Fraunhofer Einrichtung
Systeme der
Kommunikationstechnik

Drahtlose Kommunikation in sicherheitskritischen Systemen

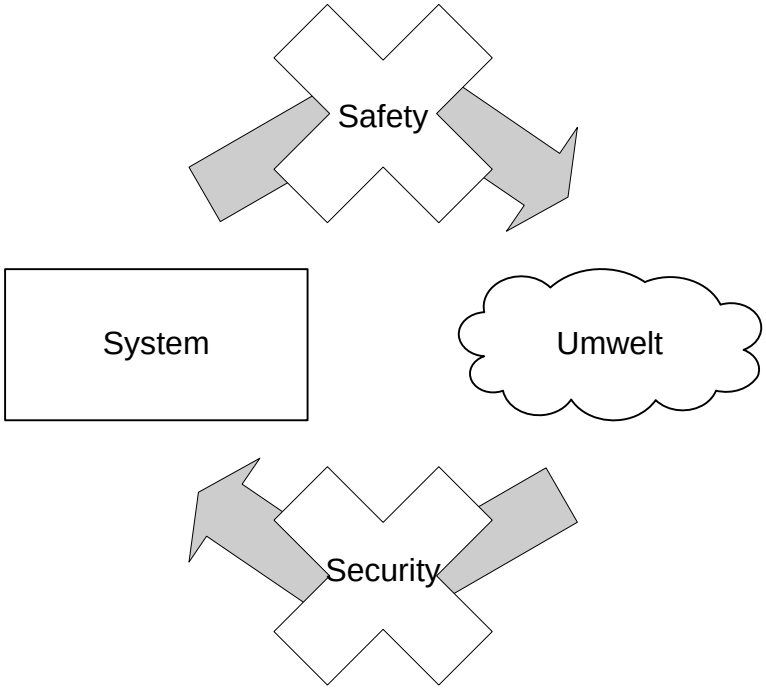
Sicherheit mit Wireless?

Dipl.-Inform. Markus Augel

Oktober 2006

Was ist Sicherheit?

Sicherheit = Safety & Security



Safety

- Schutz der Umwelt vor dem System
- Ziel: negative Wirkungen des Systems (durch Betrieb oder Ausfall) vermeiden
- Beispiel: Reaktorsicherheit, Alarmanlagen

Security

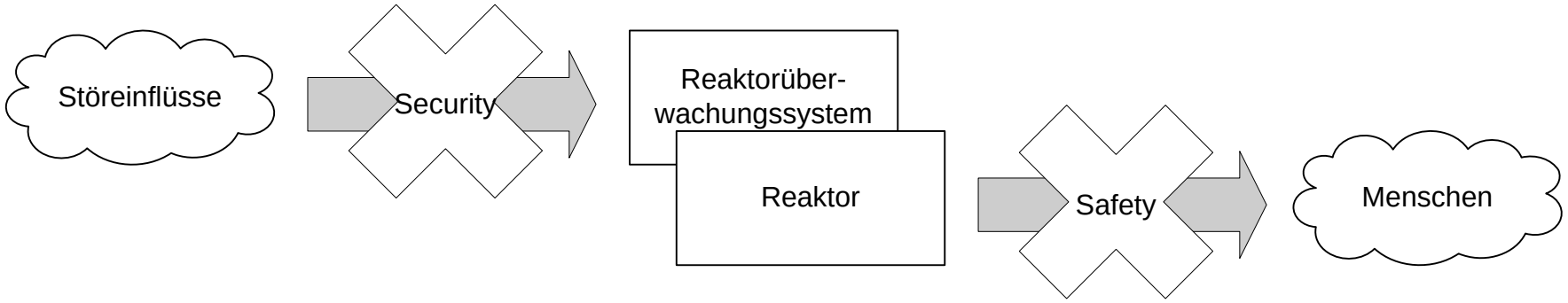
- Schutz des Systems vor der Umwelt
- Ziel: negative Wirkungen der Umwelt auf das System vermeiden
- Beispiel: Schutz eines Datenübertragungssystems vor Hackern

Dipl.-Inform. Markus Augel
Oktober 2006

ESK
Fraunhofer Einrichtung Systeme der Kommunikationstechnik

Mehr Safety durch Security

- von Security eines Systems kann Safety eines anderen abhängen
- Beispiel:
  Sicherheit eines Datenübertragungssystems zur Reaktorüberwachung (Security)
  kann Auswirkungen auf Reaktorsicherheit haben (Safety)



- Kann ein drahtloses System so sicher (Security) sein,
  dass damit Sicherheitsaufgaben (Safety) erfüllt werden können?

