Sichere Lokalisierung und Nachweisführung durch Galileo PRS

OMNISECURE
Berlin, 21. Januar 2020

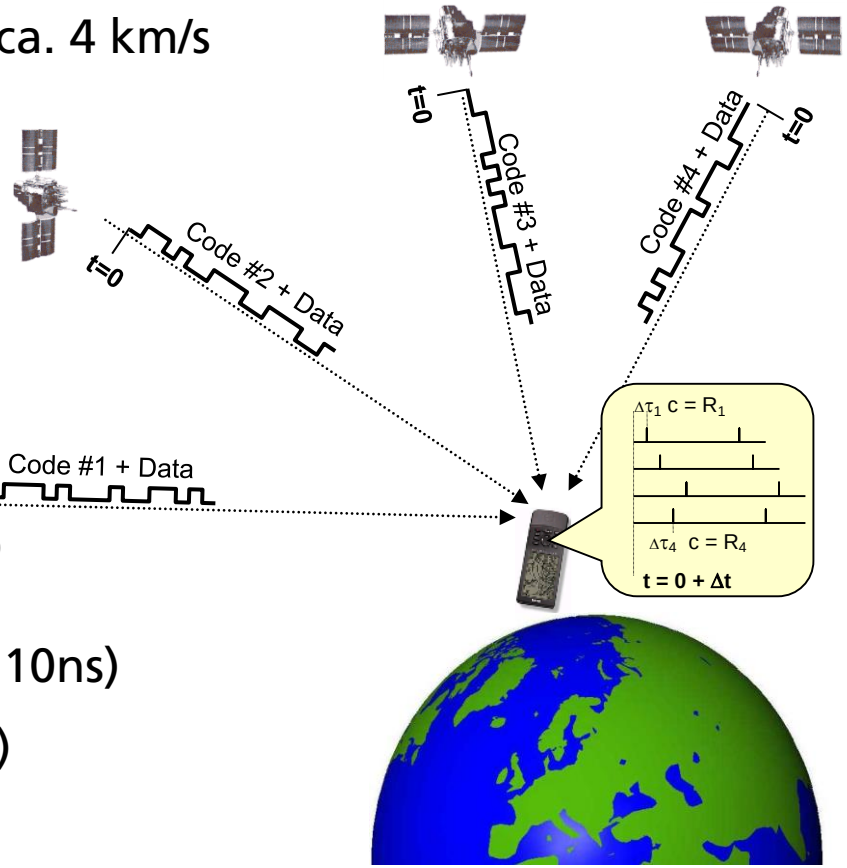
Alexander Rügamer

alexander.ruegamer@iis.fraunhofer.de
Fraunhofer IIS, Nürnberg

Fraunhofer IIS

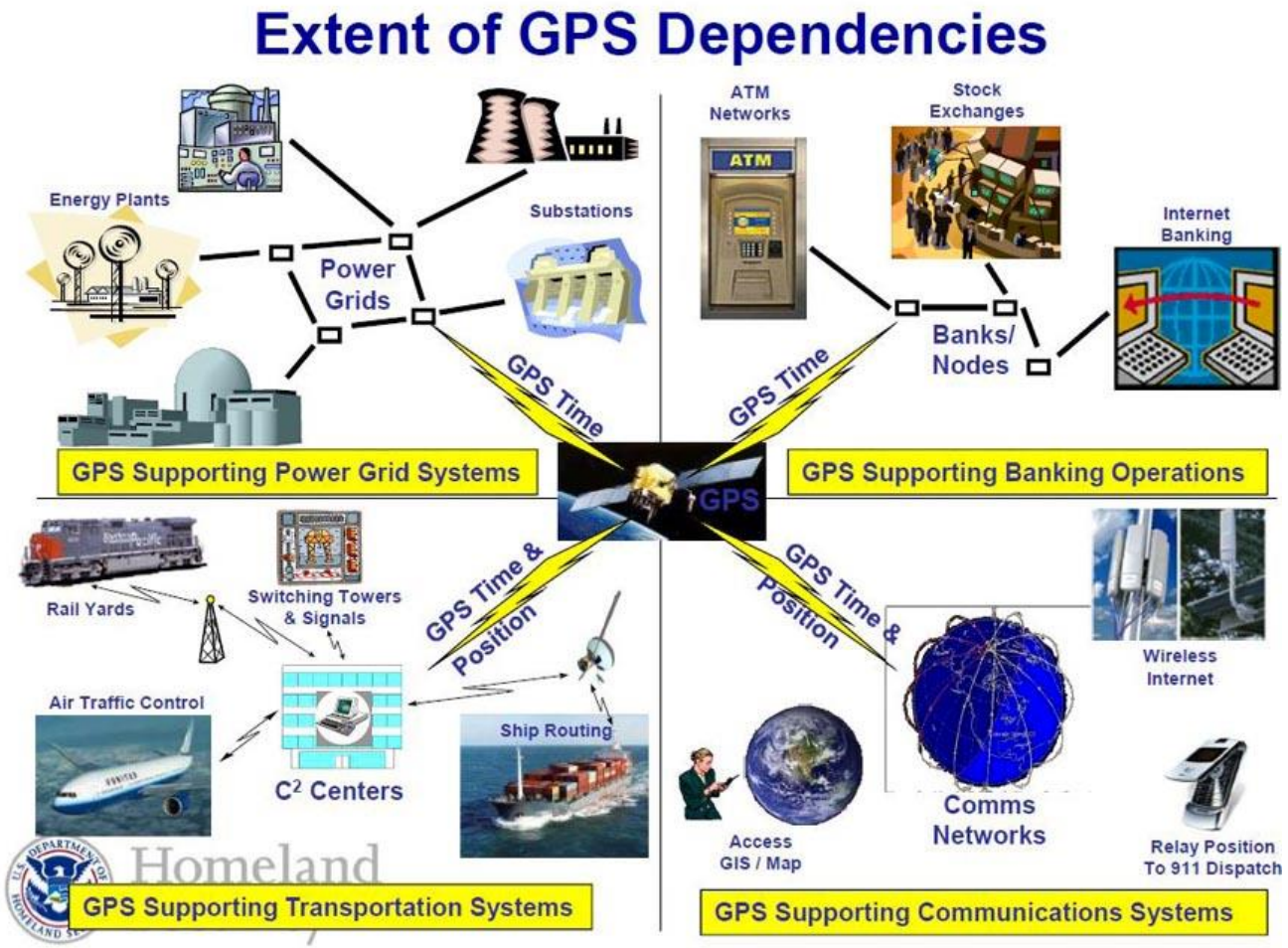
Motivation
Prinzip Satellitennavigation

- Satelliten bewegen sich in ca. 20.000 km Höhe um die Erde mit ca. 4 km/s
  - Senden aktuelle Position mit Zeitstempel und Navigationsnachricht (Bahndaten, Korrekturdaten, etc.)
- Empfänger werten gleichzeitig min. 4 Satelliten aus
  - ➔ Ermittlung 3D-Position und Zeit
- Alleinstellungsmerkmale Satellitennavigation:
  - Weltweit ohne Infrastruktur verfügbar
  - Unabhängig von Wetter, Ländergrenzen, etc.
  - Hohe Genauigkeiten (Position: Meter bis Zentimeter; Zeit: < 10ns)
  - Günstige und miniaturisierte Empfänger (passiver Empfang!)
  - „Immer“ verfügbar ?!



