



Fraunhofer

Einrichtung
Systeme der
Kommunikationstechnik

Ein selbstorganisierendes Funkschließsystem

Ein Kooperationsprojekt
von Fraunhofer ESK und der Uhlmann & Zacher GmbH

Gefördert durch das Bayerische Staatsministerium für
Wirtschaft, Infrastruktur, Verkehr und Technologie

Dipl.-Ing. Josef Jiru
Dr.-Ing. Markus Zeller

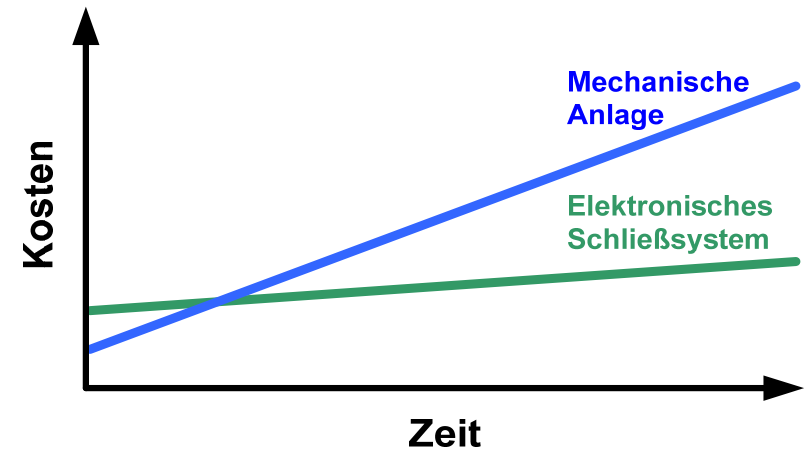
in Vertretung von
Dipl.-Inform. Markus Augel

Motivation

Stand der Technik: Ablösung mechanischer durch elektronische Schließanlagen

Vorteile von elektronischen Schließsystemen

- Hohe Flexibilität
(Frei programmierbare Schließpläne, Schließgruppen, ...)
- Umstrukturierungen und nachträgliche Schließplanänderungen problemlos möglich
- Verloren gegangene Schlüssel können einfach gesperrt werden
- Schließereignisse werden protokolliert
- Auf Dauer deutliche Kostenreduzierung gegenüber mechanischer Anlage

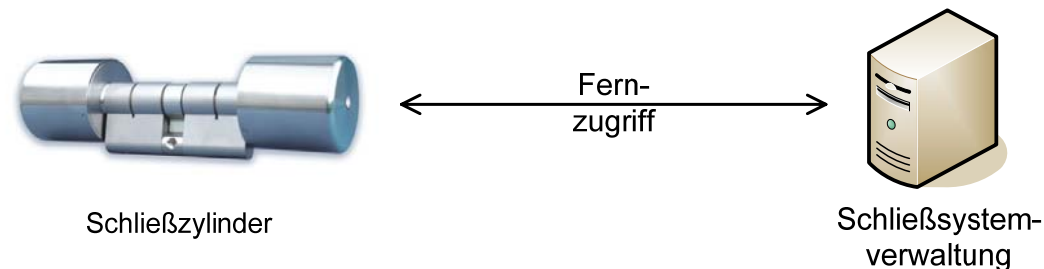


Vernetzung elektronischer Schließzylinder

Problem: Hoher Verwaltungsaufwand bei größeren Schließanlagen

Lösung: Zentrale Verwaltung aller Schließzylinder per Fernzugriff

- Reduzierter Verwaltungsaufwand
- Steuerung aller Zugangsberechtigungen von einem zentralen Punkt
- Einfache Realisierung von temporären Schließberechtigungen
- Schnelle Sperrung von verlorenen Schlüsseln
- Zeitnahe Status- und Protokollabfrage
- Zentrales Öffnen und Schließen (z.B. in Notsituationen)



Kabelbasierte vs. Drahtlose Vernetzung

Nachteile kabelbasierter Installationen

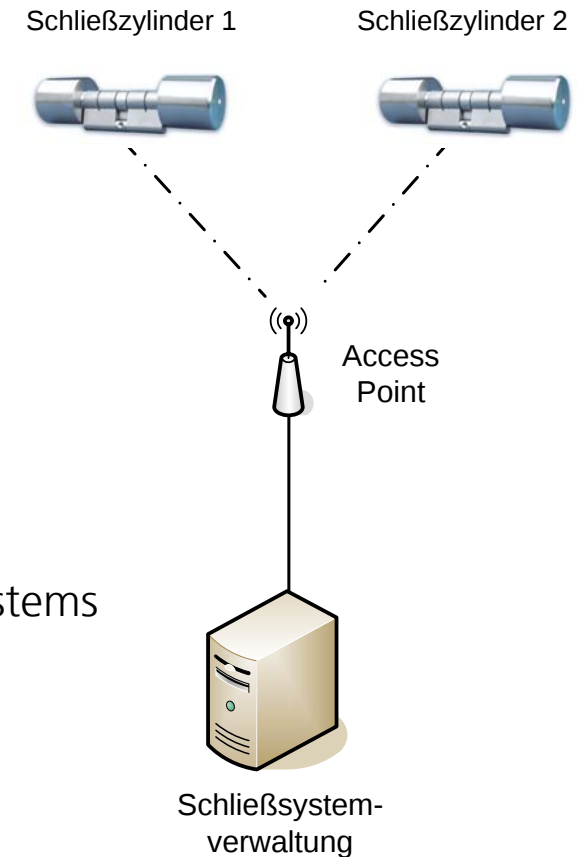
- Neubauten: Kabelziehen zu jeder Tür nötig
- Nachträgliche Installationen aufwändig und teuer