Dipl.-Inform. Markus Augel
Oktober 2006

ESK
Fraunhofer Einrichtung Systeme der Kommunikationstechnik

Security-Anforderungen und -Mechanismen (1)

- Abhörsicherheit und Vertraulichkeit
  - erreichbar durch: Verschlüsselung (symmetrisch, asymmetrisch, hybrid)
- Datenintegrität
  - erreichbar durch: Message Authentication Codes
  - kryptographische Prüfsumme aus Daten und Schlüssel
- Authentizität des Kommunikationspartners
  - nachweisbar durch: Challenge-Response-Verfahren
  - Nachweis der Kenntnis geheimer Informationen

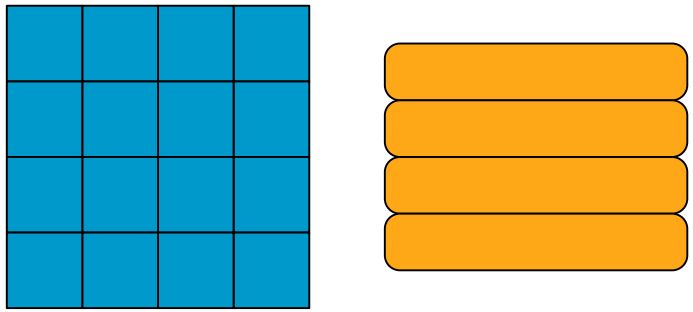
➔ Mechanismen sind nur so gut wie die dahinter stehenden Algorithmen

Dipl.-Inform. Markus Augel
Oktober 2006

Fraunhofer ESK Einrichtung Systeme der Kommunikationstechnik

Beispiel: WLAN-Verschlüsselung mit AES

- AES = Advanced Encryption Standard
- symmetrisches Verfahren
- rundenbasierte blockweise Verschlüsselung
- Schlüssellänge 128, 192 oder 256 Bit
- Angriffe auf AES
  - related-key attack (2000): nur erfolgreich bei reduzierter Rundenanzahl
  - choosen-plaintext attack (2000) : nur erfolgreich bei reduzierter Rundenanzahl
  - XSL attack (2002): theoretisch, gilt als fehlerhaft
  - cache timing attack (2005): Zugriff auf Prozessorcache nötig
- AES ist von der US-NSA für TOP SECRET Informationen zugelassen



Dipl.-Inform. Markus Augel
Oktober 2006

Fraunhofer ESK Einrichtung Systeme der Kommunikationstechnik

Security-Anforderungen und -Mechanismen (2)

- Robustheit und Verfügbarkeit
  - verschiedene Modulationsverfahren
  - verschiedene Bandspreizverfahren
  - Fehlerschutz- und -korrekturmechanismen
  - redundante Übertragung
  - Neuübertragung im Fehlerfall

➔ geeignete Auswahl und Kombination:
Einsatz in Umgebungen mit hohem Störpotential möglich

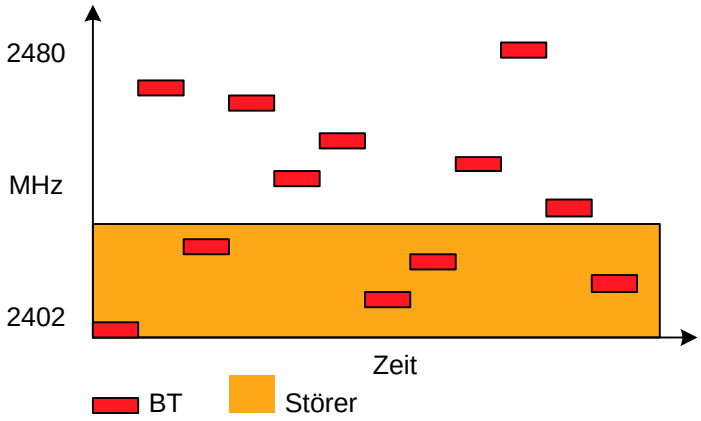
Dipl.-Inform. Markus Augel
Oktober 2006

Fraunhofer ESK Einrichtung Systeme der Kommunikationstechnik

Beispiel: Bluetooth-Bandspreizung

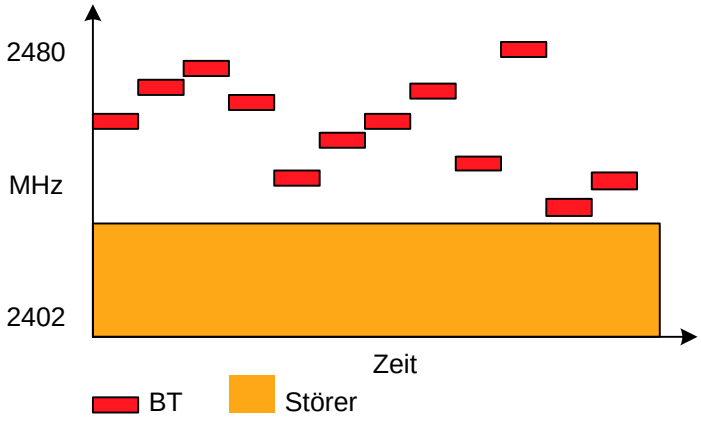
Adaptive Frequency Hopping

- 1.600 Frequenzwechsel pro Sekunde
- dabei automatische Erkennung und Vermeidung gestörter Frequenzen (ab v1.2)



