Universität Stuttgart
Institute of Industrial Automation and Software Engineering

# Architekturen und Schutz der Kommunikation von CPS

Prof. Michael Weyrich

IoT / CPS Workshop im Rahmen von MicroTEC

30. Oktober 2013

# Mikrosysteme und CPS digitalisieren unsere Lebenswelt


blog; blog.cebit.de; acatech

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

**> PRESSEMITTEILUNG**

**Cyber-Physical Systems: Das Internet der Dinge, Daten und Dienste wird Branchen und Märkte prägen**

**Berlin, 12. April 2012.** *Cyber-Physical Systems werden klassische Wirtschaftsbereiche wie die Energie oder Mobilität durch die Vernetzung in Echtzeit revolutionieren. Die Deutsche Akademie der Technikwissenschaften hat die europaweit erste umfassende Studie zu den wirtschaftlichen und gesellschaftlichen Auswirkungen dieses disruptiven Technologietrends erarbeitet. Am 12. April 2012 diskutierten deutsche und internationale Experten die Ergebnisse in den Berliner EIT ICT Labs mit Staatssekretär Georg Schütte (BMBF). Ein Fazit: Um Treiber und nicht Getriebener dieser Entwicklung zu sein, müssen Politik, Wissenschaft und Wirtschaft rasch zu neuen Formen der kollaborativen Entwicklung finden und konzertiert handeln.*

In Berlin diskutierte die Projektgruppe unter Projektleiter Prof. Dr. Manfred Broy ihre umfassenden Ergebnisse mit Staatssekretär Georg Schütte (BMBF) und internationalen Kollegen, darunter Willem Jonker, Vorsitzender der EIT ICT Labs und Martin Curley, Direktor Intel Labs Europe. Bundeskanzlerin Angela Merkel war bereits beim 6. Nationalen IT-Gipfel im Dezember auf die wirtschaftlichen, technologischen und gesellschaftlichen Herausforderungen durch Cyber-Physical Systems eingegangen. Die Akademie hatte beim Gipfel in München ihre an Politik und Gesellschaft gerichtete kurze Position vorgelegt. Diesen Empfehlungen liegen Ergebnisse eines zweijährigen interdisziplinären, öffentlich geförderten (BMBF) Projekts zugrunde, in dem Wissenschaftler und Wirtschaftsexperten eng zusammengearbeitet hatten.

Schon heute arbeiten etwa 98 Prozent der Mikroprozessoren eingebettet in größeren technischen Systemen. Ein klassisches Beispiel ist das Antiblockiersystem im Auto. Cyber-Physical Systems sind

Informationen für die Verb

BITKOM

ARKT & STATISTIK PRESSE VERANSTALTUNGEN PUBLIKATIONEN WIR ÜBER UNS

YBER-PHYSICAL SYSTEMS

Suchbegriff eingeben

WACHTUMSFELD EMBEDDED SOFTWARE

**„Eingebettete Systeme“ – die Hidden Champions der Industrie**

- Studie: Verarbeitende Industrie erzielt rund 80 Prozent ihrer Wertschöpfung mit Produkten, die eingebettete Systeme enthalten
- Marktvolumen liegt weltweit bei über 160 Milliarden Euro
- Volkswirtschaftliche Bedeutung dieser Querschnittstechnologie in Deutschland unterschätzt

**Hannover, 21. April 2008** - Die verarbeitende Industrie erzielt nach einer Studie von Roland Berger Strategy Consultants im Auftrag des BITKOM rund 80 Prozent ihrer Wertschöpfung mit Produkten, die so genannte Embedded Systems enthalten. Ob in der Automation von industriellen Anlagen, der ABS- und Airbag-Steuerung im Auto oder in Herzschrittmachern und Magnetresonanztomografen: Sie alle werden gesteuert, geregelt oder überwacht durch Embedded Systems. Diese

