Möglichkeiten zum Nachweis der Unversehrtheit von Daten

– Einführung in die Problematik –

Norbert Zisky
Physikalisch-Technische Bundesanstalt

246. PTB-Seminar: Revisionssicheres System zur Aufzeichnung von Kassenvorgängen und Messinformationen

„Eins ist sicher:
Nichts ist sicher, und
nicht einmal das ist
sicher.“

Joachim Ringelnatz

Physikalisch-Technische Bundesanstalt Braunschweig und Berlin

1887- 2009

Dr. Norbert Zisky

Leiter der AG 8.52
„Datenübertragung und -sicherheit“

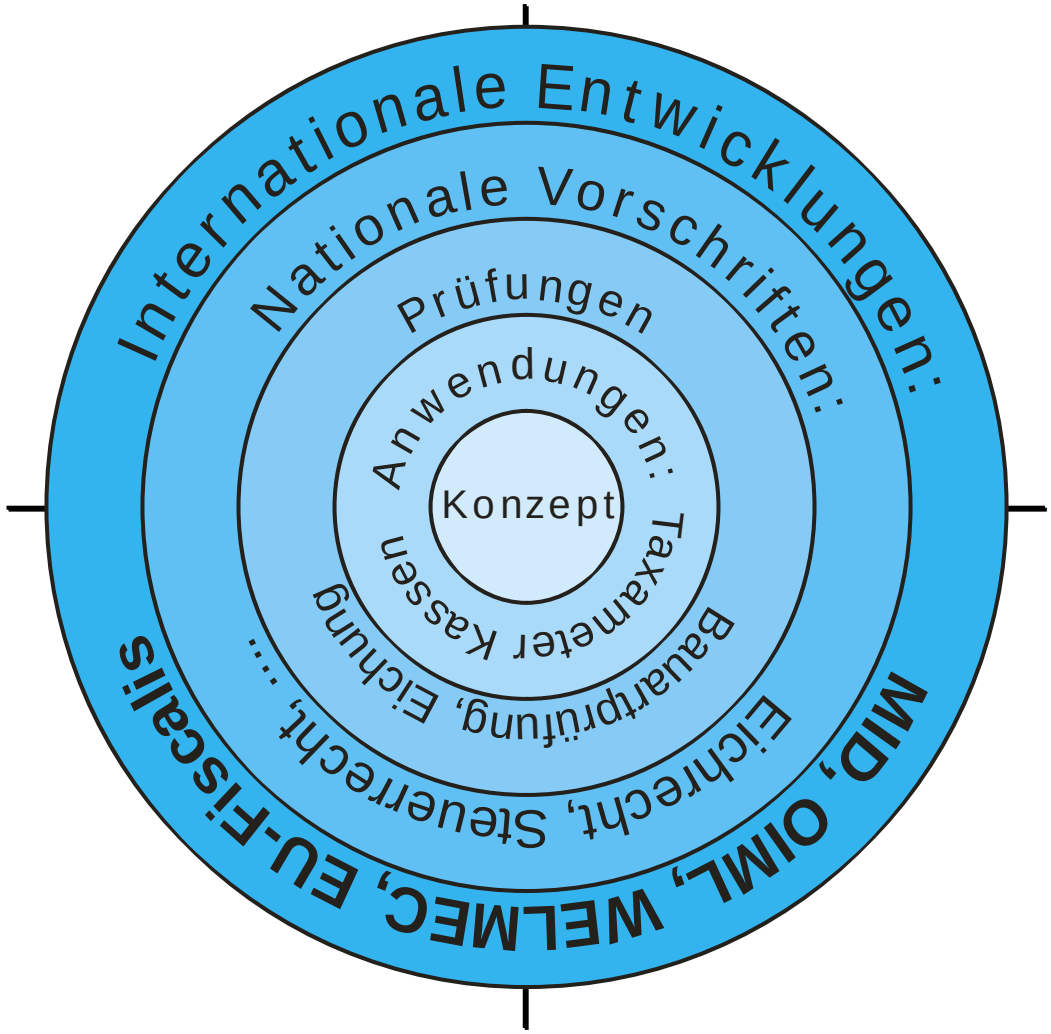
Wichtige Gremien

- VDI/VDE FA 9.1 „Messverfahren in der Informationstechnik“
- Obmann beim DIN NA Tank „Schnittstellen“
- Mitarbeiter beim DIN NA Technische Grundlagen „Schnittstellen“