Praxisbeispiel

- Deutsche Firma
- Steuerung von mobilen Brennöfen über Bluetooth
- Security von Bluetooth dafür ausreichend
- hohe Verfügbarkeit



Dipl.-Inform. Markus Augel
Oktober 2006

Fraunhofer ESK Einrichtung Systeme der Kommunikationstechnik

Wireless Safety Anwendungen - Beispiele

Szenario: Brandschutz

- drahtlose Sensoren zur Temperaturüberwachung
- für gefährdetes Gelände: Wälder, Felder etc.
- Brandfrüherkennung

Szenario: Überwachung der statischen Integrität

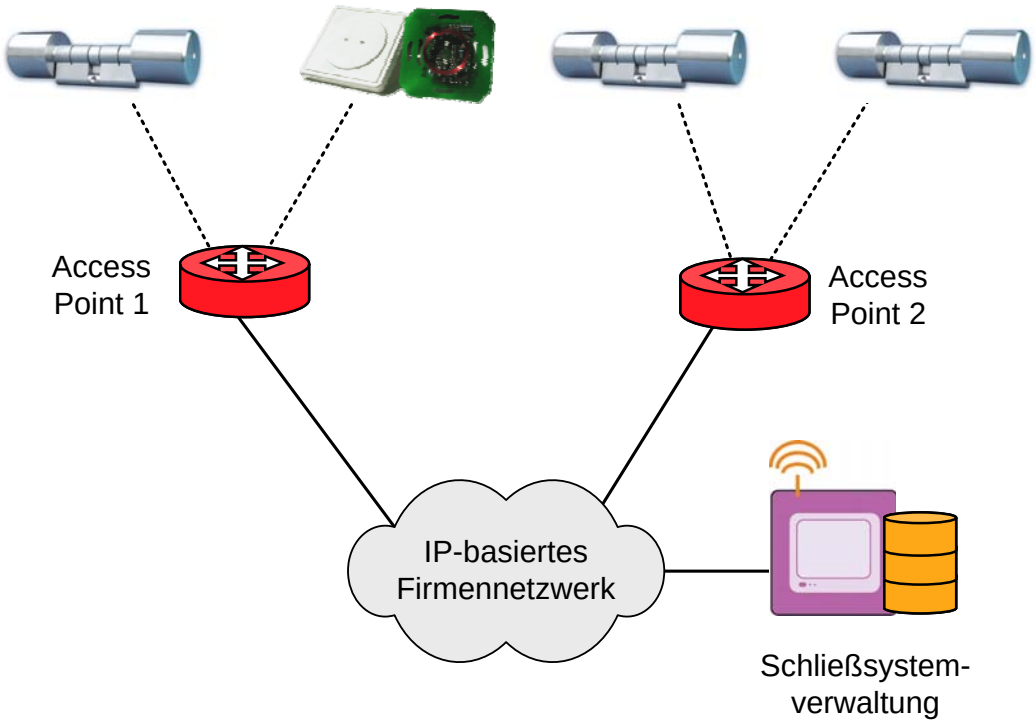
- drahtlose Sensoren zur Erfassung von Vibrationen
- für Großbauwerke: Hallen, Brücken, Staudämme etc.
- rechtzeitige Evakuierung

Dipl.-Inform. Markus Augel
Oktober 2006

ESK
Fraunhofer Einrichtung Systeme der Kommunikationstechnik

Kooperationsprojekt: Vernetzung elektronischer Schließzylinder

- Funksystem in Schließzylindern
- Kryptographisch gesicherte Kommunikation
- Selbstorganisierende Vernetzung
  - automatische Einbindung der Netzelemente
  - Erkennung und Kompensation von Störungen
- Zentrale Verwaltung aller Schließzylinder
- Zeitnahe Statusabfrage
- Zeitnahe Sperrung von Schlüsseln
- Geringer Installationsaufwand



Uhlmann & Zacher
SYSTEME AUS EINER HAND

Dipl.-Inform. Markus Augel
Oktober 2006

Fraunhofer ESK
Einrichtung
Systeme der
Kommunikationstechnik

Zusammenfassung

Drahtlose Kommunikation und sicherheitskritische Systeme sind kein Widerspruch

- Einzelne Anwendungen mit Wireless erst praktikabel
- Herausforderung bleibt: Auswahl der richtigen Funktechnik
- Analyse des Anwendungsfalls erforderlich
- Wesentlicher Aspekt: Selbstorganisation

Anwendungsfall Schließsystem

- Gemeinschaftstand: Fraunhofer ESK - Uhlmann & Zacher GmbH
- Halle 12, Stand 214
- Wir freuen uns auf Ihren Besuch!

Hansastr. 32
80686 München
Tel.: 089-54 70 88-0
www.esk.fraunhofer.de

Dipl.-Inform. Markus Augel
Oktober 2006

Fraunhofer ESK Einrichtung Systeme der Kommunikationstechnik