Lösung: Drahtlose Kommunikation

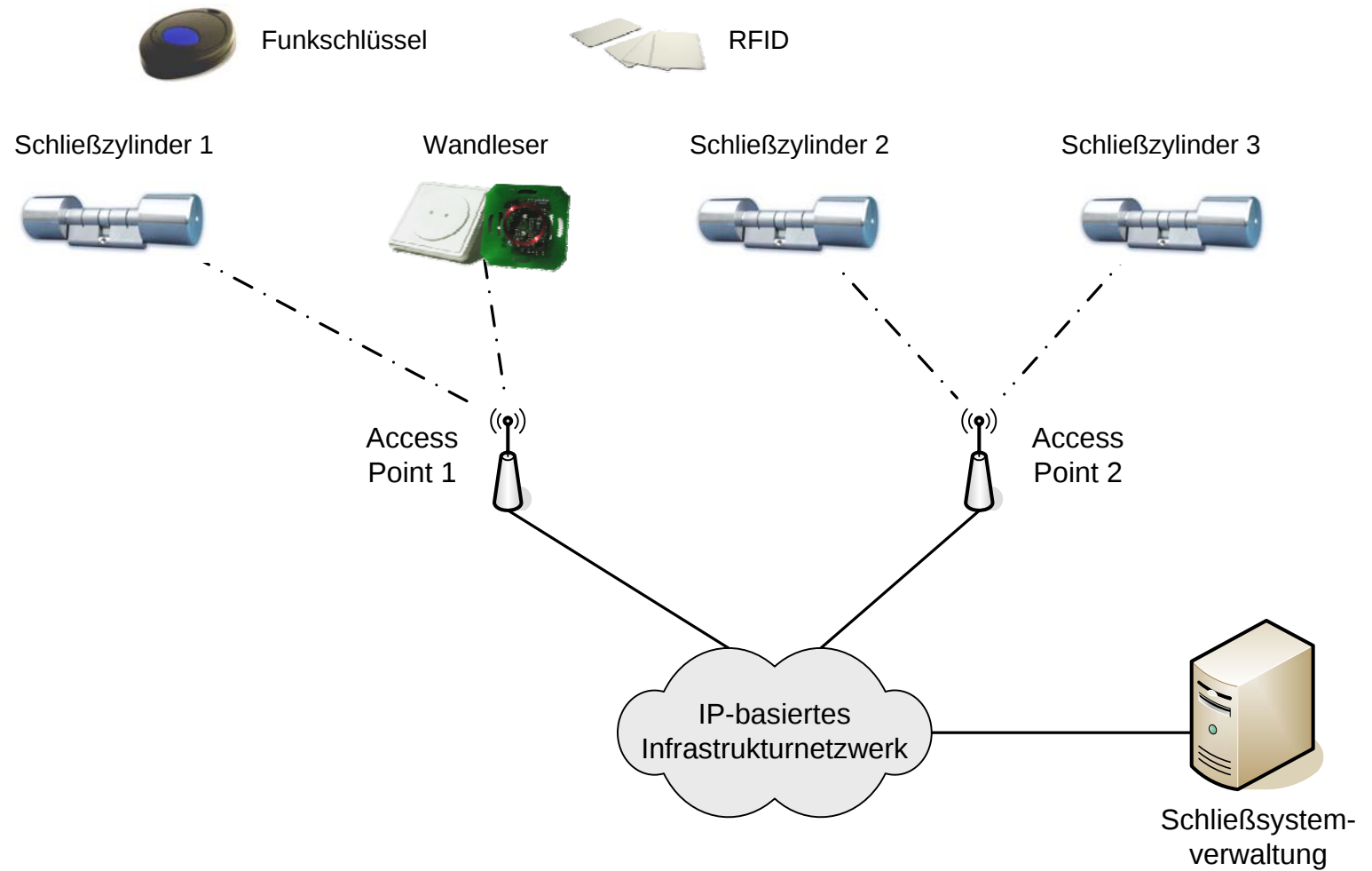
- Integration eines Funksystems in die Schließzylinder
- Geeignete Funktechnologie verfügbar

Zentrale Anforderungen

- Unkomplizierte Inbetriebnahme und Administration des Systems
- Entlastung und Komfort für den Anwender
- Robustheit und Sicherheit
- Hohe Funktionalität