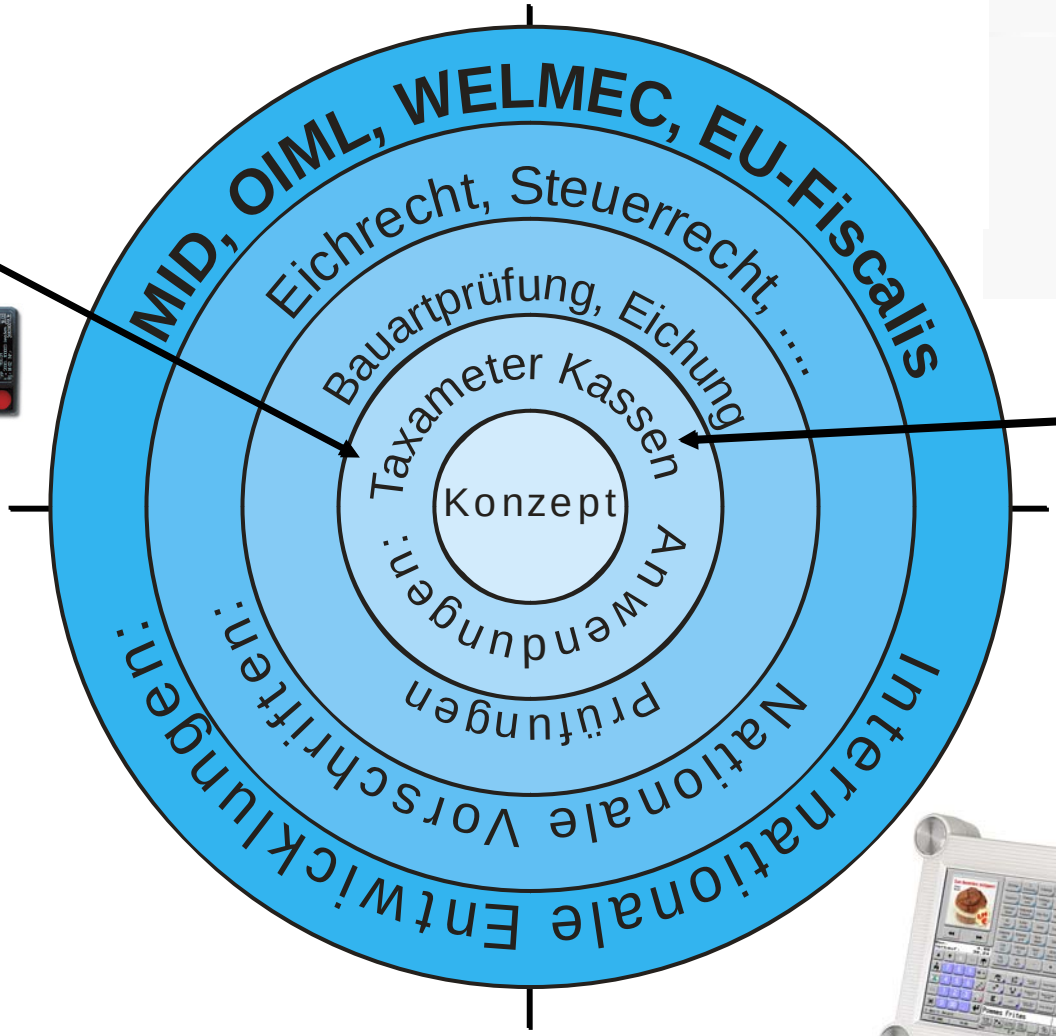
Übersicht

- Rahmen und Ziel des Symposiums
- Grundthesen
- Systemarchitektur
- Modell
- Ausblick

Der Rahmen und das Ziel



Anwendungen



Ziele des Seminars

- Information über ein für Kassen neuartiges Sicherungskonzept
- Diskussion der Übertragbarkeit auf Messsysteme
- Ausloten von Synergien aus den verschiedenen Systemumfeldern

Grundthesen

- Mit klassischen Sicherungsverfahren können moderne IT-Systeme kaum noch geschützt werden
- Geldwerte Transaktionen sind besonders bedroht
- Komplexe Systeme erschweren den Funktionsnachweis definierter Schutzanforderungen
- Jedes System ist angreifbar → Jede Sicherheitsanalyse und jedes darauf aufbauende Sicherheitskonzept muss ein Restrisiko ausweisen