**PRESSE-ANSPRECHPARTNER**

Marc Thylmann
m.thylmann@bitkom.org
Tel.: 030.27576-111
Fax: 030.27576-400

**ANSPRECHPARTNER**

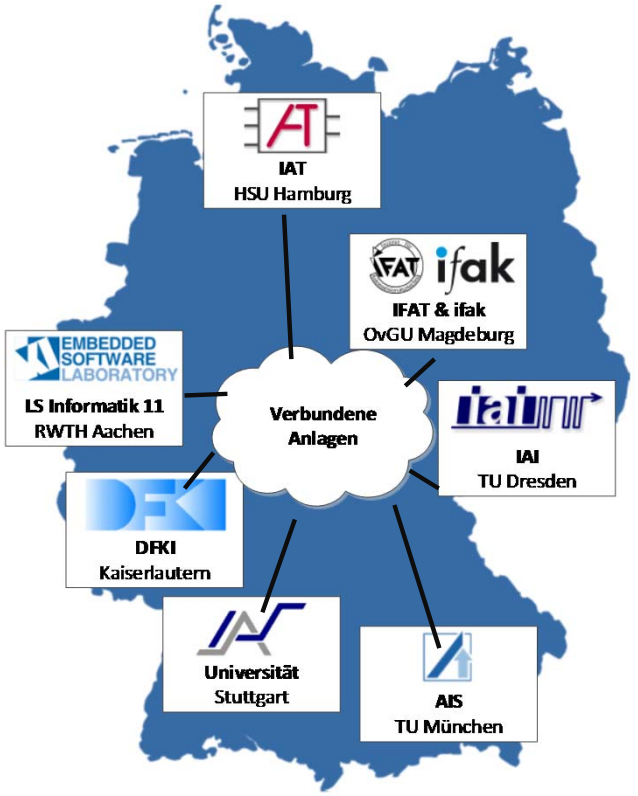
# Gliederung

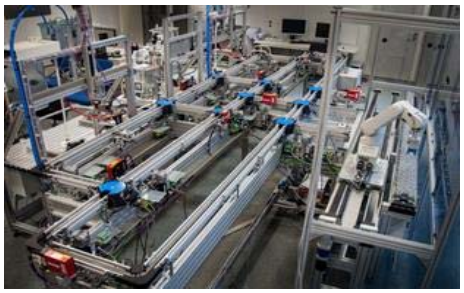
- **CPS im Einsatz in der Industrie 4.0**
- **Angriffsvektoren**
- **Beispielprozess - Schutz der Kommunikation**
- **Architektur des Schutzes**
- **Realisierung und Demonstrator**

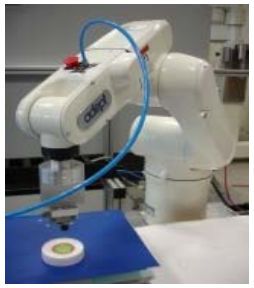
# Beispiel: Industrie 4.0 Szenarios zur Produktkonfiguration Univ.-Kooperation zw. Automatisierungstechnik und Informatik

- ***Anwendungsidee MyJoghurt:***
  Der Kunde kann über das Internet eine beliebige Menge frei konfigurierbaren Joghurt bestellen, der auf unterschiedlichen Anlagen gefertigt wird.

- Forschungsaspekte
  - Virtuelle Zuteilung der Anlage
  - Anlagenoptimierung
  - Rekonfigurierbarkeit
  - Diagnose / Fehlerprävention



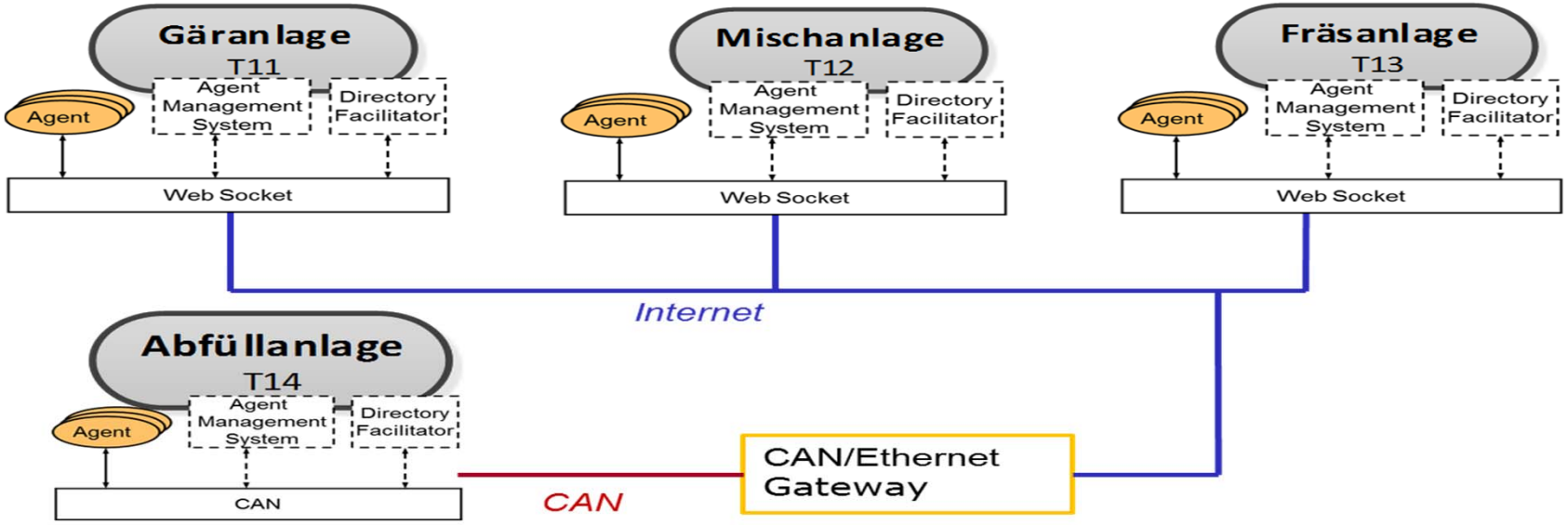




Bildquelle: [Christian Diedrich, OvGU]

