Sichere Kommunikation mit EuroBalise und GSM-R

Volker Knollmann

Deutsches Zentrum
für Luft- und Raumfahrt e.V.
in der Helmholtz-Gemeinschaft

Motivation

Wozu „sichere“ Kommunikation?

Quelle: Heise Verlag, c't

Motivation

Wozu „sichere“ Kommunikation?

Boeing's new 787 Dreamliner passenger jet may have a serious security vulnerability in its onboard computer networks that could allow passengers to access the plane's control systems, according to the U.S. Federal Aviation Administration.

The computer network in the Dreamliner's passenger compartment, designed to give passengers in-flight internet access, is connected to the plane's control, navigation and communication systems, an FAA report reveals.

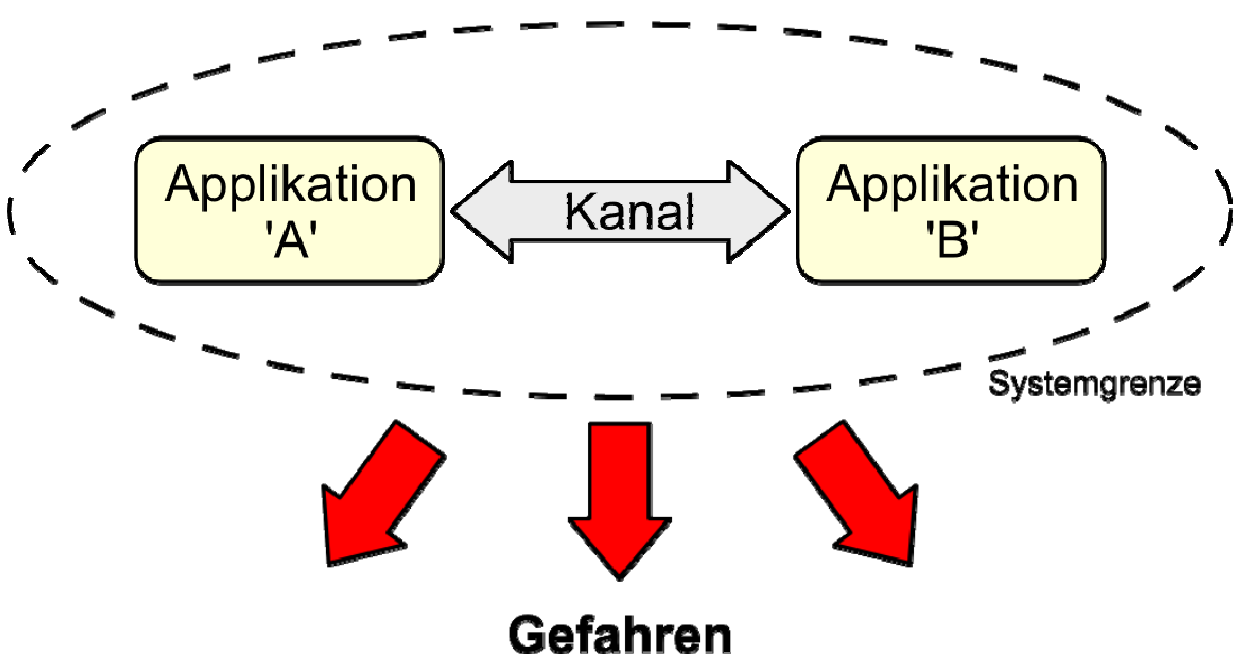
Quelle: Online-Magazin „Wired“, 04. Jan. 2008

Vortragsinhalt

- Aspekte „sicherer“ Kommunikation
  - Safety (Gefährdungen aus dem System heraus)
  - Security (Gefährdungen durch Externe)
- Transponderbasierte Funkdatenübertragung im Bahnbereich
  - Übertragungsverfahren der EuroBalise
  - Mögliches „Angriffsszenario“ auf EuroBalisen
- Netzwerkbasierte Funkdatenübertragung im Bahnbereich
  - GSM-R (Architektur, Netz und Authentifizierung)
- Zusammenfassung, Diskussion, Überleitung zum Folgevortrag