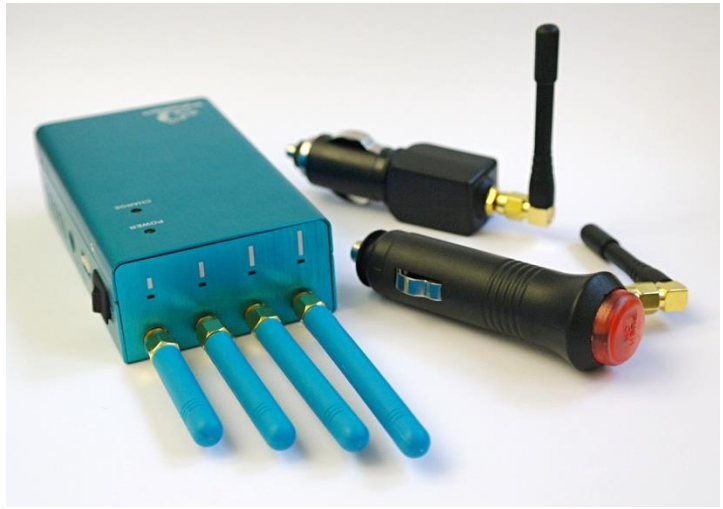
Motivation

Vielfältige Anwendungen…. auch in sicherheitsrelevanten Bereichen



Quelle: http://www.insidegnss.com/auto/popupimage/GPS%20Dependencies_small.jpg

GNSS Störungen und Vorfälle
Jamming



- “Personal” oder “Privacy Protection Devices” (PPD)s
  - Werden über das Internet (z.B. eBay) ab 30€ verkauft
  - Kauf ist legal, Verwendung weltweit illegal
- Einsatzgebiete:
  - GPS-basierenden Auto-Diebstahlschutz ausschalten
  - „Pay-as-you-drive“-Versicherungen umgehen
  - „Fleet Management Systems“ ausweichen
  - Privatsphäre von Paketzustellern vor ihren Arbeitgebern schützen
- Beworben werden PPDs mit
  “…protect the privacy of its user in a radius of at least 15 m...”
  - Nutzer wissen nicht, was sie damit wirklich anrichten…

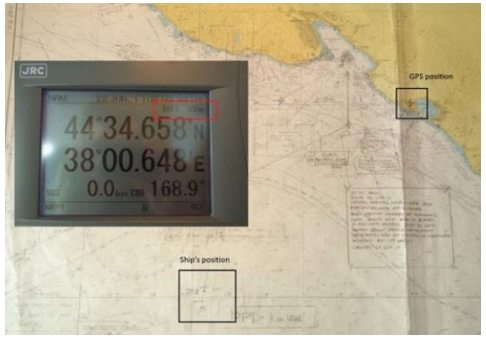
GNSS Störungen und Vorfälle
Jamming

- FCC bestraft GPS PPD Jammer Nutzer für Störung des Newark Airport GBAS (2013)
  - Ähnliche Vorfälle finden täglich statt, auch in Deutschland
- Car-jammer Monitoring-Kampagne:
  - München, Deutschland A9
    ca. 6 Jamming-Vorfälle pro Woche
  - London, UK
    ca. 10 Jamming-Vorfälle pro Tag
- 40 von 100 Drohnen für Licht-Show durch Jamming abgestürzt und massiven Schaden verursacht (2018)

http://insidegnss.com/criminal-investigation-underway-in-gps-jamming-incident-that-crashed-drones-caused-hk1m-in-damage/

GNSS Störungen und Vorfälle
Spoofing

- Spoofing: Übertragung eines gefälschten GNSS-Signals
- Zweck: Vortäuschen einer GNSS-Empfänger-Positions- bzw. Zeitlösung
- „Proof-of-Concept“, u.a. University of Austin, Texas:
  - 2012: Drohnen-Fernsteuerung
  - 2013: Selbstbau GPS “Spoofer” für $3,000 und spoofen 80-Millionen-$-Yacht
- „Realität“:
  - 2016: „Pokemon Go“-Spoofer mit HackRF frei verfügbar, <250€ Hardware-Kosten
  - 2017, 22-24. Juni „Spoofing in the Black Sea”
    - GPS-Position von 20 Schiffe plötzlich 25 Nautische Meilen falsch
    - Schiffsposition „auf Land“
  - 2019 „Thousands of GPS spoofing incidents have occurred in Shanghai since July 2018“
    - Bisher unbekannte Herkunft und Intension



Shepard, et al. “Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks”. ION GNSS 2012, Nashville, TN, September 2012, pp. 3591-3605., 2012.
https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea
https://insidegnss.com/sinister-spoofing-in-shanghai/