# Forschungsverbundanlage - Vernetzung über das Internet mit Virtual Private Network sowie auf der Feldebene mit CAN

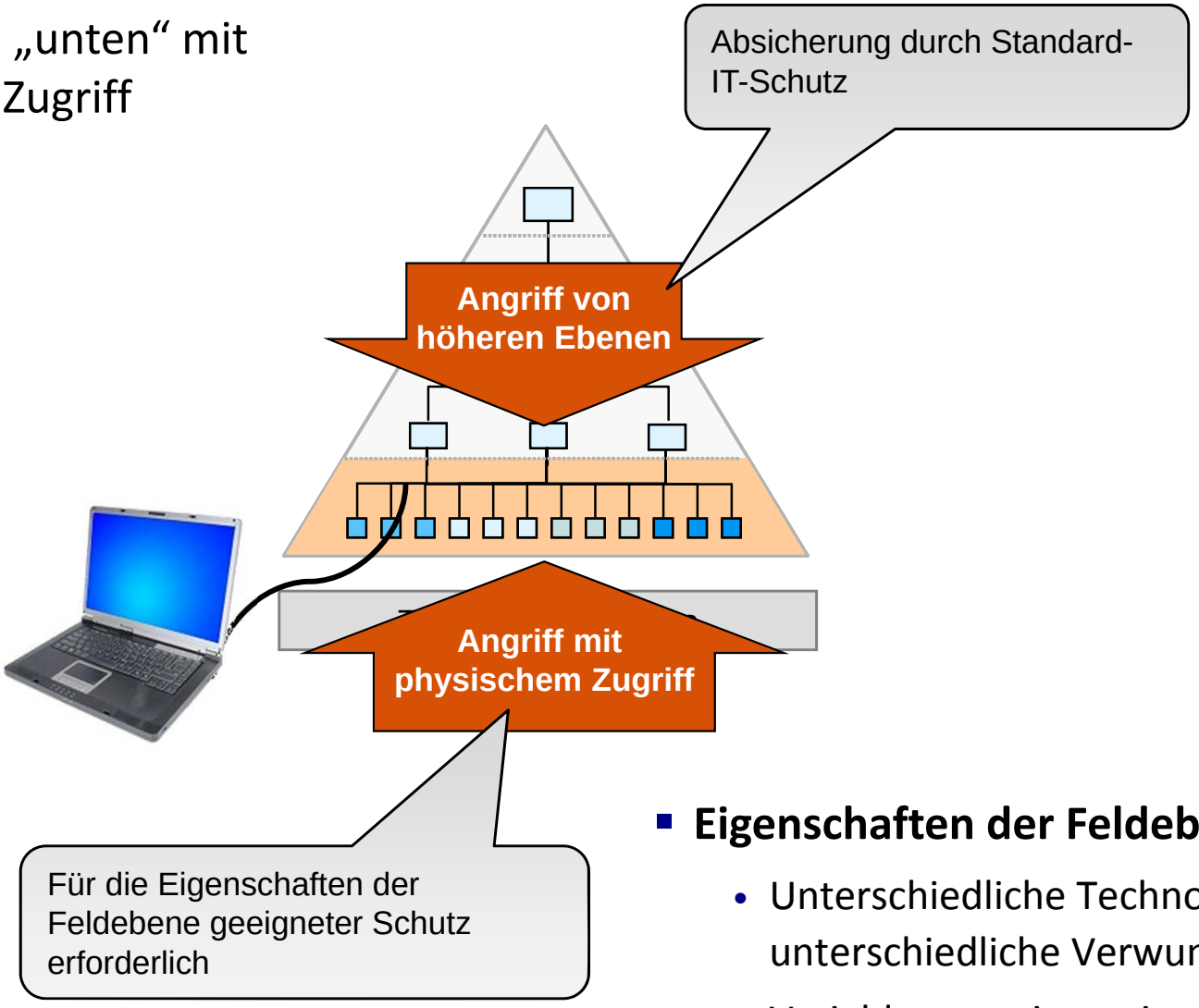
- Network Management - Web Based Enterprise Management (WBEM)
- Cloud-Dienst zur Validierung eingebetteter Systeme
- Systemübergreifende Diagnose mit Service-orientierter Architektur
- Planung von Aufträgen an die Produktionsanlagen über Agenten




Bildquelle: [Christian Diedrich, OvGU]

# Angriffesvektoren

- Angriffe von höheren Ebenen
- Angriffe von „unten“ mit physischem Zugriff



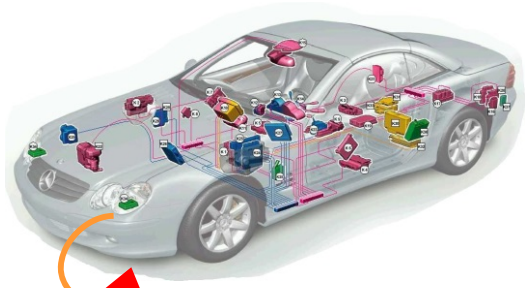

- **Eigenschaften der Feldebene**
  - Unterschiedliche Technologien – unterschiedliche Verwundbarkeiten
  - Variable, zumeist geringe Ressourcen
  - Enge Kopplung

# Forschung zum Schutz der Kommunikation am IAS

Sind Automatisierungssysteme über die Feldebene angreifbar?