Safety und Security

Endogene Gefahr vs. exogene Gefährdung

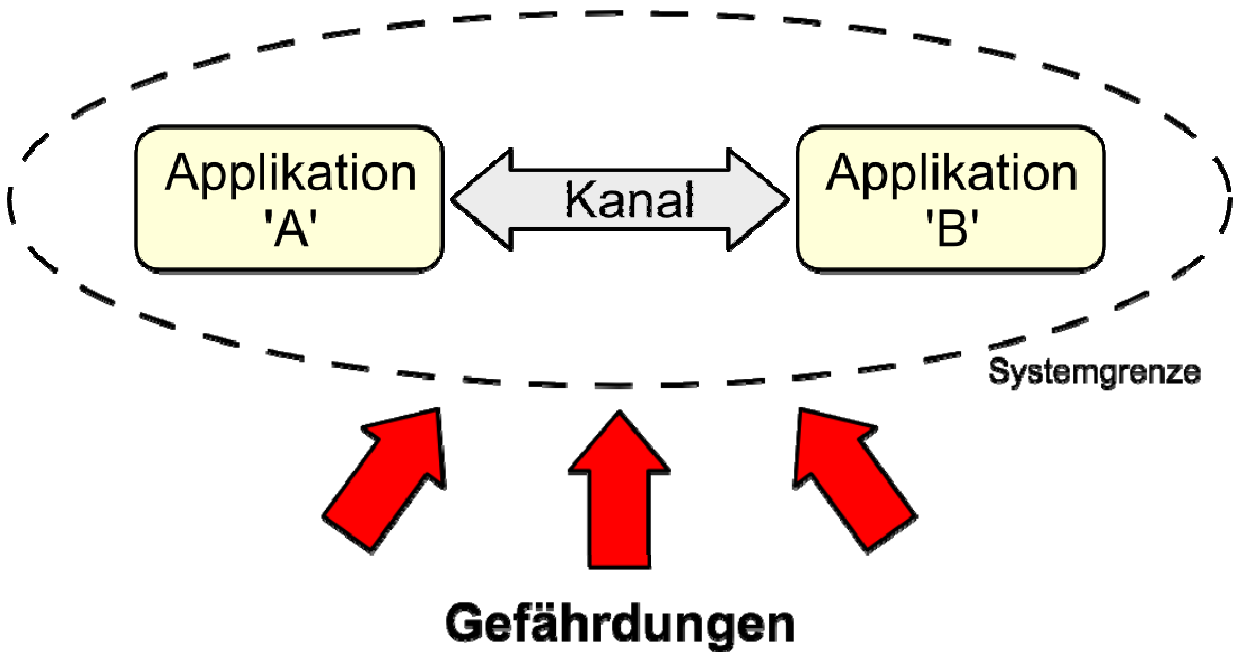


- Ausfall oder Störung des Kanals ohne Beteiligung Dritter (endogen)
- Kanalstörung führt zu fehlerhaftem Systemverhalten
- Systemverhalten mündet in Gefahr bzw. Risiko für Andere

➔ **Safety**

Safety und Security

Endogene Gefahr vs. exogene Gefährdung



- Kommunikationsbeeinträchtigung durch äußere Einwirkung (exogen)
- Beeinträchtigung führt zu fehlerhaftem o. ungewolltem Systemverhalten
- Systemverhalten mündet in Gefahr bzw. Risiko für Andere

➔ **Security**

Beispiele für Safety-bezogene Störungen
Beeinflussung der Kanalqualität

- Minderung der Signalqualität durch…
  - Rauschen
  - EMV-Störungen (EMV = Elektromagnetische Verträglichkeit)
  - Signallaufzeiten, Abschattung, Mehrwegeempfang (Funk)

  ➔ fehlerhafter und/oder nicht zeitgerechter Nachrichtenempfang

- Totalausfall des Kanals durch…
  - Leitungsbeschädigung
  - Ausfall von Infrastruktur (Router, Bridges, Konzentrator, …)
  - Stromausfall

  ➔ kein Nachrichtenempfang (nicht immer detektierbar!)

Beispiele für Security-bezogene Störungen
Vorsätzliche Beeinflussung durch Dritte

- Gezieltes Herbeiführen eines Kanalausfalls oder einer Kanalstörung

  ➔ Konsequenzen: siehe voherige Seite

- Abhören oder Protokollieren von Daten

  ➔ kein unmittelbarer Schaden,
  kann aber der Vorbereitung dienen

- Veränderung von Daten oder Einbringen eigener Daten
  (Wiederholen, Löschen, Einfügen, Umsortieren, Korrumpieren, Verzögern)

  ➔ Fehlerhaftes oder ungewolltes Systemverhalten,
  nicht immer detektierbar!