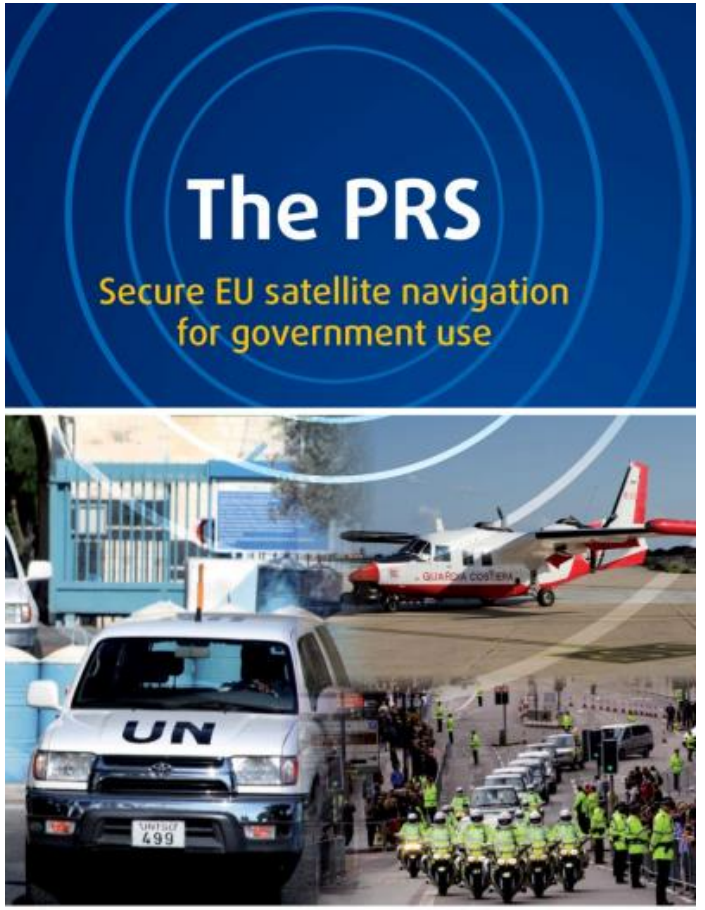
Fraunhofer IIS

Galileo PRS

Galileo PRS = Sicherheit

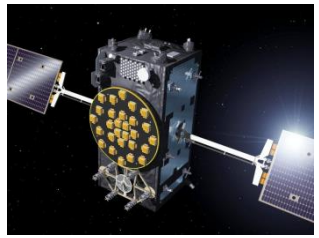
PRS
Public Regulated Service
Secure, robust and always available

- Galileo bietet drei globale SatNav-Dienste:
  - Open Service (OS)
  - Commercial Service (CS)
  - Public Regulated Services (PRS)
- Galileo PRS ist ein verschlüsselter und besonders geschützter SatNav-Dienst (Anti-Spoofing, Anti-Jamming)
- Sichere Signale für Zeit- und Positionsdaten beim Einsatz in kritischer Infrastruktur und Militär
- Entspricht dem militärischen GPS (PPS, M-Code) allerdings unter europäischer Kontrolle
- Unabhängige, sichere und robuste GNSS-Lösung



Fraunhofer IIS

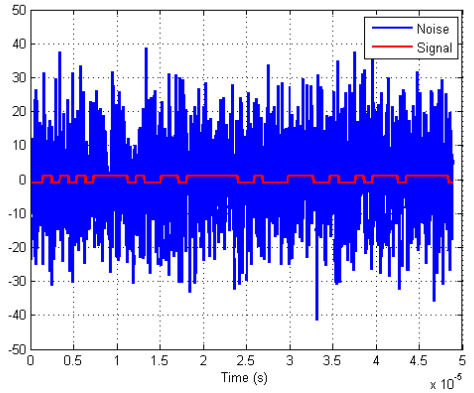
Galileo PRS-Empfänger
Funktionsweise PRS



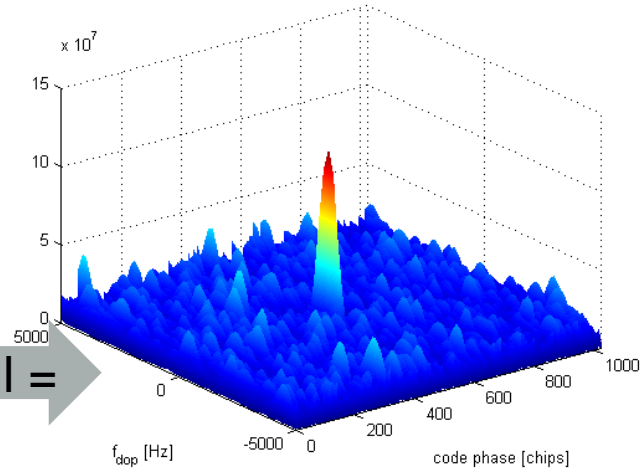
PRS-Signal

- “konventionelle” PRS-Empfänger:

Keying



- PRS-Schlüsselspeicherung und -Verwaltung
- PRS-Krypto-Algorithmen
- PRS-Sicherheitsfunktionalitäten
- PRS-Nachricht Entschlüsselung
- PRS-PRN-Generierung x empfangenes Signal =
- ➔ hohe Sicherheitseinstufung



Galileo PRS-Empfänger-Entwicklung

Deutsche Entwicklungen seit 2010

BaSE
(2010 – 2014)

PROOF
(2015 – 2017)

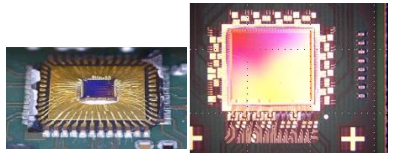
P3RS-2
(2014 – 2017)

COMPRISE
GPS P(Y) + PRS
(2017-2019)

PRISMA
(2016 – 2018)

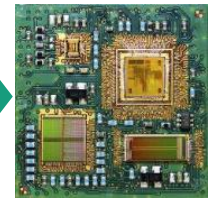
PASCAL/
GUARDIAN
(2018 – 2020)

Entwicklung
Security Module ASIC



Ziel:

PRS-Chipsatz
- PASCAL
- GUARDIAN
- SM-ASIC



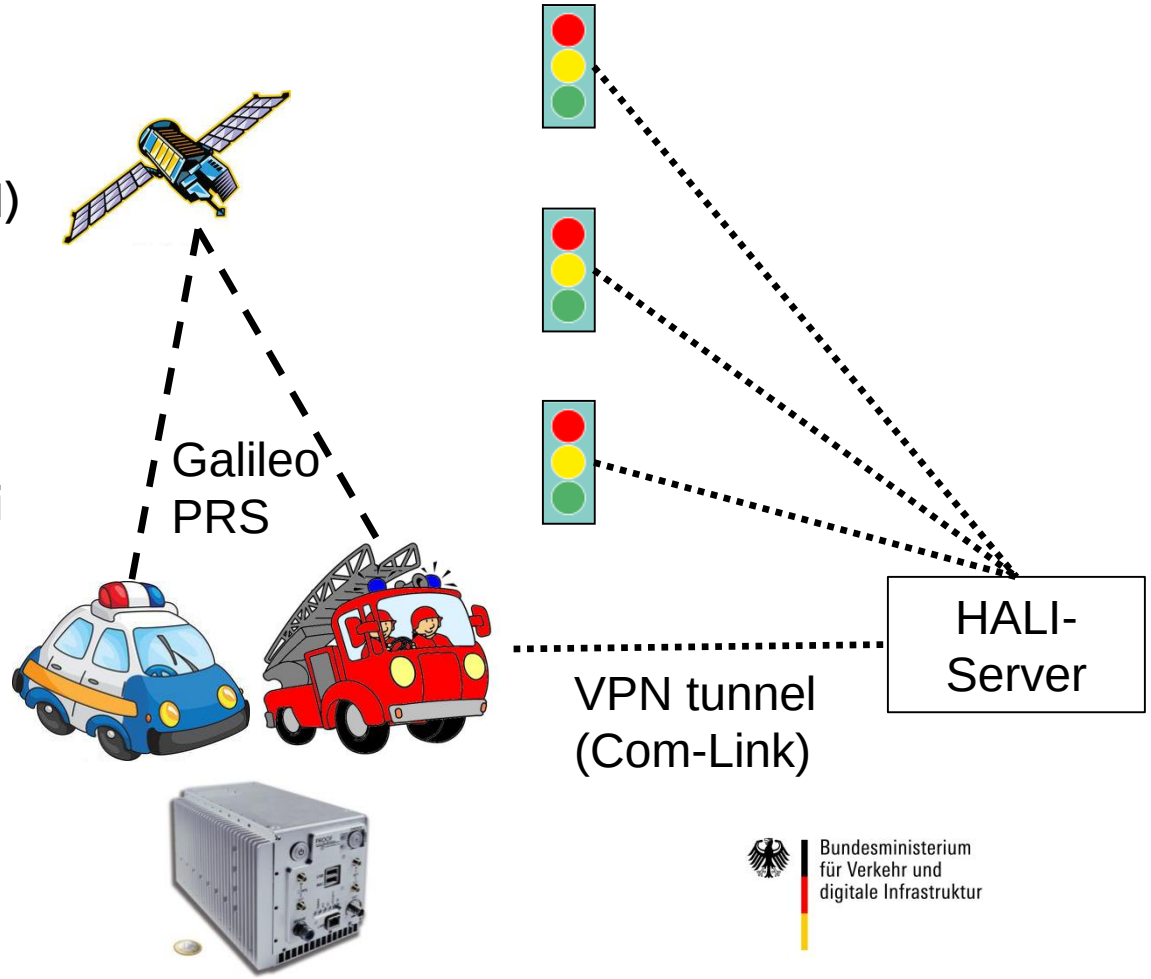
2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026