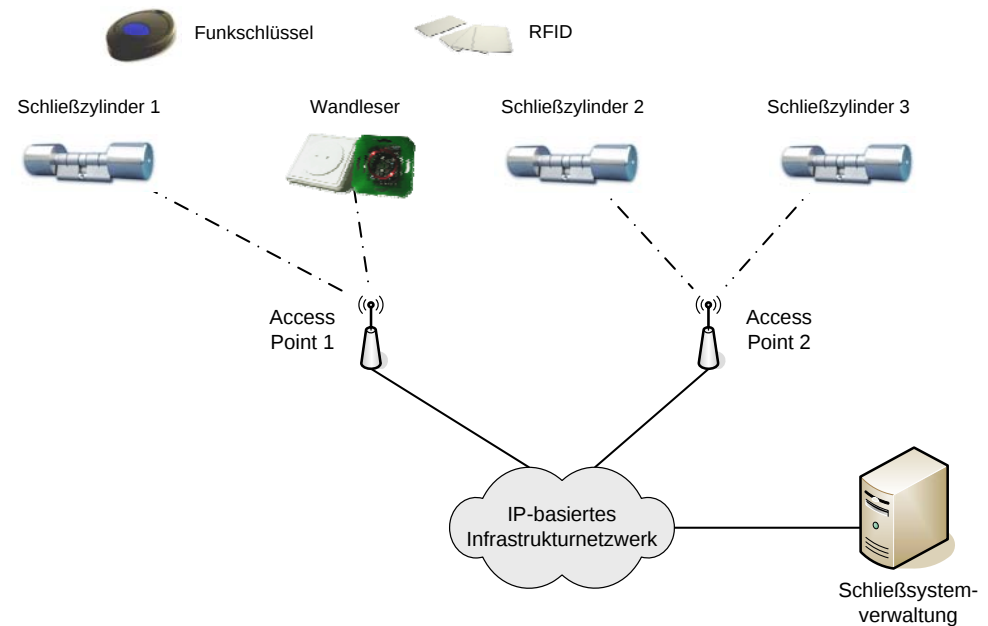


Topologie



Entwurfsgrundsätze

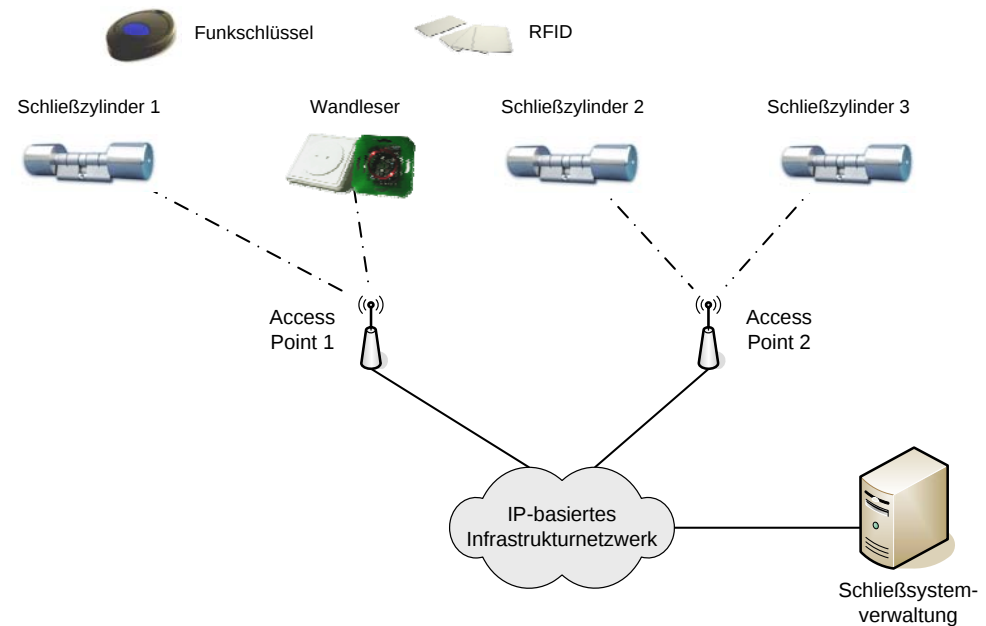
- Zuverlässigkeit
- Energieeffizienz
- Sicherheit
- Selbstorganisation
 - Selbstkonfiguration
 - Selbstheilung
 - Selbstschutz
 - Selbstoptimierung



Entwurfsgrundsätze

- **Zuverlässigkeit**

- Energieeffizienz
- Sicherheit
- Selbstorganisation
 - Selbstkonfiguration
 - Selbstheilung
 - Selbstschutz
 - Selbstoptimierung



Zuverlässigkeit bei drahtloser Kommunikation

Robustheit und Verfügbarkeit

- Verschiedene Modulations- und Bandspreizverfahren
- Diverse Fehlerschutz- und -korrekturmechanismen
 - Redundante Übertragung
 - Neuübertragung im Fehlerfall