**Anlage**

**Kraftfahrzeug**



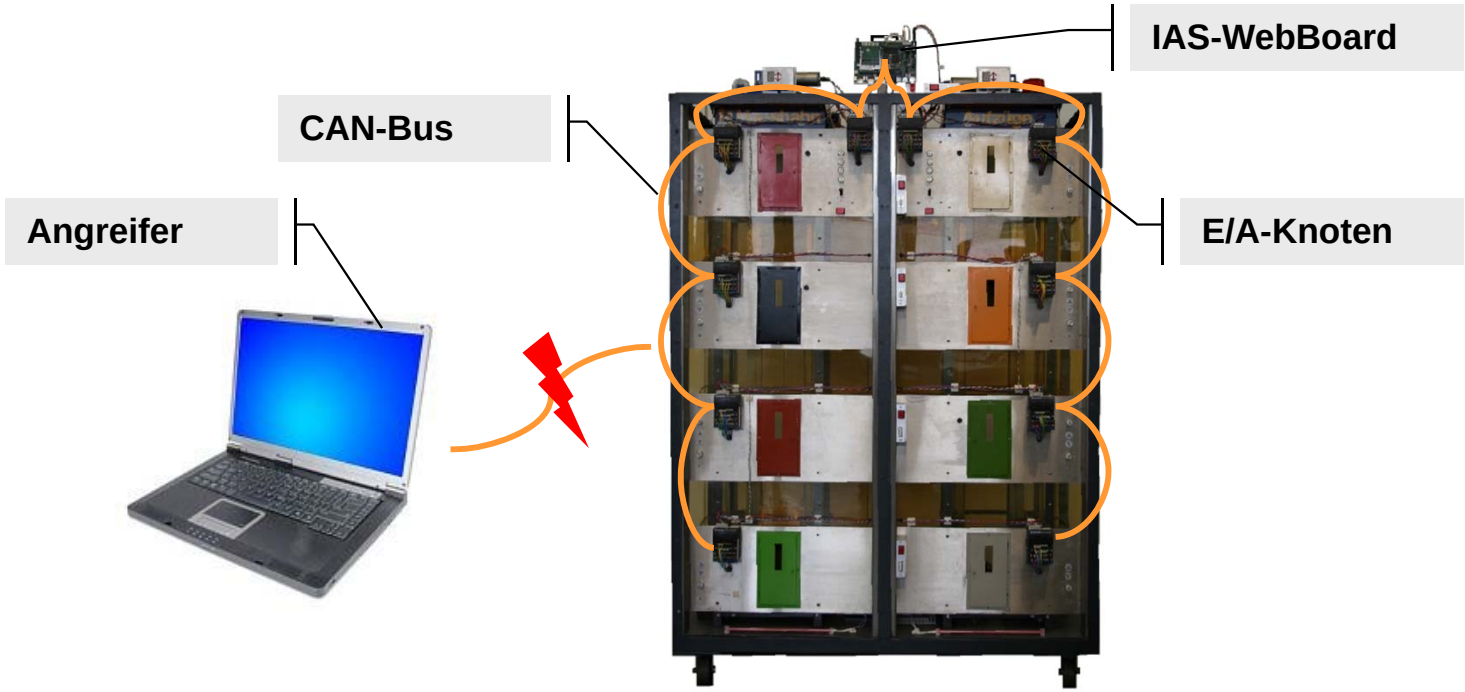
**Aufzug**

## Angriffsarten

- Abhören
- Manipulation inhaltlicher Integrität
- Erzeugung eigener Daten
- Manipulation zeitlicher Integrität (z.B. senden abgehörter Botschaften)
- Manipulation der Funktionalität (z.B. Verändern der Firmware)