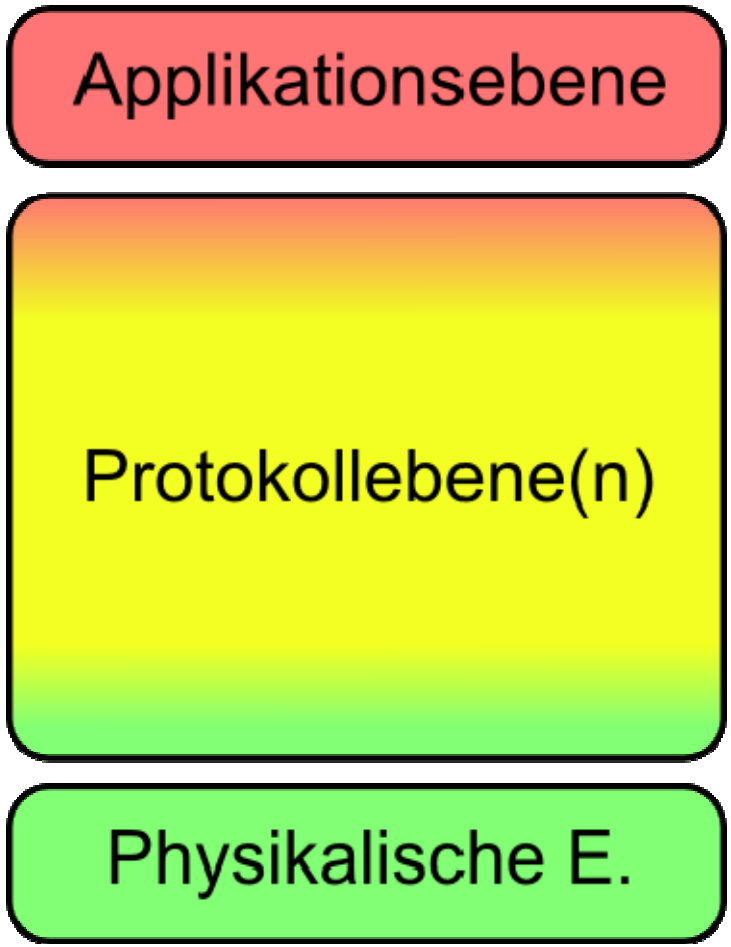
Maßnahmen gegen Safety- o. Security-Einflüsse

Robuste Kanäle, Kryptographie, Zugangsbeschränkung

- Auswahl störunempfindlicher Übertragungsverfahren und Modulationen
- Verwendung geeigneter Protokolle inkl. Fehlererkennung
- Einsatz kryptographischer Verfahren
- Zugangsbeschränkung zu Anlagen, Leitungen und Netzen
  - physikalisch
  - logisch (z. B. Zugriff über andere Netze)

Implementierungsebenen für robuste Übertragungen

Physik, Datensicherung, Applikation



Applikation:

- Plausibilitätscheck
- Check gegen (dyn.) Randbedingungen

Protokoll:

- Kryptographie
- Prüfsummen
- Redundanz
- Authorisierung / Authentifizierung

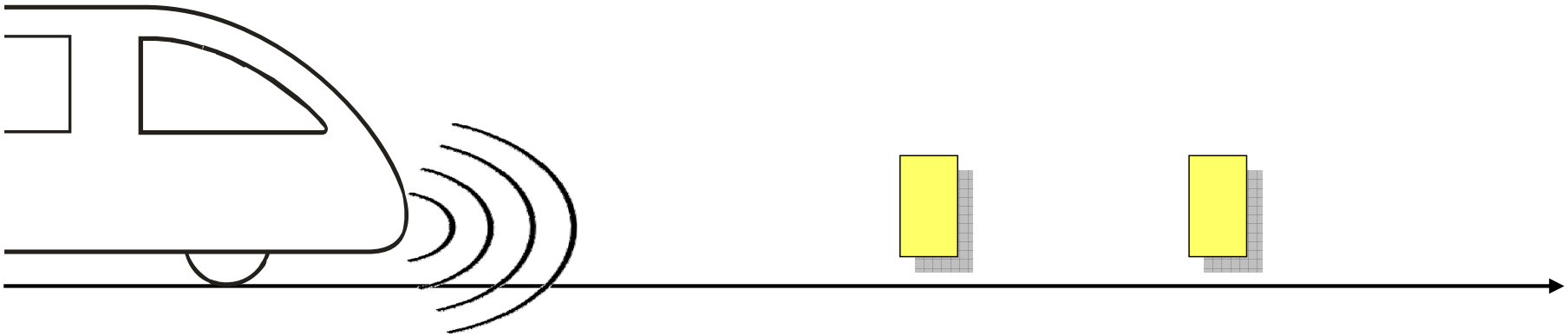
Physikalische Ebene:

- Modulation, Buszugriff, …

Praxisbeispiel EuroBalise
Funktionsweise

- Passiver Transponder im Gleis
- Sendet vorab gespeicherte Datentelegramme bei Anregung durch Zug
- Telegramminhalt: Streckeninformation, Signalbegriffe, Ortung