IABG SIEMENS AIRBUS Fraunhofer IIS

Demonstratorprojekt für hoheitliche PRS Einsatzgebiete

HALI-Berlin

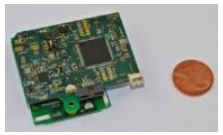
- Always Green for Emergency Vehicles with Galileo PRS
  - Gefördert über das nationale PRS-Programm (BMVI)
- Ziele
  - Nutzung von PRS zur LSA-Bevorrechtigung von Sondereinsatzfahrzeugen
  - Demonstration in 6 Fahrzeugen der Berliner Polizei und Feuerwehr
  - Optimierung der PRS-Signalverarbeitung im städtischen Umfeld mit Sensorfusion
  - Integration des PROOF-Empfängers mit Antenne und Sensoren in Einsatzfahrzeuge
- Verwendung von konventionellen PRS-Empfängern

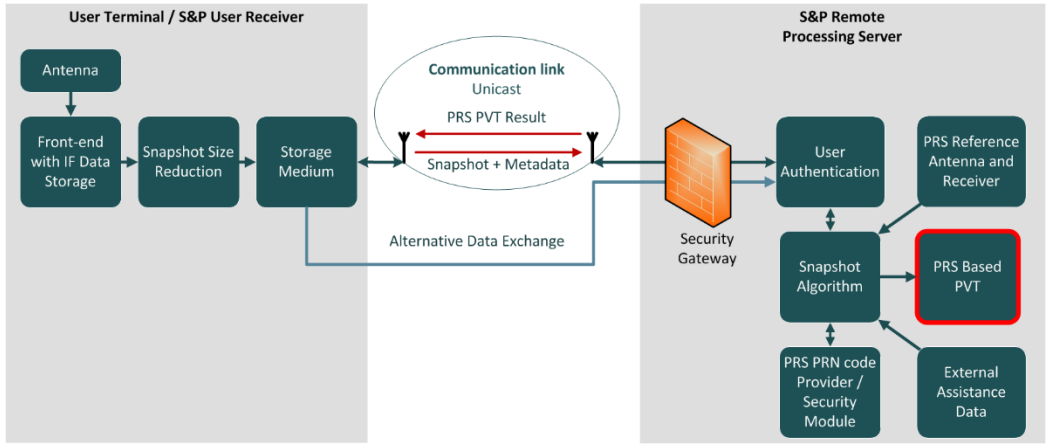


Bundesministerium für Verkehr und digitale Infrastruktur

“Serverbasierte” Galileo PRS-Empfänger
Motivation

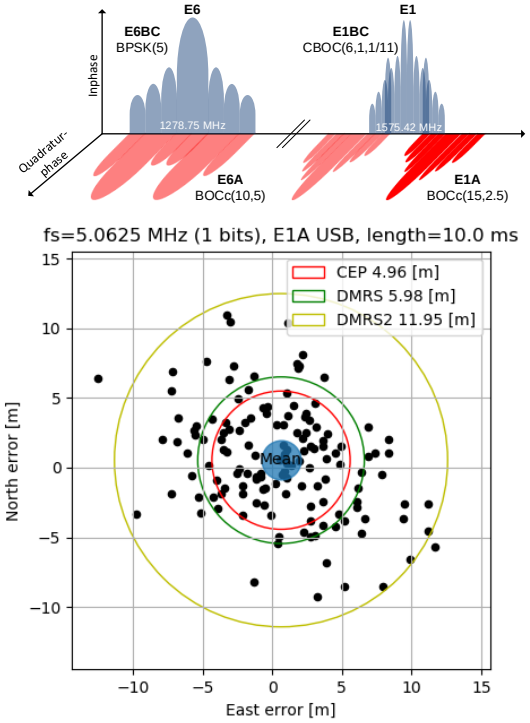