# Angriffe auf IAS-Modellprozess „Aufzug“ (1)

- **Ereignisgesteuerter Bus mit zufälligem Buszugriffsverfahren (CSMA/CA)**

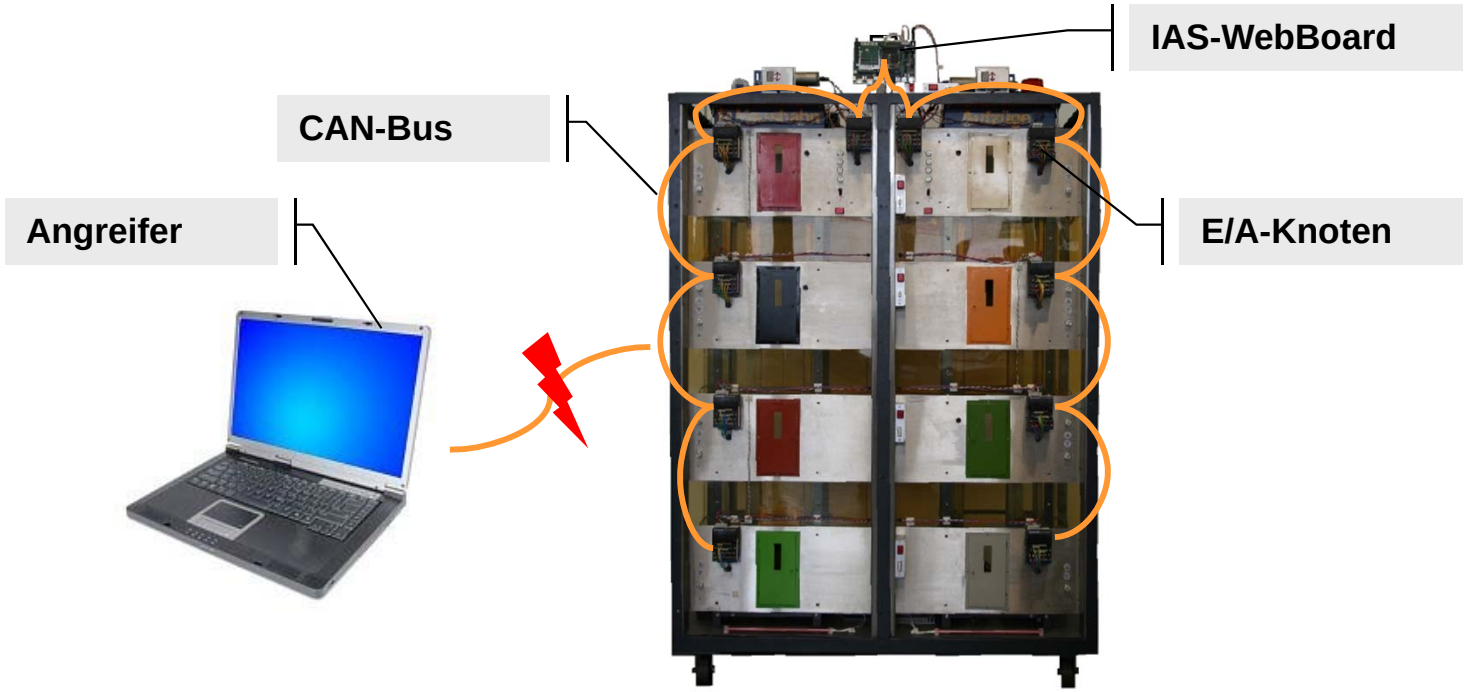



- Manipulation des Buszugriffs
  - Vortäuschung ständiger Busbelegung durch kontinuierliches Senden von hochprioren Nachrichten
  - Keine Buskommunikation mehr möglich