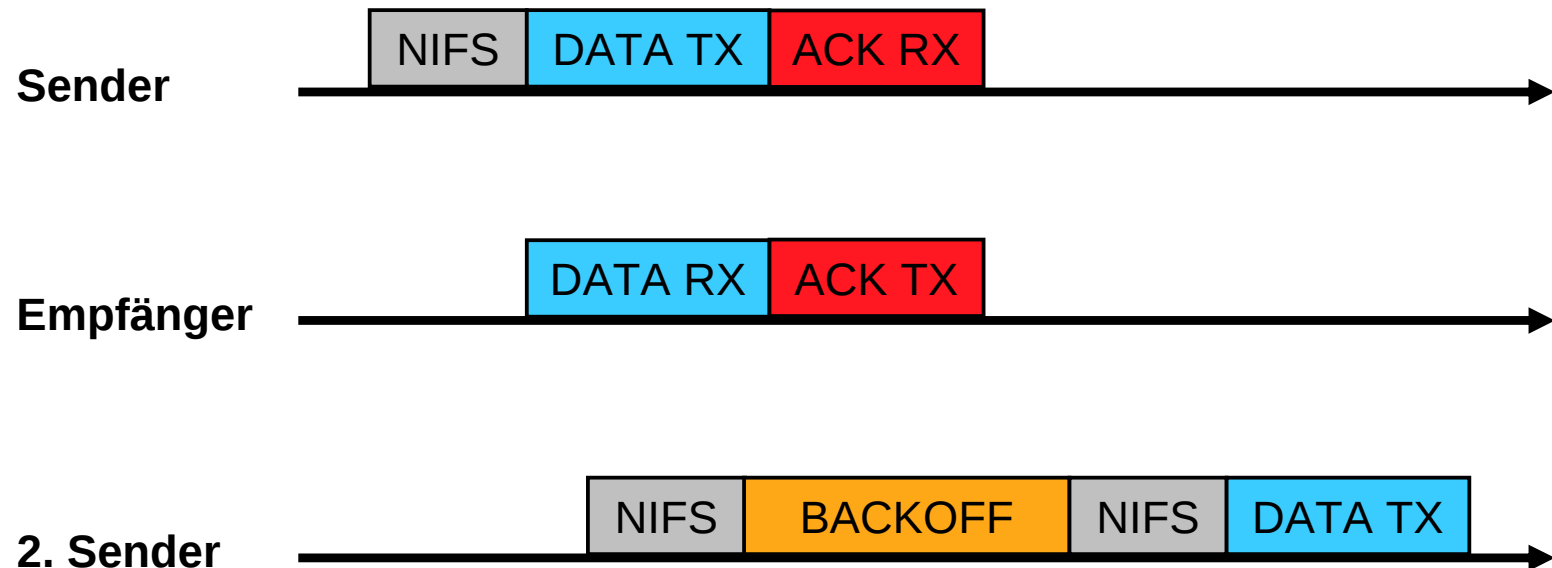
Bei geeigneter Auswahl und Kombination

- Einsatz in Umgebungen mit hohem Störpotential möglich
- Praxisbeispiel: Deutsche Firma steuert mobile Brennöfen über Bluetooth



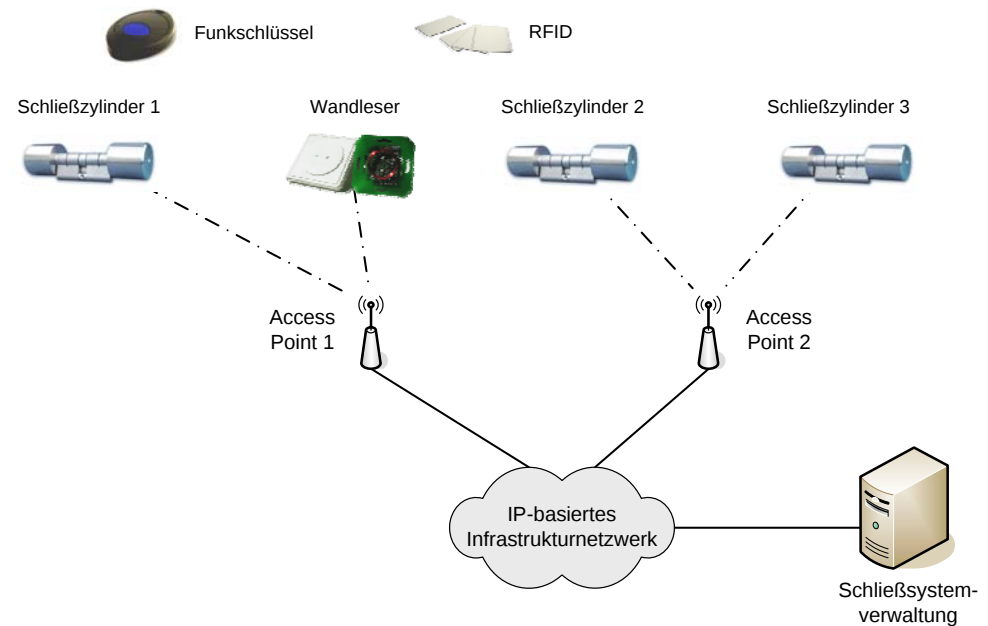
Zuverlässigkeit – MAC Schicht

- Abhören des Funkmediums bei Sendewunsch
- Warten für zufällige Backoff – Zeit bei belegtem Funkmedium
- Bestätigung von jedem Datenpaket durch ACK