- Nachteile des PRS-Dienstes:
  - Im Vergleich zu Massenmarkt-Empfängern teure PRS-Empfänger / nie „Massenmarktprodukte“
  - Benutzung des PRS-Dienstes ungewohnt / aufwändiger (Schlüsselmanagement, logistische Verwaltung)
- Idee: Sicherheitsmodul nicht im Benutzer-Endgerät, sondern ausgelagert!
  - Damit kein Keying des Endgerätes / einfache Handhabung
  - Potentiell günstige, kleine, energiesparsame Endgeräte möglich
- Allerdings anderweitige Einschränkungen / Trade-offs



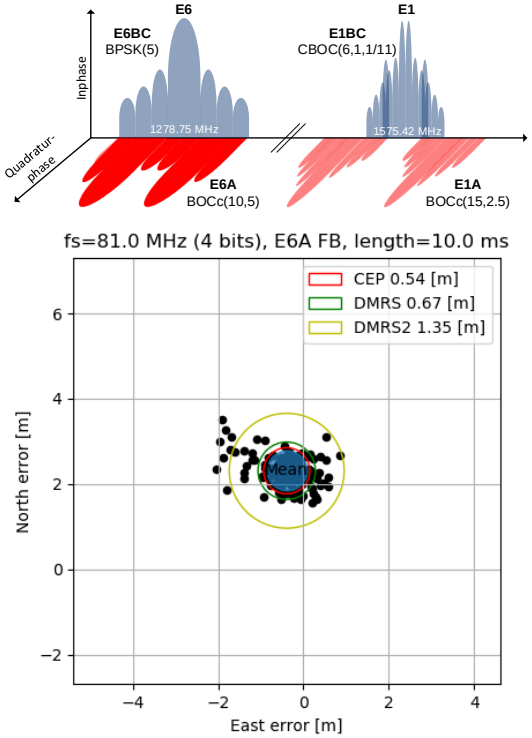


“Serverbasierte” Galileo PRS-Empfänger

Beispiel „Nürnberg“

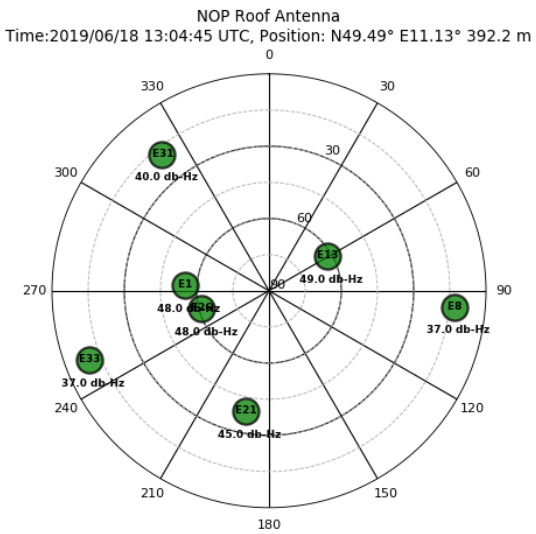


- Low snapshot size: E1A USB / BPSK(2.5)
  - 12.7 kByte / Snapshot for single PRS PVT



- High performance: E6A Full BOCc(10,5)
  - 810 kByte / Snapshot for single PRS PVT