**Auswirkungen: z. B. Aufzug kollidiert mit Schacht-Ende, Motor schaltet sich nicht ab.**

# Angriffe auf IAS-Modellprozess „Aufzug“ (2)

- **Angriff auf Adressierung**

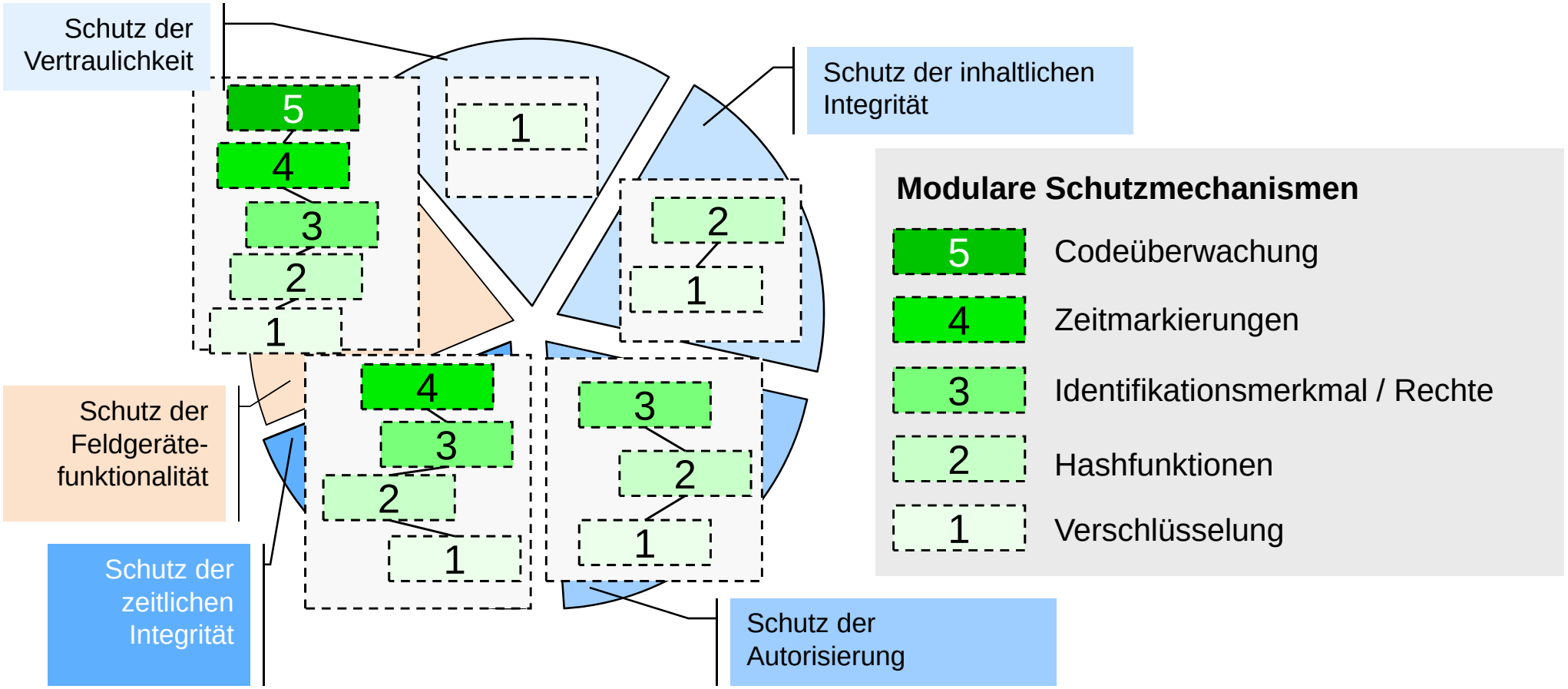



- Manipulation der Adressierung
  - Aufzug verwendet Nachrichten-ID zur Identifikation des Absenders
  - Senden der Nachricht „Tür geschlossen“ mit „Absender-ID“ des Tür-Knotens

**Auswirkung: Aufzug fährt trotz offener Tür an**

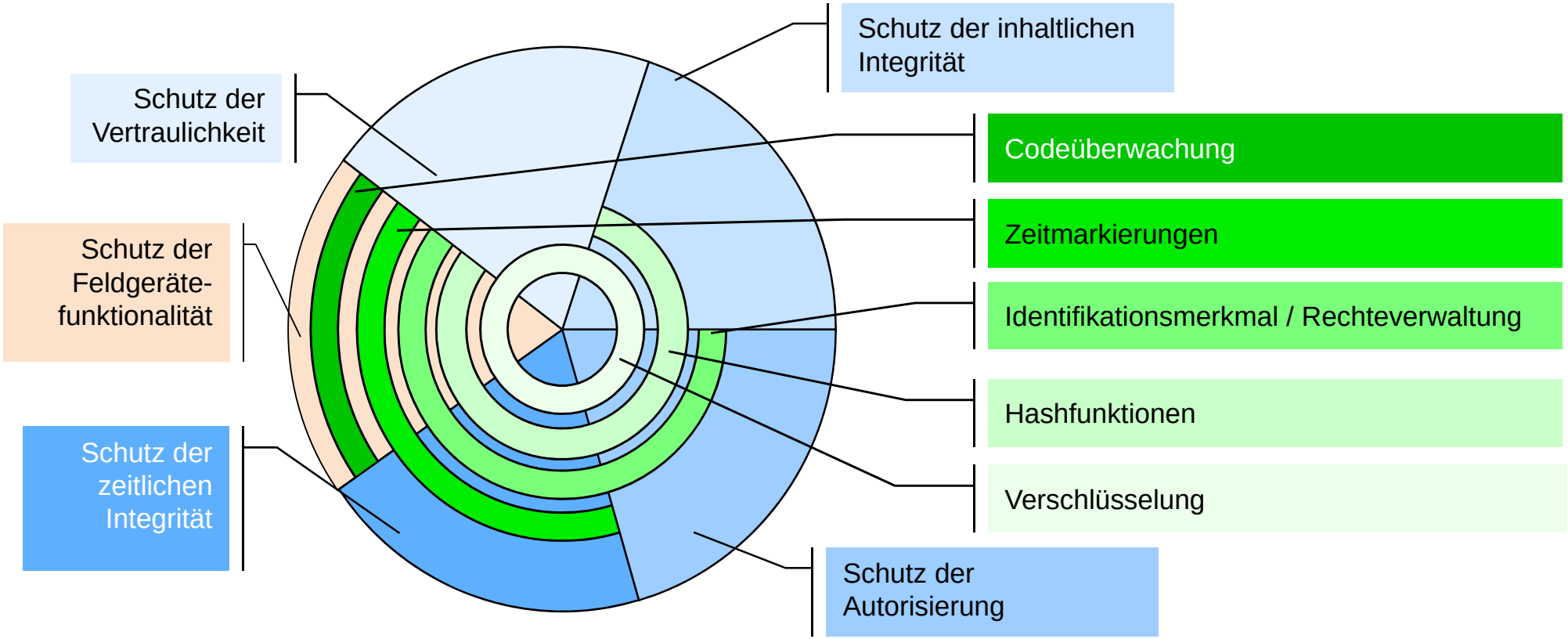
# Entwurf des Schutzes zur Detektion von Manipulationen