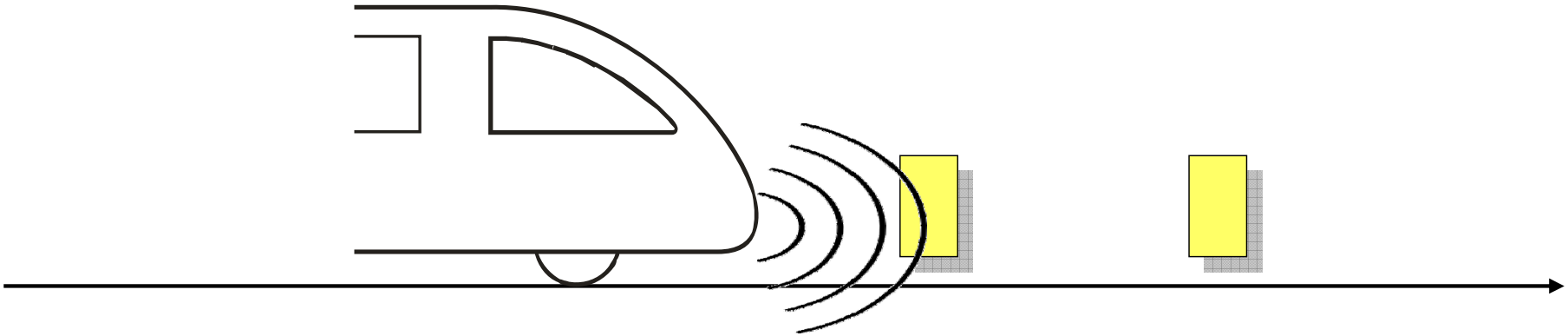
➔ **sicherheitsrelevant!**



Praxisbeispiel EuroBalise
Funktionsweise

- Passiver Transponder im Gleis
- Sendet vorab gespeicherte Datentelegramme bei Anregung durch Zug
- Telegramminhalt: Streckeninformation, Signalbegriffe, Ortung

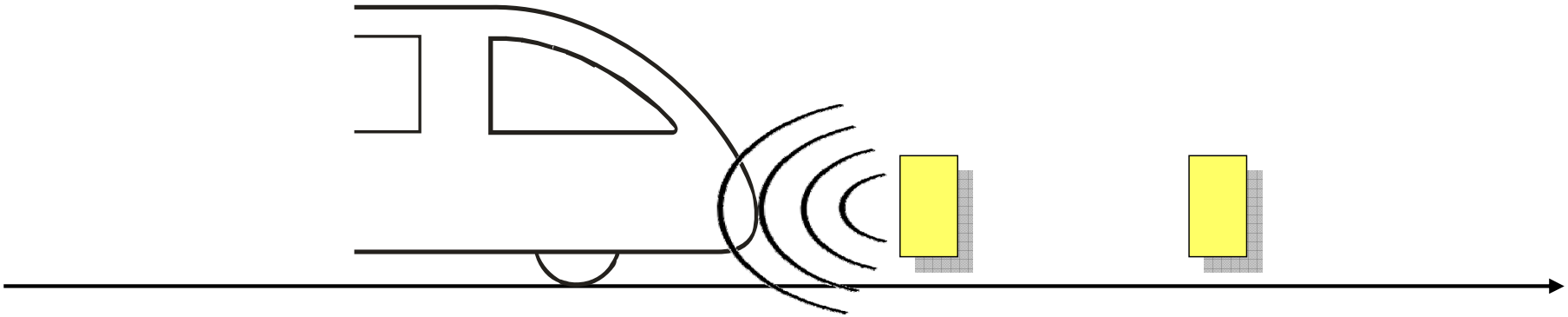
➔ **sicherheitsrelevant!**



Praxisbeispiel EuroBalise
Funktionsweise

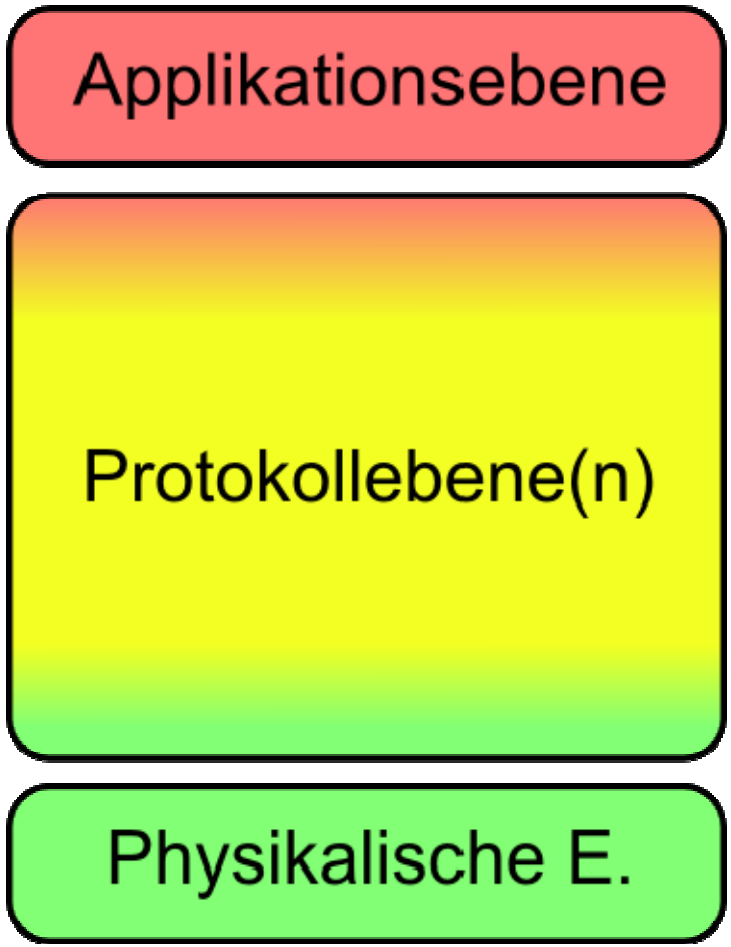
- Passiver Transponder im Gleis
- Sendet vorab gespeicherte Datentelegramme bei Anregung durch Zug
- Telegramminhalt: Streckeninformation, Signalbegriffe, Ortung