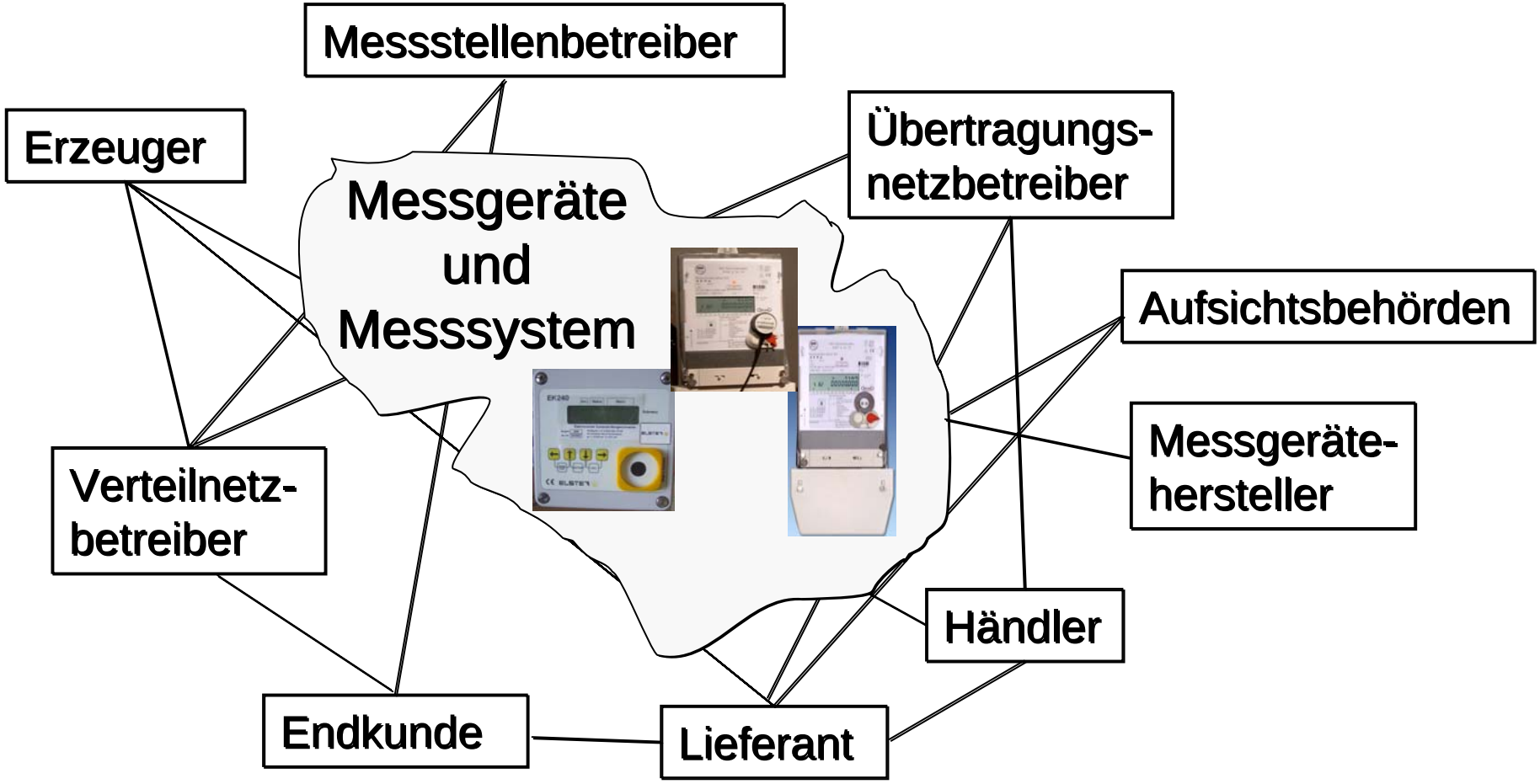
Revisionssichere Systeme

- Kontroverse Diskussion
- Einmal korrekt erfasste Daten können nicht mehr unerkannt verändert werden
- Die Korrektheit der Datenerfassung ist nachweisbar und hält jeder Prüfung stand

