaces
U4 – Kommunikationsinterface
U5 – Schutz gegen zufällige Veränderungen
U6 – Schutz gegen absichtliche Softwareänderungen
U7 – Parameterschutz
U8 – Software Authentizität und Darstellung von Messergebnissen
U9 – Einfluss von anderer Software

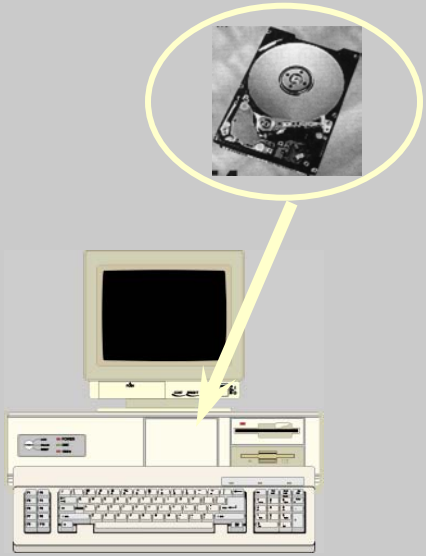


Ausführungen von Langzeitspeichern

Integrierte Speicher



Speicher in Universal-Computern

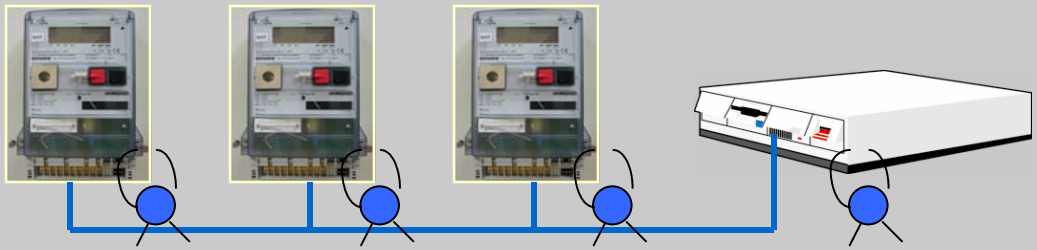


Entnehmbare oder dezentrale Speicher

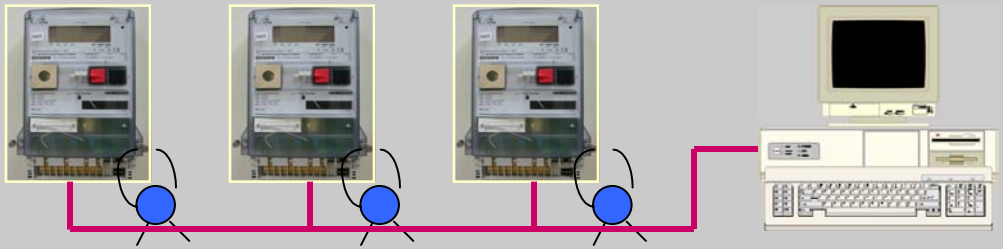
Netzwerk-Topologien zur Datenübertragung