➔ **sicherheitsrelevant!**



Praxisbeispiel EuroBalise

Eingesetzte Sicherungsverfahren



Applikation:

- Linking (Balisen verweisen aufeinander)
- Check: Empfangsdauer vs. Geschw.

Protokoll:

- 10-zu-11-Bit-Substitution
- Scrambling
- CRC-ähnliche Checksumme
- Besondere Anf. an gültige Telegramme

Physikalische Ebene:

- Modulation: Frequenzumtastung („FSK“)
- Nutzung der magnetischen Kopplung

Praxisbeispiel EuroBalise

Sicherungsverfahren auf Applikationsebene

- Linking
  - Balisen werden mit ID und Ort angekündigt
  - Bei unerwarteten oder fehlenden Balisen: Sicherheitsreaktion

- Check: Empfangsdauer vs. Geschwindigkeit
  - Empfangsfenster der Balisendaten: ca. +/- 1 m um Balisenmitte
  - Tatsächliche Empfangsdauer wird gemessen
  - Vergleich mit theoretischer Empfangsdauer aus Zuggeschwindigkeit
  - Bei Abweichung: Notbremse

Praxisbeispiel EuroBalise

Sicherungsverfahren auf Protokollebene (1)

- 10-zu-11-Bit-Substitution
  - Ersetzen eines 10-Bit-Datenwortes durch ein 11-Bit-Datenwort
  - D. h. Abbildung von 1024 Datenworten auf 2048 Datenworte
  - Es verbleiben 1024 ungültige Datenworte
  - Dadurch Erkennung von Einzelbitfehlern möglich

- Scrambling:
  - Verwürfeln des gesamten Telegramms durch ein Schieberegister
  - Burst-Fehler werden so zu Einzelbitfehlern zerschlagen
  - Dadurch verbesserte Erkennung von Burst-Fehlern

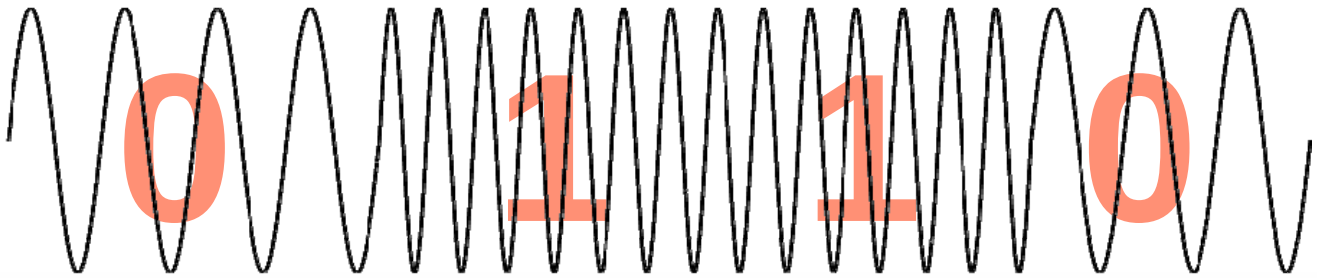
Praxisbeispiel EuroBalise
Sicherungsverfahren auf Protokollebene (2)

- CRC-ähnliche Checksumme
  - Prüfsumme von 85 Bit Länge
  - Bildung durch Division der Nutzdaten mit vordefiniertem Polynom
  - Dadurch weiterer Schutz gegen Übertragungsfehler
- Weitere Randbedingung an das Telegramm:
  - Keine unzulässige Periodizität
  - Unterabtastung muss ungültiges Telegramm ergeben
  - „Off-Synch-Parsing Condition“:
    - Telegramm wird zyklisch gesendet
    - Empfänger muss Telegrammstart im Datenstrom detektieren
    - Fehlerhafte Wahl des Telegrammstarts darf keinen gültigen Inhalt ergeben.