- Mehrfachverwendung gleichartiger Operationen durch unterschiedliche Schutzfunktionalitäten



# Architektur des Schutzes zur Detektion von Manipulationen

- Schutzmechanismen bauen auf anderen Schutzmechanismen auf

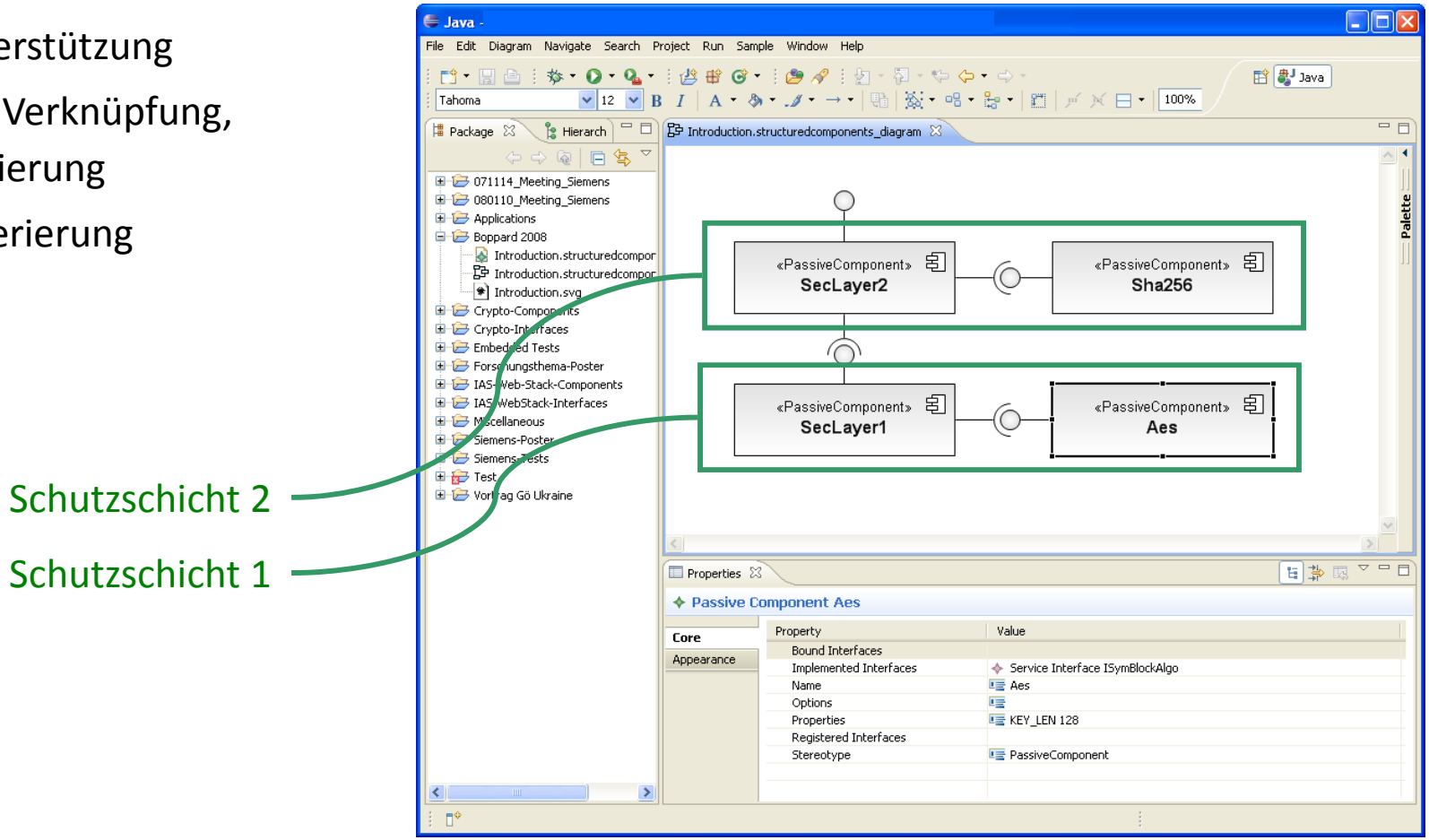



- Eigenschaften der Architektur
  - Anpassbar — Modulare Schutzfunktionalitäten und Schutzmechanismen
  - Ressourcenschonend — Mehrfachverwendung, Auswahl ressourcenschonender Module
  - Echtzeitfähig — Festlegung von Mechanismen, Auswahl zeitl. deterministischer Module