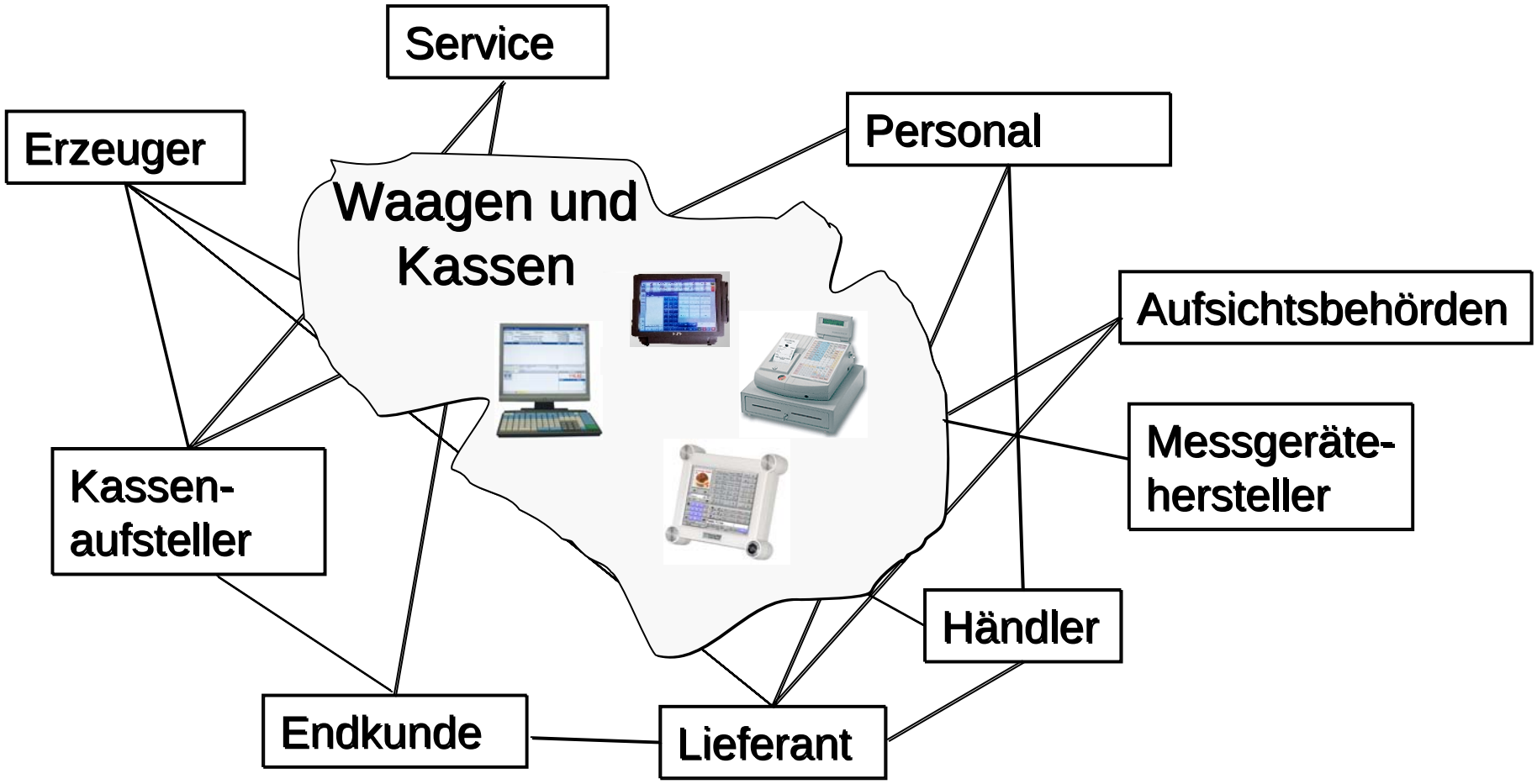
Systemumfeld

- Isolierte Sicherheitsbetrachtungen eines Systems sind wenig Erfolg versprechend
- Identifizierung des Systemumfelds und der Marktteilnehmer
- Neben den technischen Analysen und daraus abgeleiteten Maßnahmen, müssen alle Marktteilnehmer betrachtet und deren gegenseitige Wechselwirkung im Sicherheitssystem beachtet werden

Systemumfeld Beispiel: Energiemarkt



Systemumfeld Beispiel: Handel



Systemumfeld und Bedrohungen

- Externe Zugriffe:
  Eingaben, Prozesse, Informationen, Ausgaben
- Verfälschungen und Angriffe:
  zufällige oder systematische Verfälschungen:
  Technische Fehler, äußere Störungen
  passive und aktive Angriffe

Umsatzzahlen Systeme (Schätzwerte)

- 40 Millionen Elektrozähler→16 Mrd. Euro >>
- 2 Millionen Kassen → 500 Mrd. Euro <<
- 50 000 Taxameter → 2 Mrd. Euro
- 15 000 Tankstellen →
  50 000 Zapfsäulen??→75 Mrd >>

Alle angegebenen Geldbeträge sind sehr grobe Schätzungen ohne Quelle

Verfälschungen

- Was soll nachgewiesen werden
  - Intern gespeicherte richtige Daten sind unverändert
- Zeitpunkt der Verfälschung
  - Es werden nie richtige Daten gebildet
  - Unmittelbar nach Generierung
  - Viel später