Praxisbeispiel EuroBalise

Sicherungsverfahren auf physikalischer Ebene

- Modulationsart: Frequenzumtastung
  - Null: 3,951 MHz, Eins: 4,516 MHz, Sinus, stetiger Phasenverlauf
  - Relativ störunempfindlich (vgl. z. B. Amplitudenmodulation)
  - Leicht zu erzeugen
  - Leicht demodulierbar, schmalbandiger Empfänger ausreichend
- Verwendung der magnetischen Feldkopplung
  - Keine Beeinträchtigung durch Wasser / Eis / Schnee
  - Effizient bei geringen Abständen zw. Sender und Empfänger



Praxisbeispiel EuroBalise

Eingesetzte Sicherungsverfahren

Applikation:

- Linking (Balisen verweisen aufeinander)
- Check: Empfangsdauer vs. Geschw.

Alles

Security?

Safety!

Physikalische Ebene:

- Modulation: Frequenzumtastung („FSK")
- Nutzung der magnetischen Kopplung

Praxisbeispiel EuroBalise

Mögliche „Angriffe“ (Security)

Abschrauben bzw. mit Eisen/Stahl abdecken

- Kein erhöhtes Risiko wg. Linking
- Gleicher Effekt wie Ausfall der Balise

Aussenden eines Störsignals

- Kein erhöhtes Risiko wegen umfangreicher Kanalkodierung
- Dadurch zuverlässige Erkennung von Übertragungsfehlern

Einfügen einer neuen, manipulierten Balise

- Wird anhand der Linking-Information detektiert (vereinfachte Aussage!)
- Kein erhöhtes Risiko

➔ Einzige Möglichkeit: Manipulation einer bestehenden Balise!

Praxisbeispiel EuroBalise

Manipulation einer bestehenden Balise

Grundsätzlich:

- Entweder Umprogrammieren der bestehenden Balise oder Austausch durch andere Balise
- Balisen und Programmiergeräte sind im Handel (frei verkäuflich?)
- Spezifikationen sind öffentlich

Aufbereitung der manipulierten Daten:

- Auffinden eines geeigneten Streckenpunktes
- Auslesen der alten Balise und Bestimmung wichtiger Parameter (ID, …)
- Erstellen des „Schadtelegramms“ unter Berücksichtigung der Parameter

Praxisbeispiel EuroBalise

Ansatzpunkte für manipulierten Telegramminhalt

Einstreuen eines ungültigen Fahrbefehls:

- Dadurch z. B. Einfahrt in besetzten Abschnitt möglich
- Aber: Widerspruch zu Außensignalen! Streckenkenntnis des Tf!

Ändern der Geschwindigkeitsvorgaben (z. B. Langsamfahrstellen):

- Dadurch z. B. Entgleisen an Weichen möglich
- Aber: Streckenkenntnis des Tf! Evtl. Widerspruch zu Beschilderung!

Ändern des Gradientenprofils (Änderung: Gefälle → Steigung):

- Dadurch falsche Berechnung der Bremskurven
- Wird Bremseingriff des Systems notwendig, fährt der Zug zu weit
- Aber: Streckenkenntnis! Setzt Fehlhandlung des Tf voraus!