Entwurfsgrundsätze

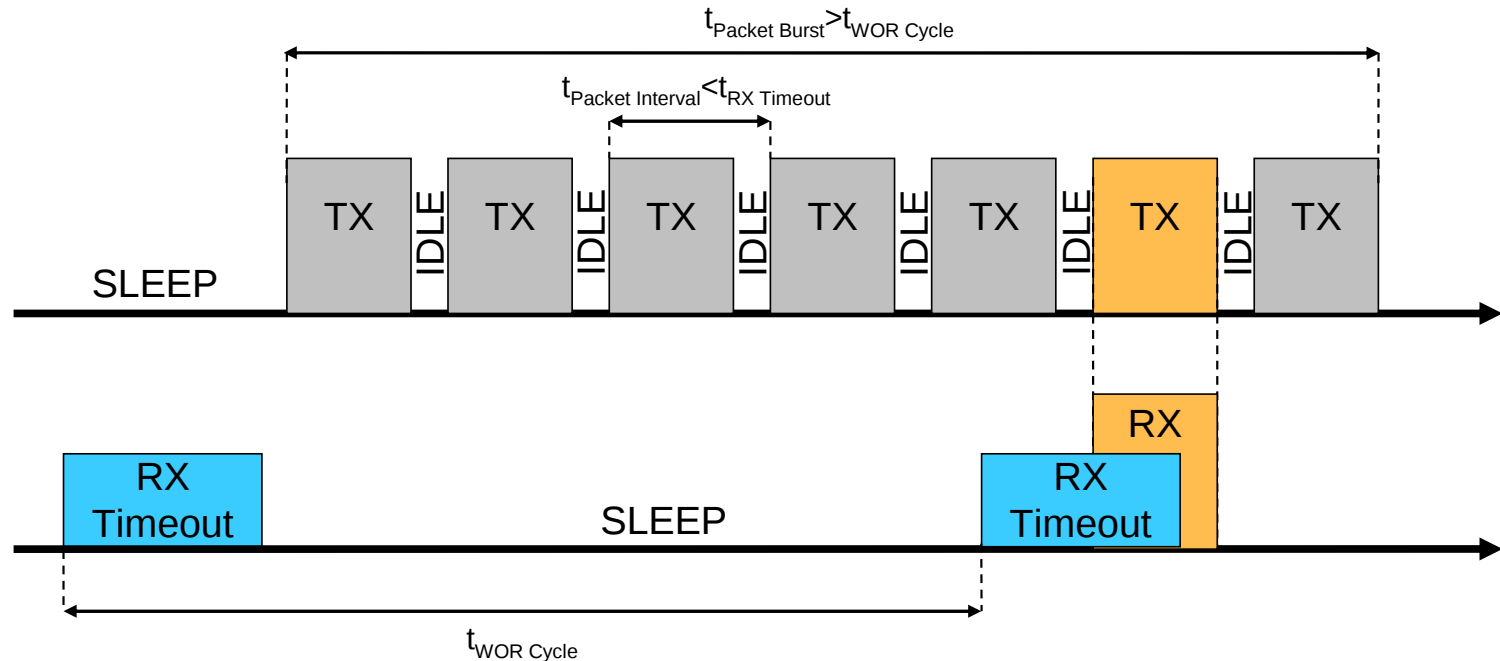
- Zuverlässigkeit
- **Energieeffizienz**
- Sicherheit
- Selbstorganisation
 - Selbstkonfiguration
 - Selbstheilung
 - Selbstschutz
 - Selbstoptimierung



Energieeffizienz - Wake on Radio, Sleep Modes

Wake on Radio

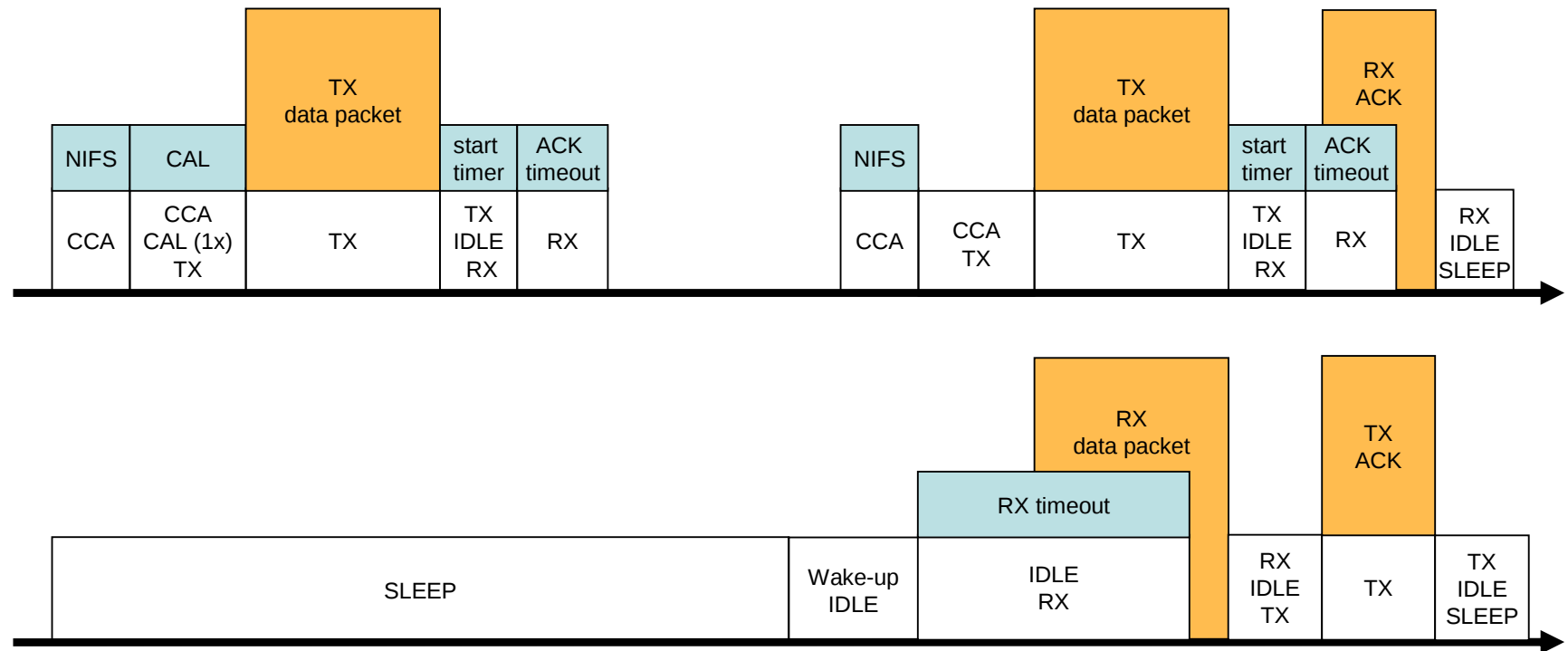
- Mikrocontroller im Sleep Mode
- Funkchip im Sleep Mode, wacht aber regelmäßig für kurze Zeit auf
- Funkchip weckt Mikrocontroller auf, wenn Daten vorhanden