Folgen von Verfälschungen

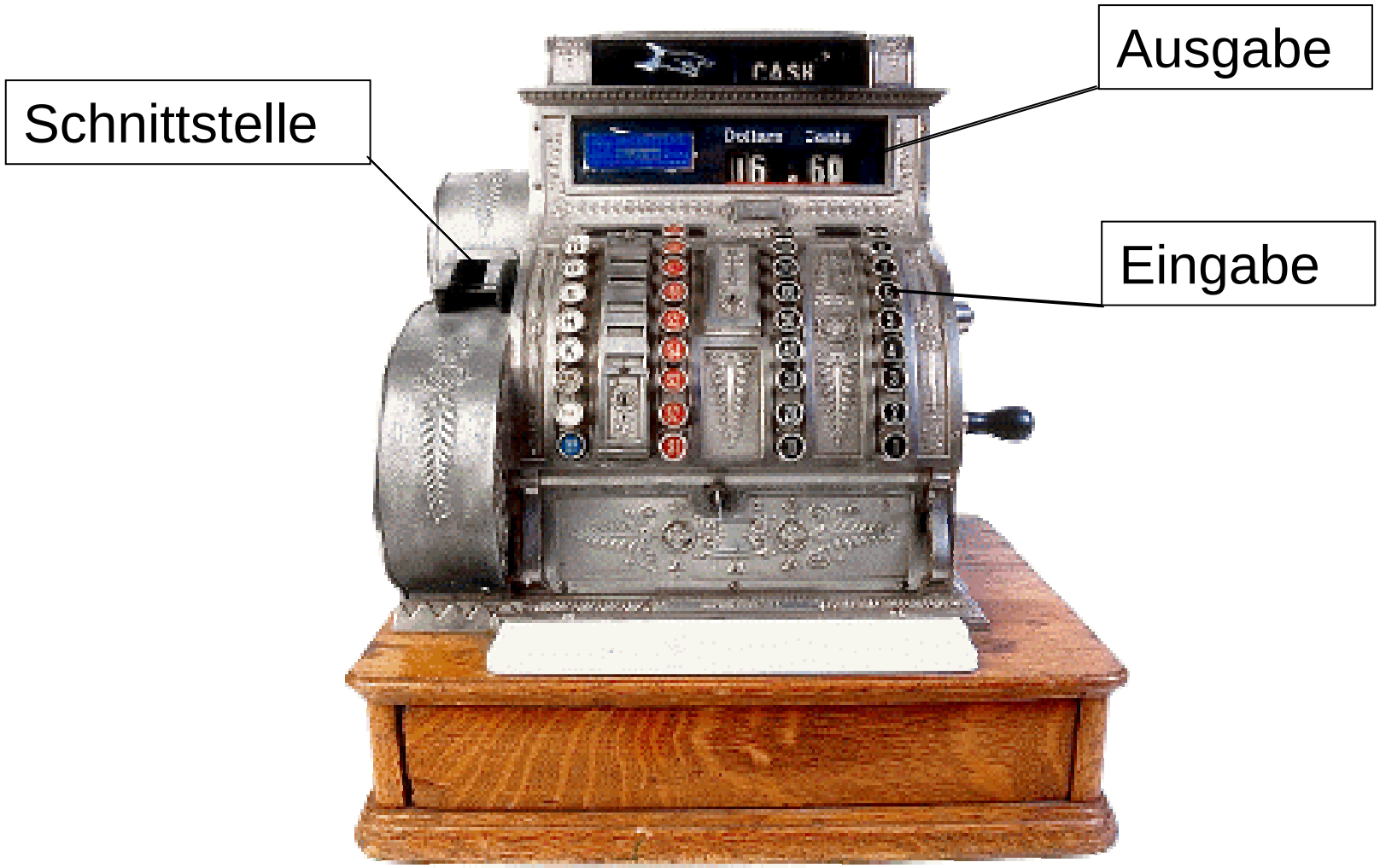
- Schädigung von Einzelpersonen oder Personengruppen
- Vorteilsnahme von Einzelpersonen oder Gruppen
- Wettbewerbsverzerrungen