PTB

Geschlossenes Netzwerk



Netzwerk mit nicht eichpflichtigen Teilnehmern



Offenes Netzwerk

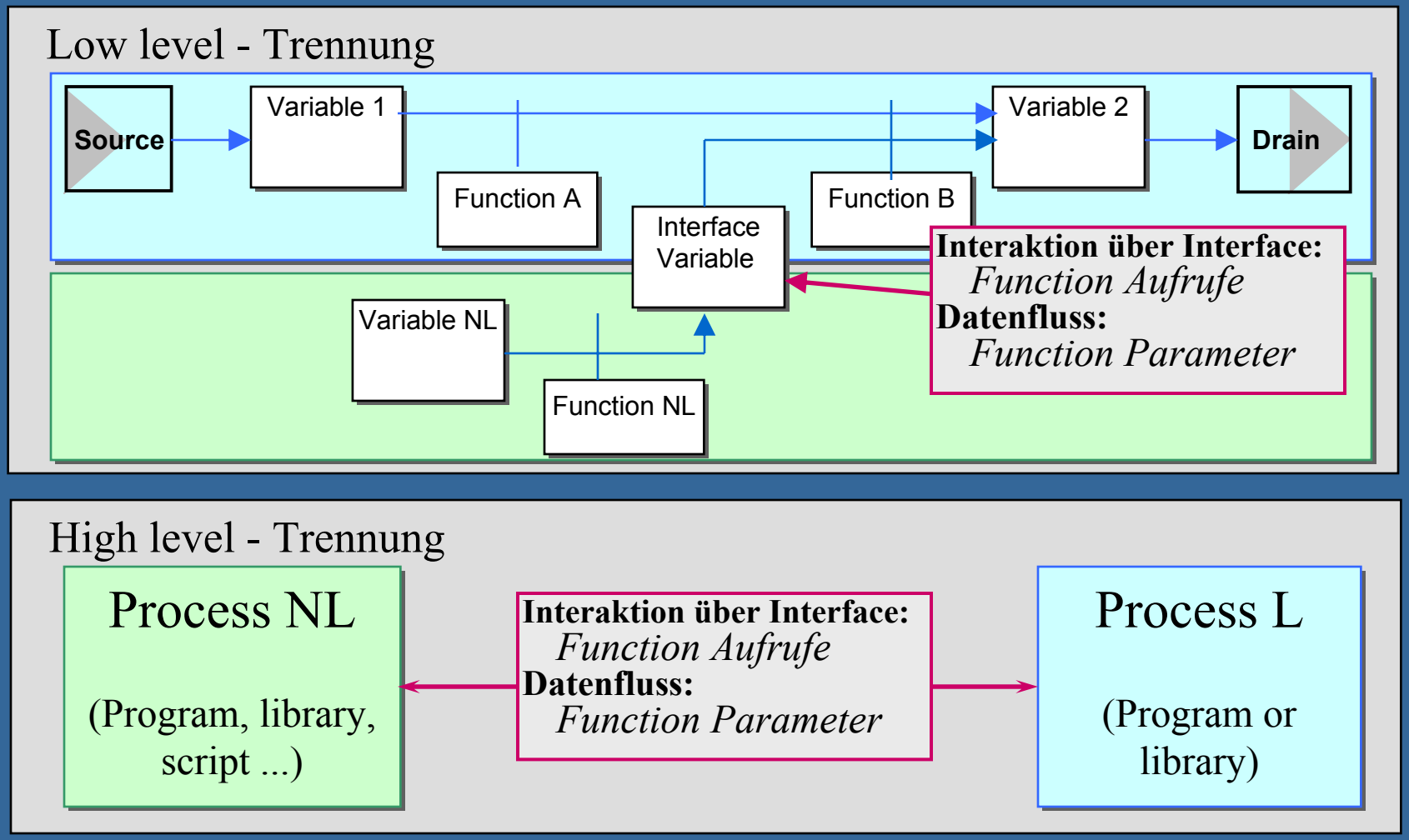
Anforderungen zur Langzeitspeicherung und Übertragung

PTB

L1 / T1: Vollständigkeit der gespeicherten oder übertragenen Daten	
L2 / T2: Schutz gegen zufällige und unbeabsichtigte Veränderungen	
L3 / T3: Integrität der Daten	
L4 / T4: Authentizität der gespeicherten oder übertragenen Daten	
L5 / T5: Vertraulichkeit der Schlüssel	
L6: Rückgewinnung der gespeicherten Daten	T6: Umgang mit verfälschten Daten
L7: Automatisches Speichern	T7: Übertragungsverzögerung
L8: Speicherkapazität und -Kontinuität	T8: Verfügbarkeit der Übertragungsdienste