Wake on Radio mit MAC-Schicht

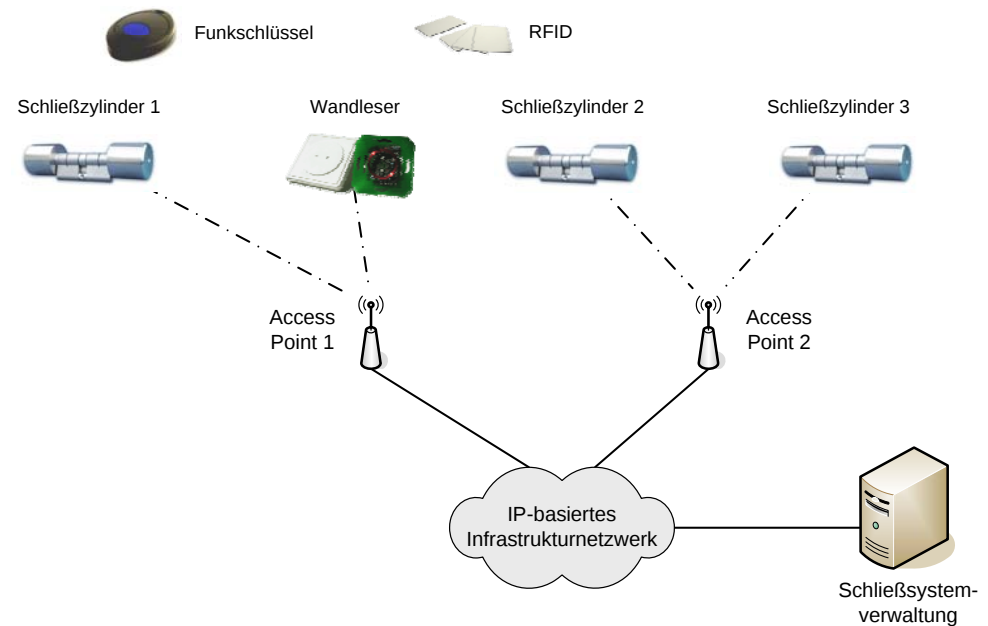
Energieeffiziente und zuverlässige Datenübertragung

- Packet Burst wird nach Empfang einer Bestätigung abgebrochen
 - Einsparung der Energie auch beim Sender
 - Geringerer Duty Cycle



Entwurfsgrundsätze

- Zuverlässigkeit
- Energieeffizienz
- **Sicherheit**
- Selbstorganisation
 - Selbstkonfiguration
 - Selbstheilung
 - Selbstschutz
 - Selbstoptimierung



Sicherheit

Abhörsicherheit und Vertraulichkeit

- Erreichbar durch Verschlüsselung (symmetrisch, asymmetrisch, hybrid)

Datenintegrität

- Erreichbar durch Message Authentication Codes
- Kryptographische Prüfsumme aus Daten und einem geheimen Schlüssel

Authentizität des Kommunikationspartners

- Nachweisbar durch Challenge-Response-Verfahren
- Nachweis von Kenntnis geheimer Informationen