Sicherheitsziele

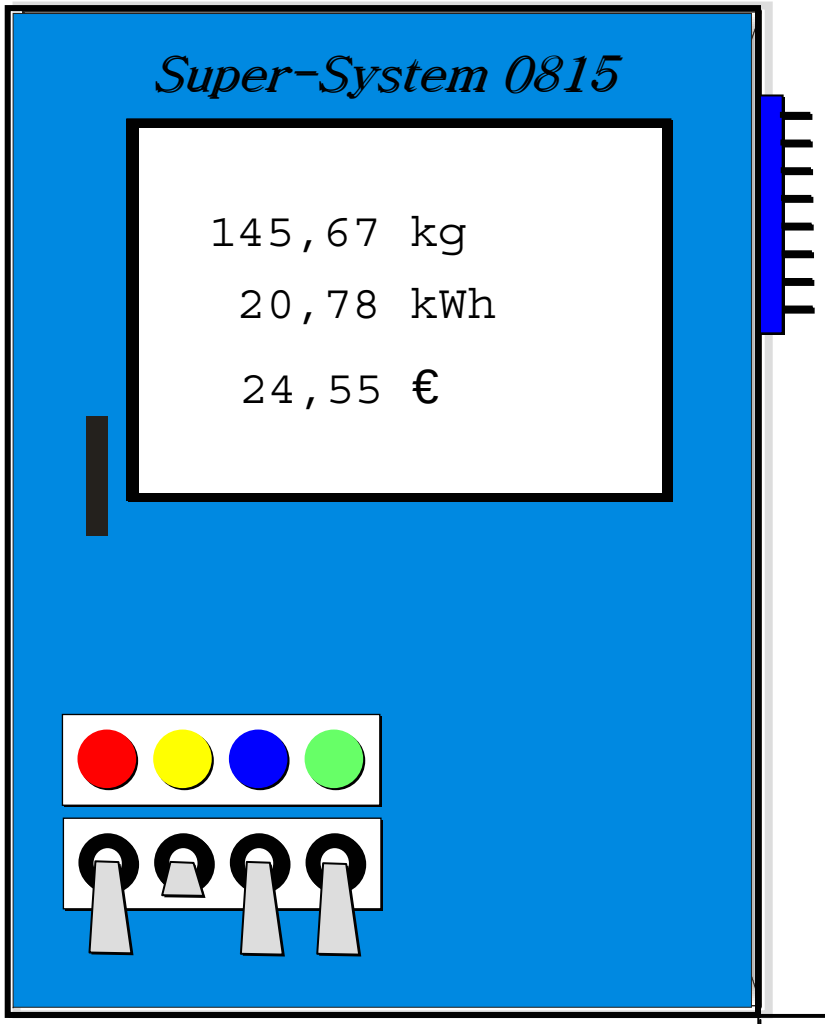
Sicherung sensibler Daten gegen
bewußte oder unbewußte Verfälschungen

- Vollständige, richtige, geordnete und zeitgerechte Aufzeichnung
- Verfälschungen von Daten sollen sicher erkannt werden
- Überprüfbarkeit von Aufzeichnungen auf Vollständigkeit und Richtigkeit durch zuständige Stellen

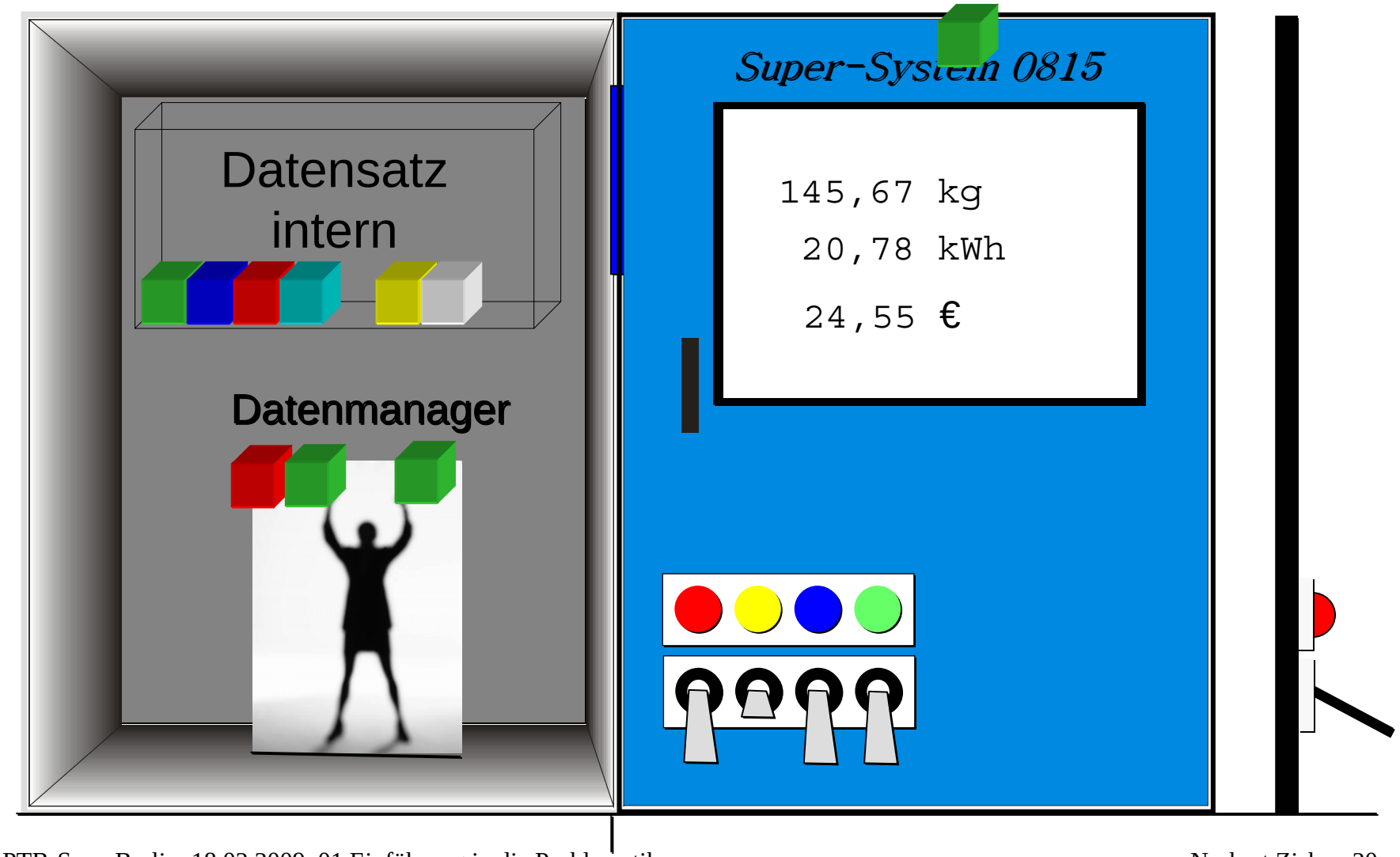
Systemmodell (real)