Softwaretrennung

PTB



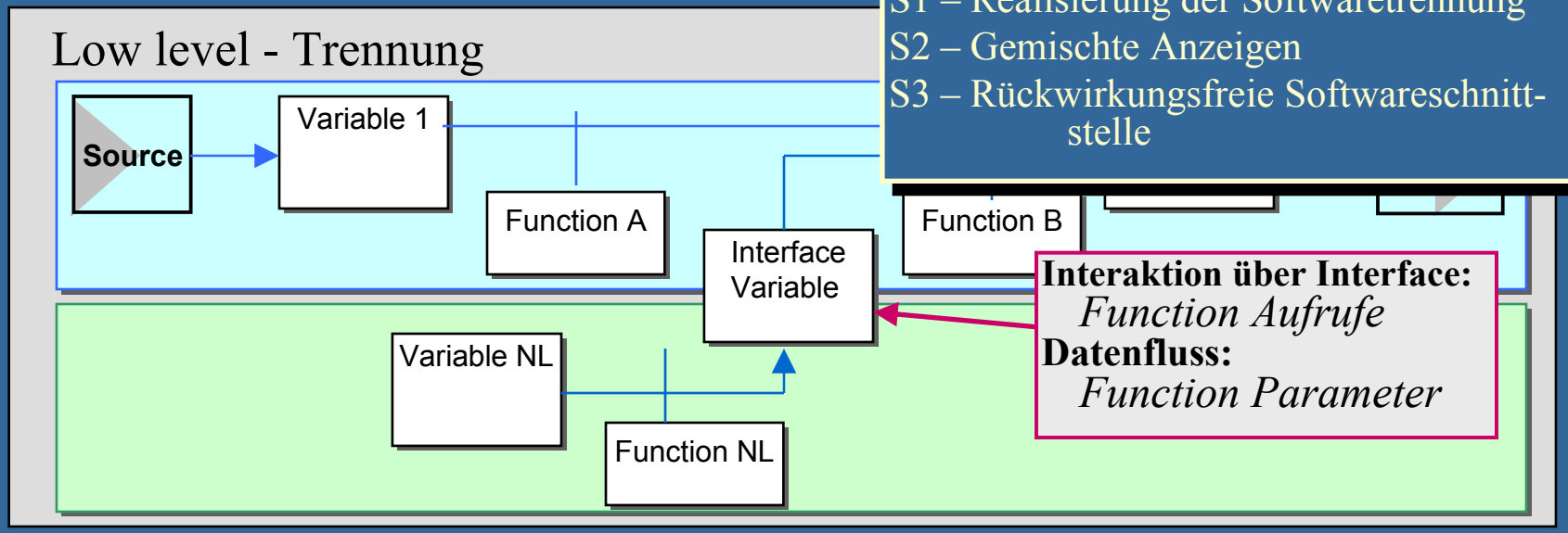
Softwaretrennung

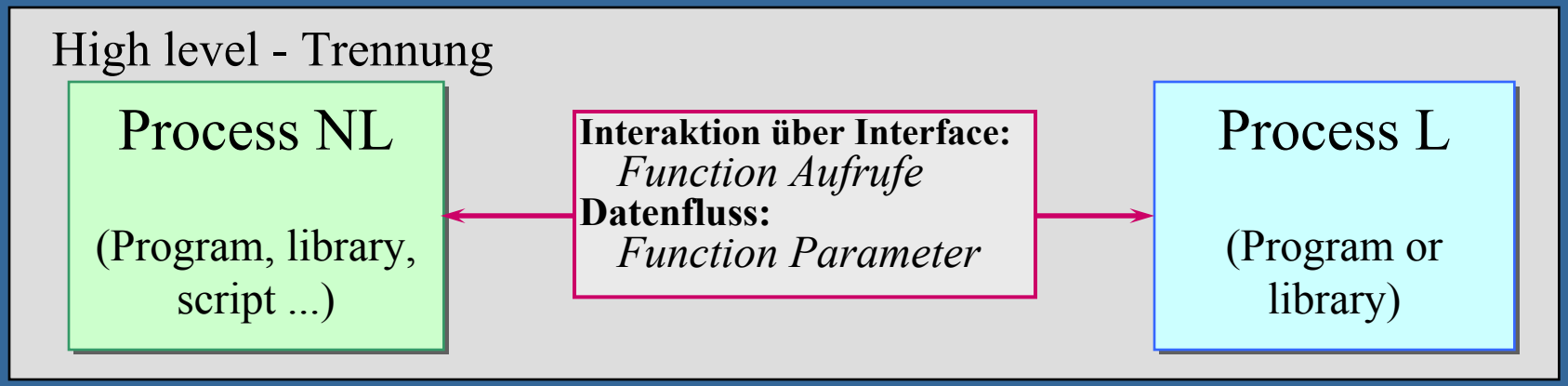
Anforderungen: Softwaretrennung

S1 – Realisierung der Softwaretrennung

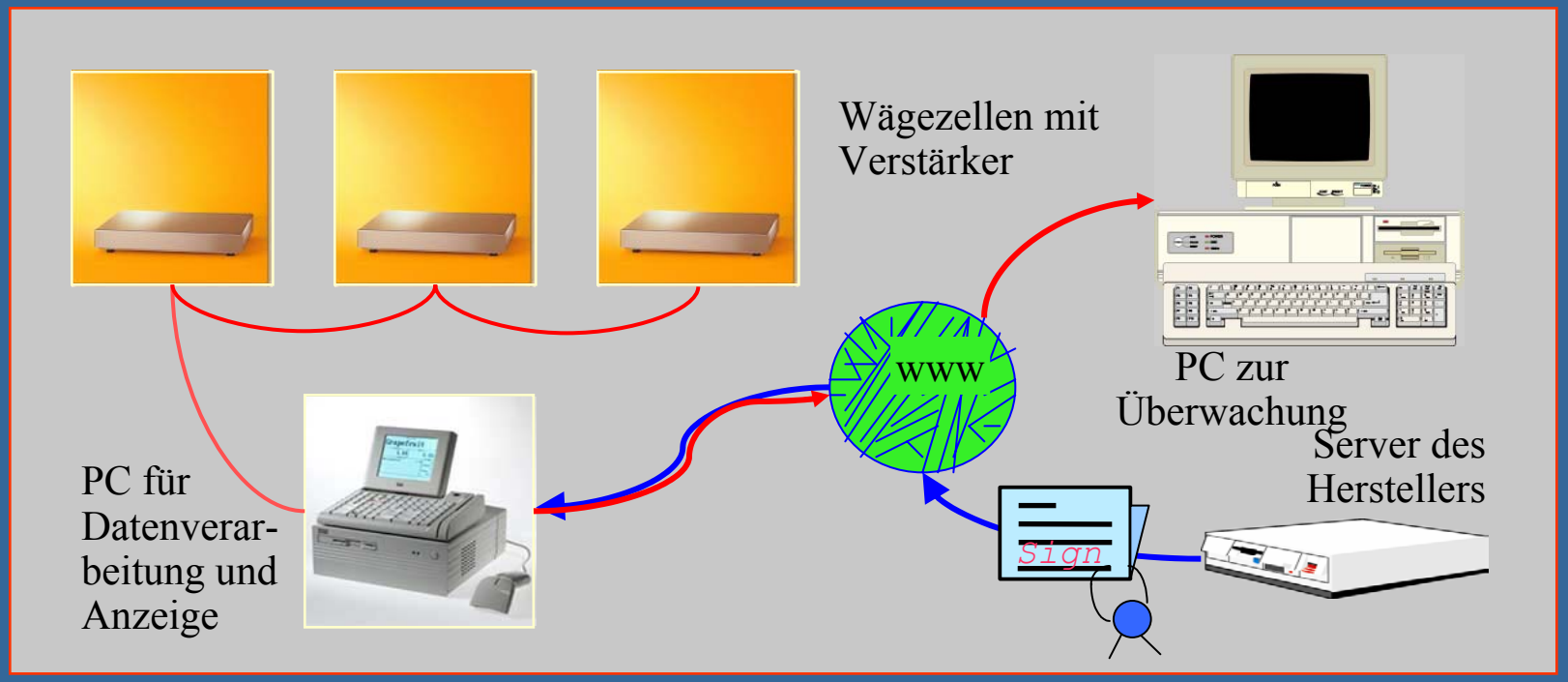
S2 – Gemischte Anzeigen

S3 – Rückwirkungsfreie Softwareschnitt-stelle





Messsystem mit Download über offene Netzwerke



Messsystem mit Download über

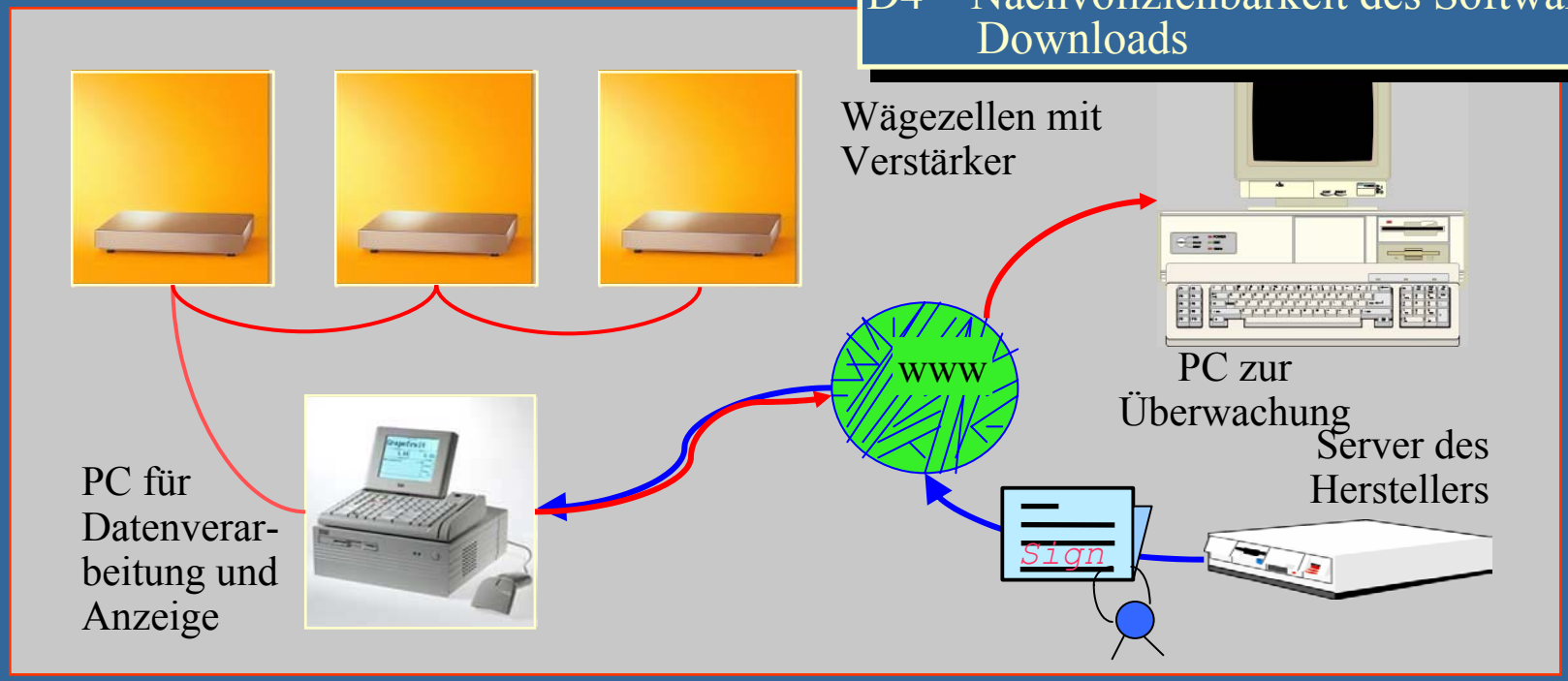
Anforderungen: Download

D1 – Download Mechanismus

D2 – Authentifizierung geladener Software

D3 – Integrität geladener Software

D4 – Nachvollziehbarkeit des Software-Downloads



WELMEC

PTB

- **Anforderungen an:**
  - Versorgungsmessgeräte, Waagen, Taxameter

- **Anforderungen (hier Versorgungsmessgeräte):**
  - Erholung nach Fehlern
  - Datenrettung bei Fehlern
  - Kein Reset kumulativer Register
