Drahtlose Sensorik über Nahbereichsfunk Chancen und Probleme

Daniel Scherer

Fraunhofer-Anwendungszentrum Drahtlose Sensorik, Coburg

Fraunhofer IIS

AGENDA

- Über mich
- Wer sind wir?
- Anwendungsszenarien
- Sicherheitsrisiken
- Ursachen und Lösungsansätze
- Fazit

Anwendungszentrum Drahtlose Sensorik
Daniel Scherer

- Wissenschaftlicher Mitarbeiter im Fraunhofer IIS – AWZ Coburg
- Projektleiter im Bereich IT Sicherheit
- B. Sc. Informatik (Abschlussarbeit über „Forensische Analyse von Flash-Speichern“)
- M. Sc. Informatik (Abschlussarbeit über „Datenschutzvorkehrungen in vernetzten Systemen“)
- Cerified Ethical Hacker (CEH)
- Freiberuflicher IT Sicherheitsberater und Penetrationtester

Anwendungszentrum Drahtlose Sensorik
Unser Angebot

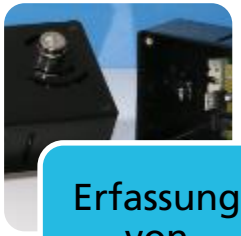
- Technologien der drahtlosen Sensoren und Sensornetze für verschiedene **Anwendungsfelder** verfügbar machen

  → Kunden bei **Digitalisierung** begleiten!

- Auswahl/Bau der **Elektronik-Hardware**
- **Maßgeschneiderte drahtlose Kommunikationslösung**
  - Mit Fraunhofer- oder standardisierter Technologie
- Von der **Machbarkeit** bis zur **konkreten Umsetzung**
- Von der **Sensorik** bis zur **Applikation**
- **Sicherheit vom Design an**