Das Modell (abstrakt)



Das Modell (abstrakt)



Lösungsmöglichkeiten

- **Mechanische Versiegelung:**

Mechanische Siegel sind angreifbar
Anerkannter Stand der internationalen Sicherheitsforschung:
es gibt praktisch keine Siegel, die nicht von einem motivierten
- Angreifer innerhalb kurzer Zeit und mit geringem Aufwand

Maßnahmen bieten gewissen Schutz
Sind aber auf Geheimhaltung des Verfahrens angewiesen
„Security by obscurity“
Nicht sicher gegen Insider-Angriffe

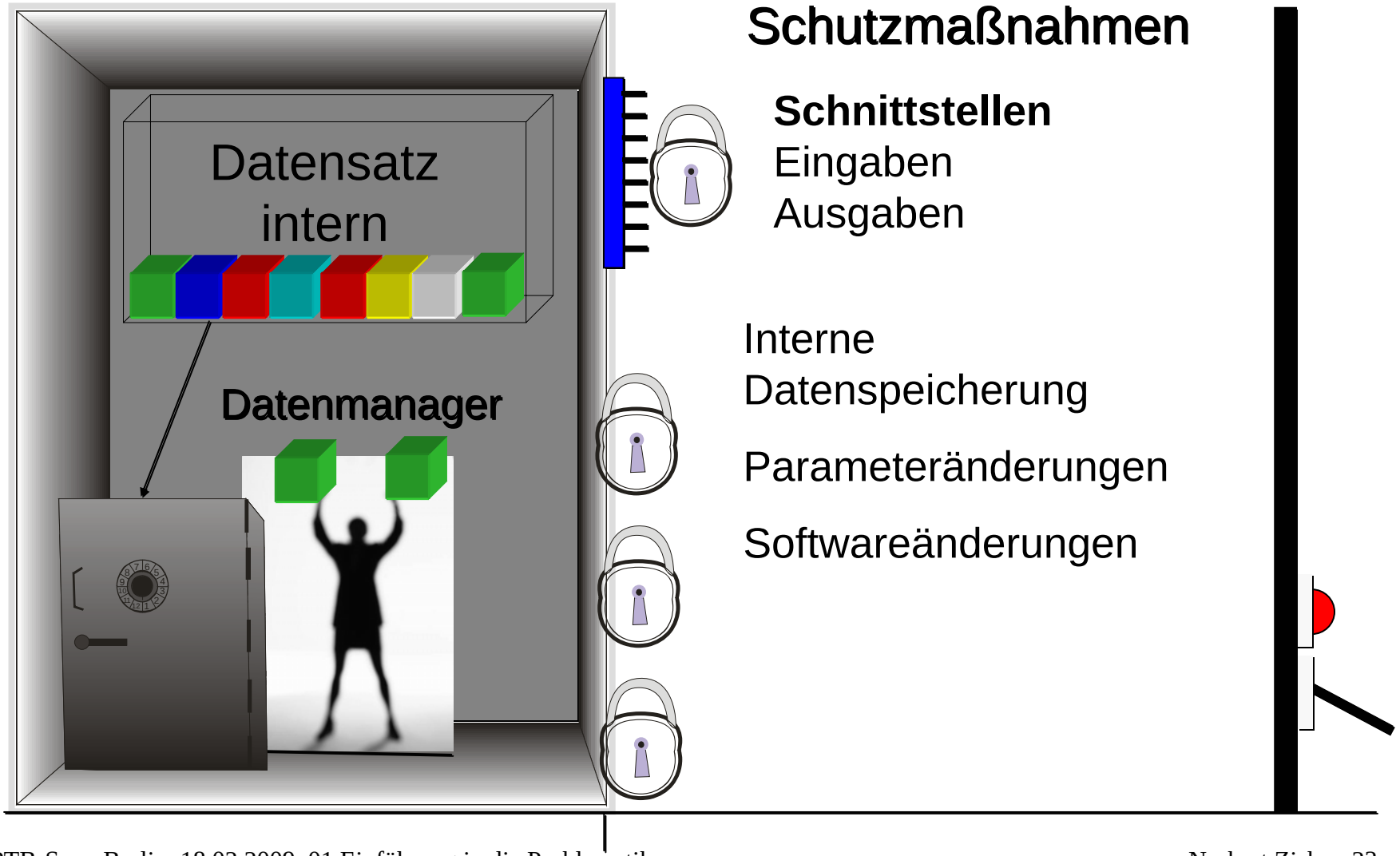
Lösungsmöglichkeiten

- **Elektronische Versiegelung der Daten:**

Einsatz symmetrischer und asymmetrischer Verfahren
Sauber definierte Sicherheitsstandards

Manipulationen nur im mikroskopischen Bereich mit Spezialtechnik möglich.

Das Modell



Schutzmaßnahmen

Schnittstellen
Eingaben
Ausgaben

Interne
Datenspeicherung

Parameteränderungen

Softwareänderungen

Restrisiken

- Direkter Angriff der Eingabedaten
- Eingriffe in die systeminternen Abläufe
- Ausnutzung von Insiderwissen
- Falsche Beurteilung von Risiken
- Fehler im Betriebskonzept des Gesamtsystems

Anforderungen vs. Prüfbarkeit

Anforderungen

- Definition von Anforderungen
- Detaillierungsgrad - Komplexität
- Konkretisierung (Vorschreiben einer Technik)

Prüfmöglichkeiten

- Je konkreter die Anforderung desto komplexer die Prüfung
- Je konkreter die Technikvorschrift desto einfacher die Prüfung