  - Ausreichende interne Auflösung der Register
  - Keine Beeinflussung des dynamischen Verhaltens durch nicht eichpflichtige Software
  - Batterie-Lebenszeit
  - Mengenumwerter
  - Testelement

- **WELMEC Leitfaden 7.2 „Software“**
  - Risikoklassen
  - Modulares Anforderungssystem
- **Prüfungen**
  - Modul B / Entwurfsprüfung H1
  - Module F, D, H1
- **Zusammenfassung**

Abk.	Beschreibung	Anwendung	Voraussetzungen	Spezielle Fähigkeiten
AD	Analyse von Dokumenten	Immer	Dokumentation	-
VFTM	Validation durch Testen der Funktion und der metrologischen Eigenschaften	Richtigkeit des Algorithmus', Messunsicherheit, Kompensationen und Korrekturalgorithmen	Dokumentation, Bauartmuster	-
VFTSw	Validation durch Testen der Funktion von Softwarelösungen	Bedienung durch den Nutzer, richtige Funktionieren von Kommunikation, Anzeige, Manipulationsschutz	Dokumentation, Bauartmuster, Hilfsmittel wie Hex- oder Texteditor	-
DFA	Metrologische Datenflussanalyse	Softwaretrennung, Bewertung des Einflusses von Befehlen auf die Messgerätfunktionen	Quellcode, Texteditor	Programmier-sprachen
CIWT	Code inspection, Walkthrough	Alle Zwecke	Quellcode, Texteditor	Programmier-sprachen
SMT	Testen von Software-Modulen	Alle Zwecke, wenn Eingangs- und Ausgangswerte klar definiert werden können.	Quellcode, Test-umgebung, beson-dere Software-Werkzeuge	Programmier-sprachen. Anweisung zur Benutzung von Werkzeugen

P-Gerät (Built-for-Purpose

Elektrizitätszähler, Abgasmessg

- Fü
- Ei
- Mes- und Anzeigefunktionen
- Keine Möglichkeit zum Laden, Programmieren oder Betreiben anderer Software

Anfor **Zweckgebauter Computer**

P1 – Doku on
P2 – Softwa ntifikation
P3 – Nutzer-In face
P4 – Kommunik tionsinterface
P5 – Schutz gegen zufällige Veränderun
P6 – Schutz gegen beabsi Softwa-änderungen
P7 – Parameterschutz

AD
VFTSw
VFTSw
VFTSw
AD
VFTSw
DFA
CIWT

- Prüfungen an jedem einzelnen Gerät vor dem In-Verkehr-Bringen

- Prüfschritte (Beispiele):
  - Soll-Ist-Vergleich Software-Identifikation (Versionenkontrolle: Nur die zugelassenen Softwaremodule aufspielen)
  - Kontrolle, dass nicht eichpflichtige Softwareteile die Regeln der Softwaretrennung einhalten
  - Aktivierung des Justage-Schutzes
  - usw.

- Prüfschritte im Modul B Prüfzertifikat beschrieben
  - Versuch der europäischen Harmonisierung

WELMEC

PTB

- Verwendung des WELMEC Leitfadens 7.2 sichert Konformität mit MID
- Anwendbar auf breites Spektrum von Messsystemen
- Software bei Prüfung nach Modulen D, F berücksichtigen

Vielen Dank für Ihre Aufmerksamkeit!