Sicherheit - Challenge-Response-Verfahren

Challenge-Response zwischen

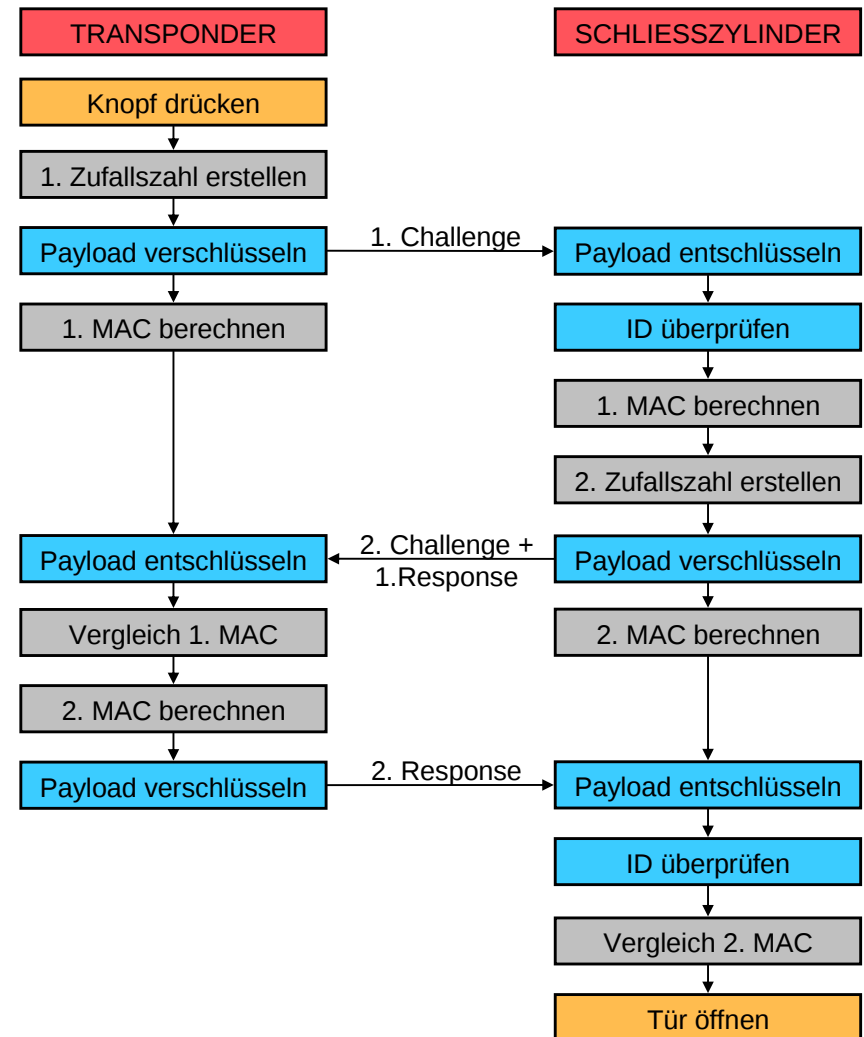
- Transponder - Schließzylinder
- Schließzylinder - Access Point
- Access Point - Verwaltung

Besonderheiten

- Keine Übertragung des geheimen Schlüssels
- Wichtig: Zuverlässiger Generator für Zufallszahlen

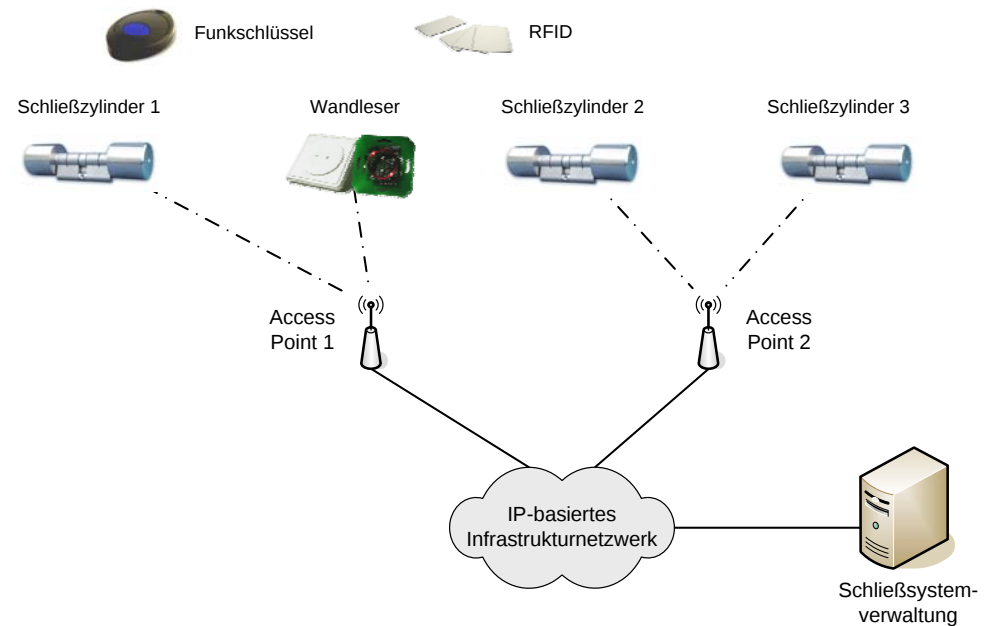
Verschlüsselung: AES 128 bit

Ablaufdauer: ca. 20 ms



Entwurfsgrundsätze

- Zuverlässigkeit
- Energieeffizienz
- Sicherheit
- **Selbstorganisation**
 - Selbstkonfiguration
 - Selbstheilung
 - Selbstschutz
 - Selbstoptimierung



Realisierte Selbstorganisation

Selbstkonfiguration

- Automatische Einbindung aller Netzkomponenten
 - Neue Zylinder
 - Neue Access Points

Selbstheilung

- Erkennung und Kompensation von Störungen
 - Zylinder-Ausfall
 - Access Point-Ausfall und verwaiste Zylinder