Manipulationsmöglichkeiten (1)

In nicht speziell geschützten Systemen können Datenbestände relativ leicht manipuliert werden – oft unter Nutzung regulärer Funktionen oder Sicherheitslücken:

- Nutzung von Funktionen für Servicetechniker zur Manipulation (Zugriff auf Zähler)
- Missbräuchliche Verwendung von Testfunktionen
- Direkte Änderung von Datenbeständen (in Dateien oder Datenbanken) bei PC-basierten Systemen

Manipulationsmöglichkeiten (2)

Bereitstellung spezieller Manipulationsfunktionen durch den Systemhersteller :

- Entfernung kompletter Datensätze aus elektronischen Aufzeichnungen und Neuberechnung aller Daten
- Erstellung von „Wunsch-Daten“
- Funktionen zur Modifikation von Schlüsselwerten auf einen wählbaren Wert

Zusammenfassung

Momentane Situation in der Praxis:

- Trotz klarer Rechtslage sehr schwierige Prüfung
- Keine konkrete Vorschrift zur Entwicklung, zum Vertrieb und Einsatz manipulationsgeschützter Systeme
- Kassendaten für Betriebsprüfungen u.U. praktisch wertlos
- Unzufriedenheit bei Stpfl., deren Kassendaten trotz korrekter Anwendung aller Systeme bei Prüfungen angezweifelt werden – Interesse an anerkannten revisionssichenen Systemen!!

➡ Erhebliche Unsicherheit für Finanzbehörden, Anwender, Vertreiber und Hersteller von Kassen

Ausblick

- Neue Systeme
- Veränderte Systemumfelder
- Neue Bedrohungen
- Neue Anforderungen
- Kostenaspekte
- Schutzbedarf

Vielen Dank!