# Realisierung des Schutzes

- Realisierung mittels Softwarekomponenten
  - Strukturierte Programmiersprache (C)
  - Funktionsentwicklung durch Auswahl, Verknüpfung und Parametrierung

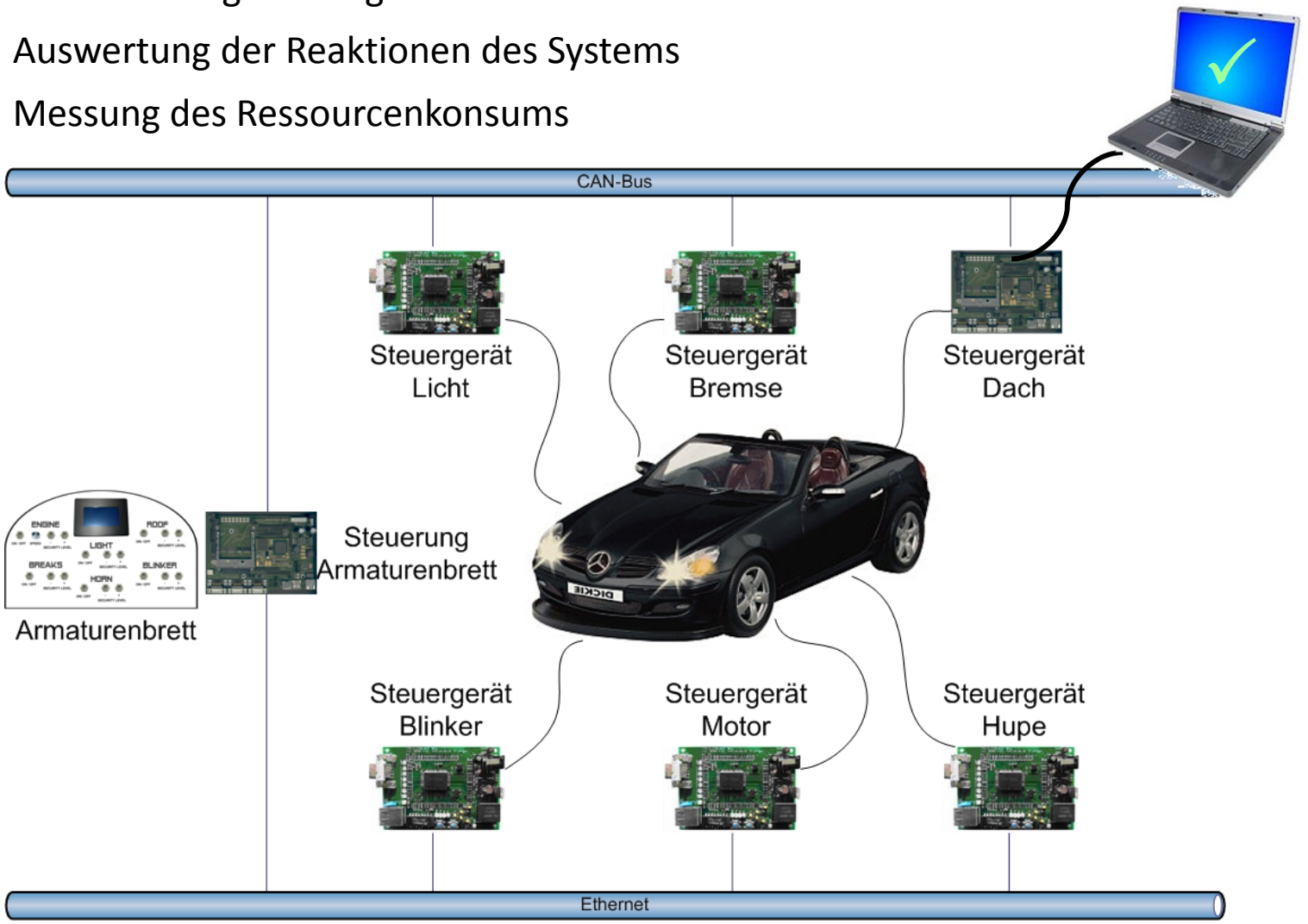
- Werkzeugunterstützung
  - Auswahl, Verknüpfung, Parametrierung
  - Codegenerierung



# Demonstrator „Kfz-Steuergerätenetzwerk“ mit unterschiedlichen Feldgerätetypen und Feldbusse

Evaluierung der Schutzwirkung durch Penetrationstests

- Durchführung von Angriffen
- Auswertung der Reaktionen des Systems
- Messung des Ressourcenkonsums



# Zusammenfassung

- Schutzkonzept zur Absicherung der IT-Sicherheit auf der Feldebene von Automatisierungssystemen
  - Verwendung bewährter Funktionsprinzipien der IT-Sicherheit
    → Wirksam gegen Manipulationen
  - Modular
    → Hohe Anpassbarkeit
  - Ressourcenschonender Entwurf und Implementierung
    → Hohe Effizienz