Selbstschutz

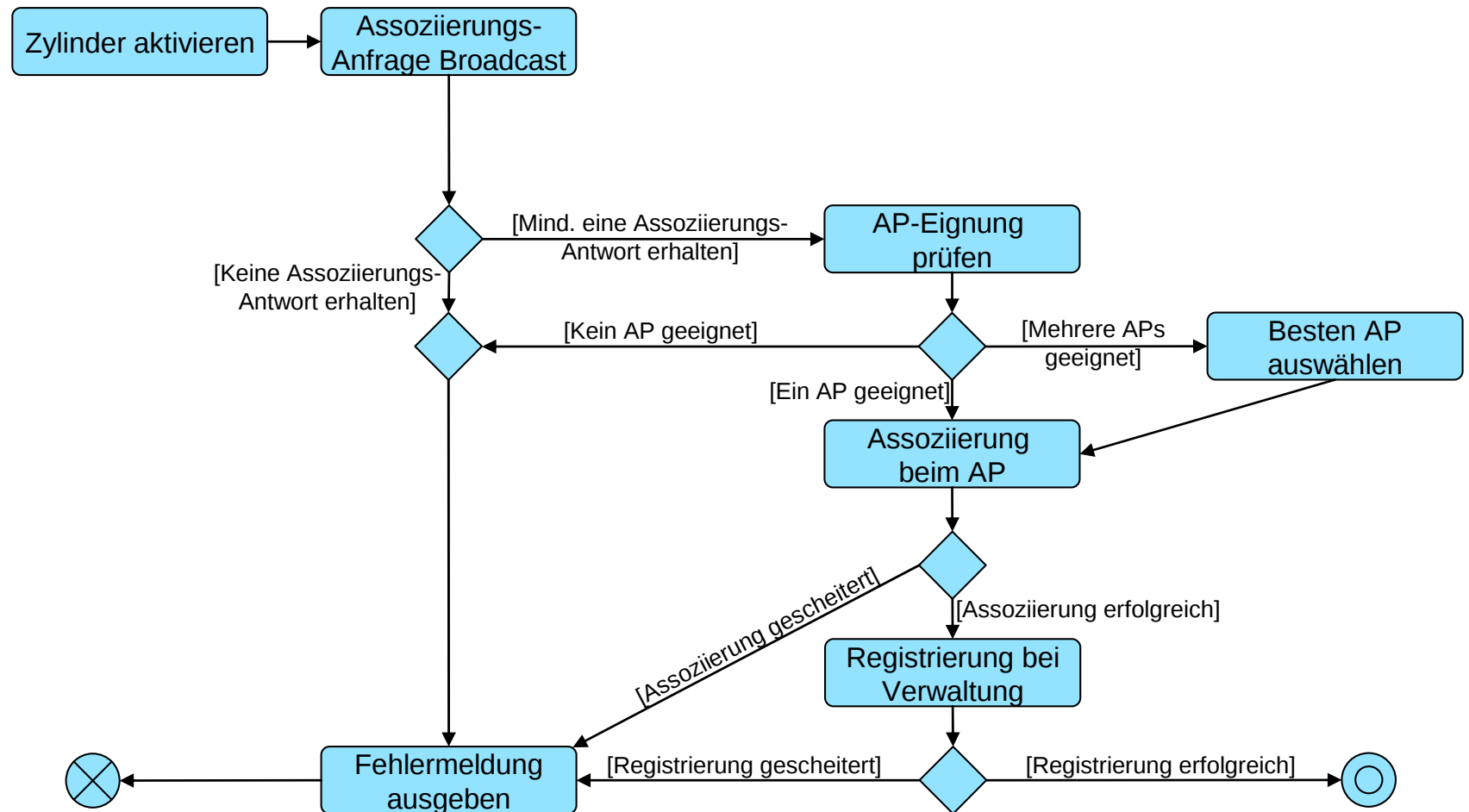
- Verschlüsselung, Authentifizierung

Selbstoptimierung

- Lastverteilung



Automatische Einbindung eines neuen Zylinders



Zusammenfassung

Drahtlose Kommunikation und sicherheitskritische Systeme sind kein Widerspruch!

- Einzelne Anforderungen erst mit Wireless praktikabel umsetzbar
- Herausforderung: Sicherheit und Anwendbarkeit
- Wesentlicher Aspekt: Selbstorganisation

Vorgestelltes Anwendungsbeispiel: Funkschließsystem

Ausblick

- Erweiterung um skalierbare Middleware für embedded Systeme
- Realisierung neuer Dienste für weitere Anwendungsbereiche, z.B.
 - Facility Management (Alarmanlagen, Jalousiensteuerung, ...)
 - Spezielle Anwendungen (Hotelgewerbe, Rechenzentren)



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



Fraunhofer
Einrichtung
Systeme der
Kommunikationstechnik



Fraunhofer Einrichtung
Systeme der
Kommunikationstechnik

Vielen Dank für Ihre Aufmerksamkeit!

Dipl.-Ing. Josef Jiru
089 547088-379
josef.jiru@esk.fraunhofer.de

Dr.-Ing. Markus Zeller
089 547088-352
markus.zeller@esk.fraunhofer.de