Praxisbeispiel EuroBalise
Fazit der Security-Betrachtung

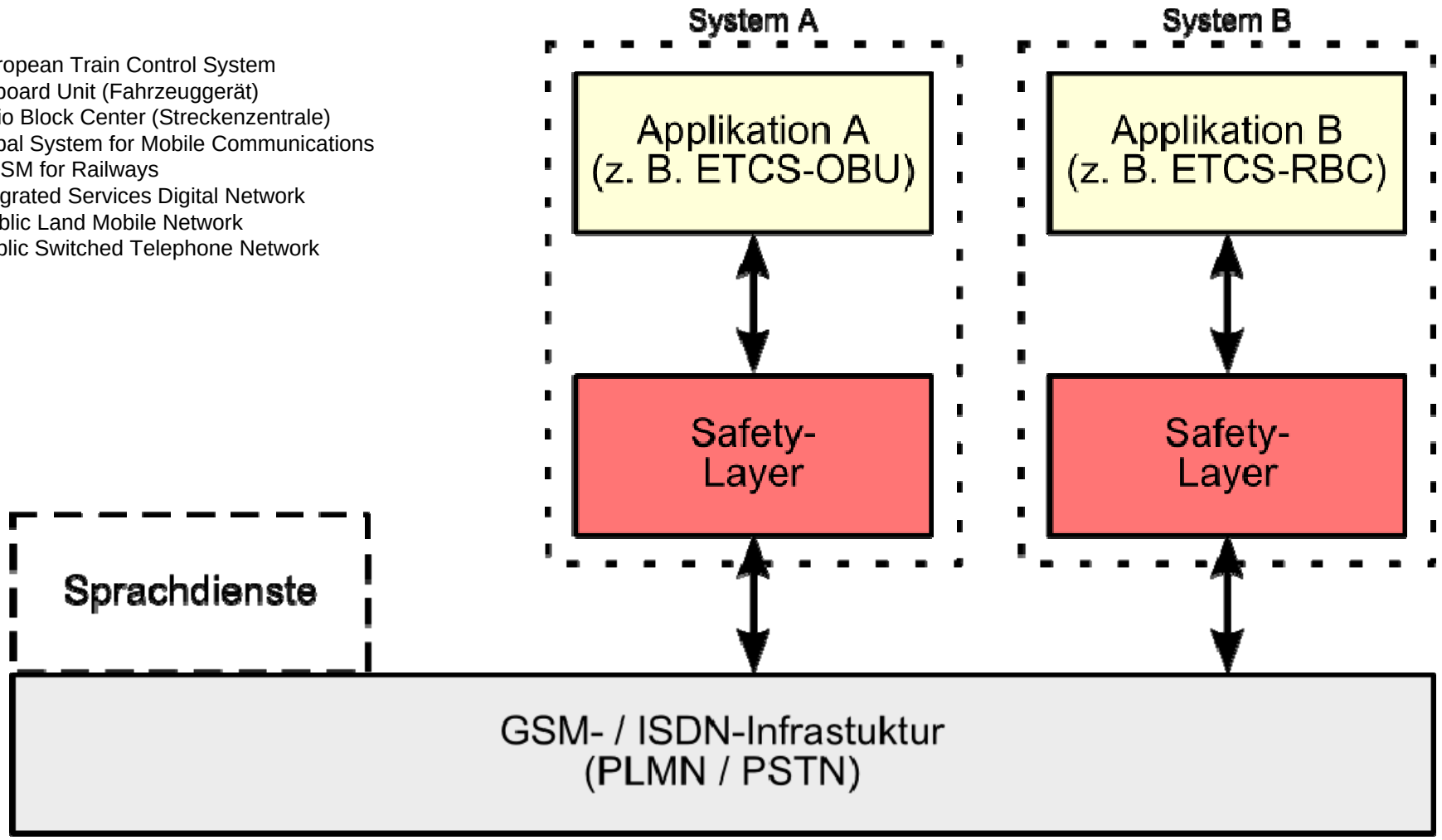
- Umfangreiches Expertenwissen notwenig
- Beschaffung bzw. Entwicklung von Spezialgeräten notwendig
- Erheblicher Aufwand bei Telegrammerstellung und –einschleusung
- **Vergleichsweise geringes Risiko eines Schadenseintritts**

- Aber: „**Denial of Service**“ durch Herbeiführen von Zwangsbremsungen ist relativ einfach realisierbar!

GSM-R

Authentifizierung im GSM-R-System
Systemstruktur

ETCS: European Train Control System
OBU: On-board Unit (Fahrzeuggerät)
RBC: Radio Block Center (Streckenzentrale)
GSM: Global System for Mobile Communications
GSM-R: GSM for Railways
ISDN: Integrated Services Digital Network
PLMN: Public Land Mobile Network
PSTN: Public Switched Telephone Network



Authentifizierung im GSM-R-System
Rolle von Safety-Layer und GSM-R-Infrastruktur

GSM-R-Infrastruktur:

- Authentifiziert den *Netzteilnehmer*
- Verschlüsselt den Datenverkehr

Safety-Layer:

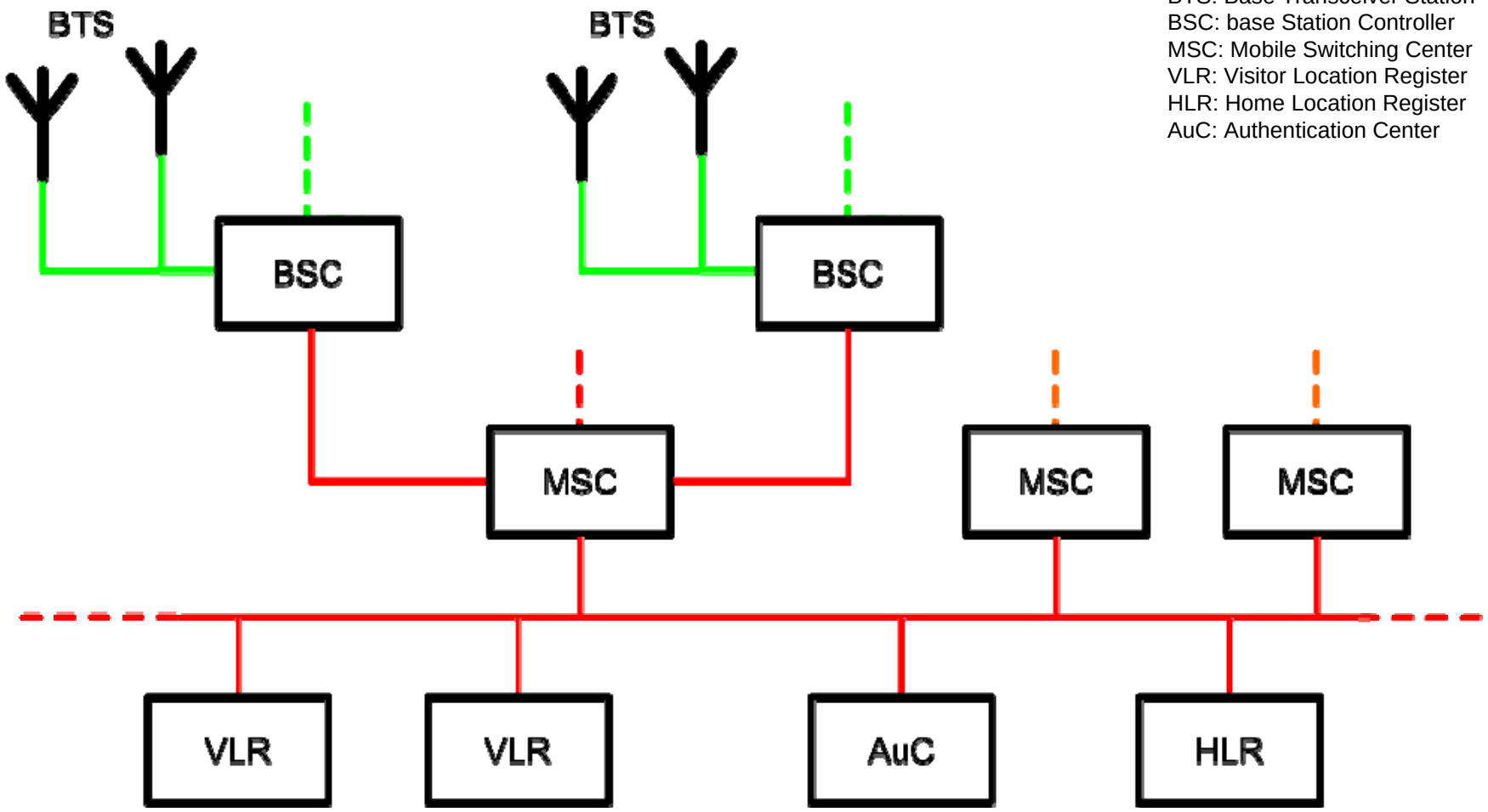
- Authentifiziert die beteiligten *ETCS-Geräte*
- Stellt die Datenintegrität sicher (inkl. Senderauthentifizierung)

Gemeinsamkeiten:

- Verwendung eines „Pre-Shared-Key“ (PSK)
- Erzeugung eines Sitzungsschlüssels aus PSK und Zufallszahl

Authentifizierung im GSM-R-System

Netzaufbau



BTS: Base Transceiver Station
BSC: base Station Controller
MSC: Mobile Switching Center
VLR: Visitor Location Register
HLR: Home Location Register
AuC: Authentication Center

Authentifizierung im GSM-R-System
Notwendigkeit für Safety-Layer und AuC

- Kommunikation erfolgt über Netze mit …
  - unbekannten Teilnehmern
  - unbekannter Teilnehmerzahl
  - „non-safe“ Hardware
  - nicht-deterministischem Routing
  - evtl. keiner oder nur eingeschränkter Kontrolle über das Netz

- Daher notwendig:
  - Prüfung der Netzzugangsberechtigung und der ETCS-Kennung
  - Verschlüsselung der Daten
  - Überprüfung der Datenintegrität (Sender und Inhalt)

  … um Manipulationen durch Dritte zu verhindern

Zusammenfassung

- „Sichere“ Kommunikation umfasst Safety- und Security-Aspekte.
- Mögliche endogene (Safety) oder exogene (Security) Fehler sind Wiederholen, Löschen, Einfügen, Umsortieren, Korrumpieren oder Verzögern von Nachrichten.
- Mögliche Ursachen sind Rauschen, EMV, Hardware- / Stromausfälle, Softwarefehler, Kabelfehler oder vorsätzliche Manipulation.
- Die Balisenkommunikation ist durch robuste Modulation, umfangreiche Kanalkodierung und Konsistenzprüfungen auf Applikationsebene effektiv gegen Übertragungsfehler geschützt.
- Security-Angriffe gegen Balisen sind möglich, aber aufwändig.
- GSM-R wird über ein problematisches Medium (Luft) und zum Teil über offene Netze abgewickelt. Daraus resultieren besondere Anforderungen.
- GSM-R stellt durch mehrfache Authentifizierung und Verschlüsselung die Identität der Kommunikationsparter sowie die Datenintegrität sicher.