Anwendungszentrum Drahtlose Sensorik

Die gesamte Anwendung im Blick

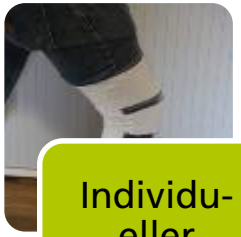


Erfassung von Sensor-daten

Drahtlose Multi-Hop-kommuni-kation

Sichere Übertra-gung und Speiche-rung

Zielgrup-penge-rechte Aufberei-tung

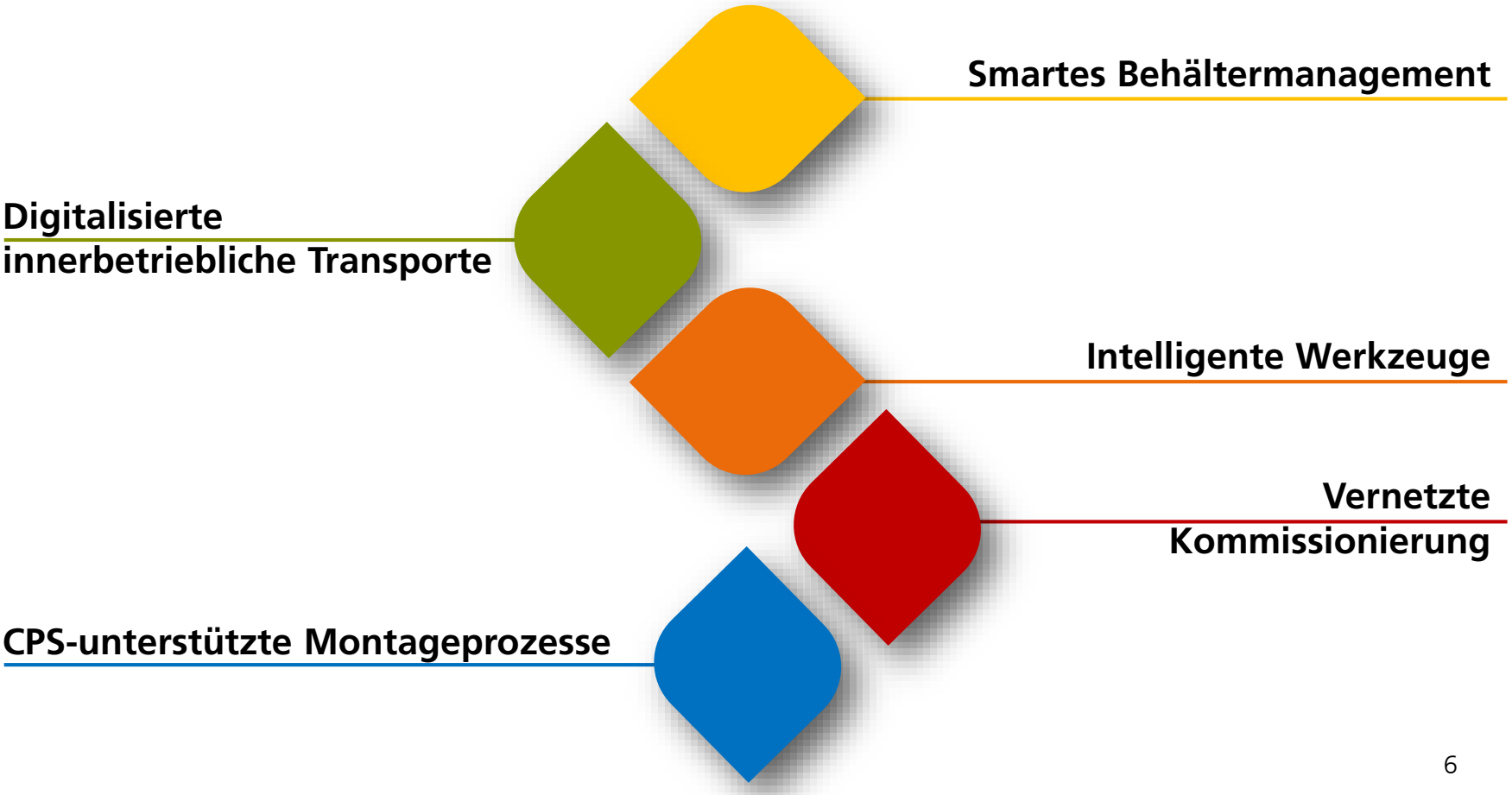


Individu-eller Daten-zugriff

Fraunhofer IIS

Anwendungszentrum Drahtlose Sensorik

Anwendungen



Fraunhofer IIS

Angriffsszenarien

Smartes Behältermanagement

Manipulation von Inhaltsdaten, Defekte vortäuschen

Digitalisierte innerbetriebliche Transporte

Falsche Wegstrecken einspeisen, Unfälle verursachen

Intelligente Werkzeuge

Montage sabotieren

Vernetzte Kommissionierung

Fehler verursachen

CPS-unterstützte Montageprozesse

Montage sabotieren, Firmengeheimnisse entwenden

Sicherheitsrisiken
Angriffsziel Produktionsbetrieb

- **Die Angriffsfläche, vor allem aber die Angriffstiefe wird größer**
  - Durch zunehmende Digitalisierung entsteht eine viel größere Abhängigkeit vom Kerngeschäft zur IT.
  - Dadurch entstehen Erpressungsmöglichkeiten durch Angriffe auf die Funktion der Systeme und damit direkt auf das Kerngeschäft.

- **Markterkundung und Konkurrenzanalyse werden Alltag**
  - Hacker sind eine neue Berufsgruppe mit hohen Gehältern und viel Freizeit.
  - Hackerangriffe stellen eine deutliche Verbilligung der Angriffswaffen dar.

- **Neuer Raum für Cyberversicherungen**
  - Der Abschluss von Versicherungen gegen Manipulation und Diebstahl wird essentielle Voraussetzung des Geschäftsbetriebs, was jedoch auch ***die Nachweisbarkeit*** des Schadensfalls voraussetzt.

Sicherheitsrisiken
Zu sicherende Assets

Ausspionieren von Produktionsanlagen

Manipulation der Funktionsweise von Anlagen

Manipulation der Arbeitszeitmodelle verketteter Anlagen

Ausspionieren des Produktionsprozesses

Sicherheitsrisiken
Verschiedene Ebenen zu betrachten

Office
- (Spear)-Phising
- Verseuchte E-Mail Anhänge
- Verseuchte Smartphones und USB-Sticks
- (Drive-by)-Downloads

Anlagen
- Anlagen direkt aus dem Internet erreichbar
- „Chaotische“ Netzwerkstruktur
- Verseuchte Smartphones und USB-Sticks
- Unsichere Fernwartungszugänge

Feldgeräte
- Funkstrecke nicht gesichert
- Verschlüsselung oft schwer implementierbar (Rechenleistung, Low-Energy,…)
- Sensoren teilweise mobil oder durch Fremde erreichbar

Ursachen und Lösungsansätze

Die wichtigsten Ursachen

Unzureichende Authentisierung

- Passwort/Identitäts-Diebstahl,
- unerlaubte Zugriffe durch Insider + Outsider

Unzureichende Vertraulichkeit

- Entwendung von Entwürfen, Produktionsverfahren

Unzureichende Integrität

- Veränderung kritischer Daten, z.B. Bohrtiefe

Unzureichendes Bewusstsein

- Drahtlose Sensoren können schwächstes Glied der Kette sein
- Zu viele veröffentlichte Informationen

Ursachen und Lösungsansätze

Lösungen für neuartige Anforderungen

Intelligente Objekte

- → Digitaler Schatten
- → Zertifikate für Anlagen

Lange Lebens- und Innovations-zyklen

- → Abgesicherte regelmäßige Updates
- → Sichere Fernwartung über vertrauens-würdige Broker

Echtzeit-anforderungen, Hochverfüg-barkeit

- → Leicht-gewichtige Kryptographie
- → Gegen-einander abgesicherte Teilnetze

Physischer Zugriff

- → Schutz vor Manipulationen
- → Schutz vor unberechtigtem Auslesen

Daten-übertragung

- → Sichere Kommunikation
- → Autorisierter Zugriff

Bildquellen: Fraunhofer IIS/Fotolia

Ursachen und Lösungsansätze
Fazit

- **Weitreichende Einsatzmöglichkeiten** vorhanden
- **Office- und Anlagen-IT** wachsen zusammen
- Auf Office- und Anlagen-Ebene viele Sicherheits-Lösungen vorhanden
- Auf Sensor-Ebene müssen **neue Techniken** entwickelt werden
- Industrie 4.0 kann nur sicher sein, wenn **alle Ebenen** berücksichtigt werden
- **Isolierte Einzelmaßnahmen** oft wirkungslos
- Schwachstellen erkennen → Angreifbarkeit verringern → Sichere Prozesse etablieren → Bewusstsein schärfen
- **Zusammenarbeit mit Experten** ausbauen

Bildquelle: Fraunhofer IIS

Vielen Dank für Ihre Aufmerksamkeit