- Nuremberg, Germany
- 2019-06-18 13:04:45 UTC
- 7 Galileo PRS SVs

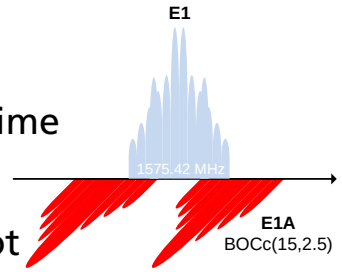


“Serverbasierte” Galileo PRS-Empfänger

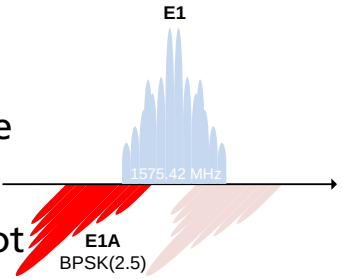
Beispiel „Vietnam“: Nachweisführung im Post-Processing

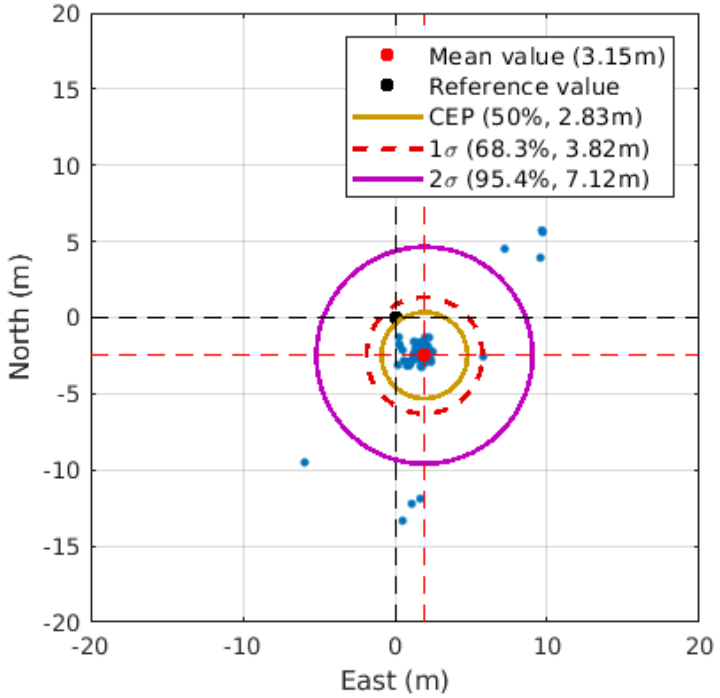
- Hanoi, Vietnam
- 2017-10-19 13:30:00 UTC
- 5 Galileo SV
- GDOP of around 3.5

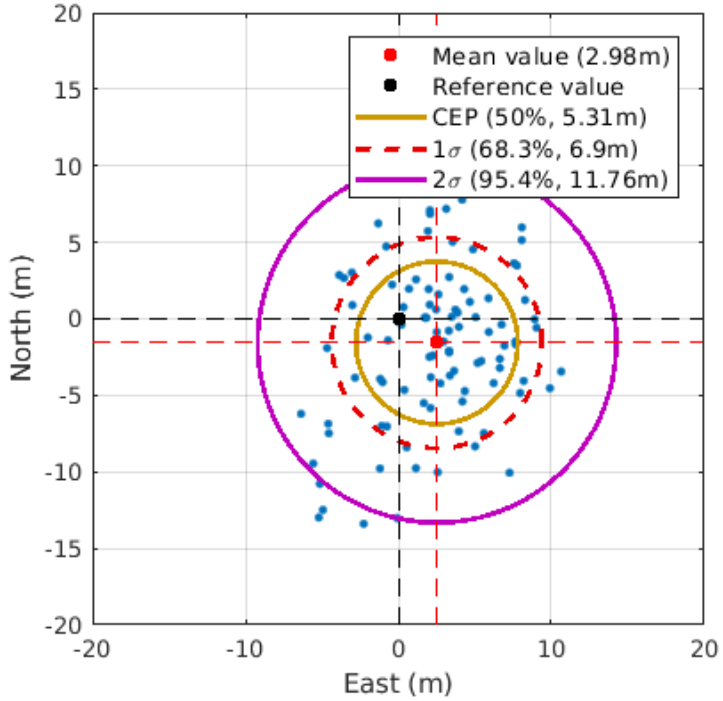
- E1A BOCc(15,2.5)
  - 10 ms integration time
  - 81 MHz @ 4 bit I/Q
    810 kByte / snapshot

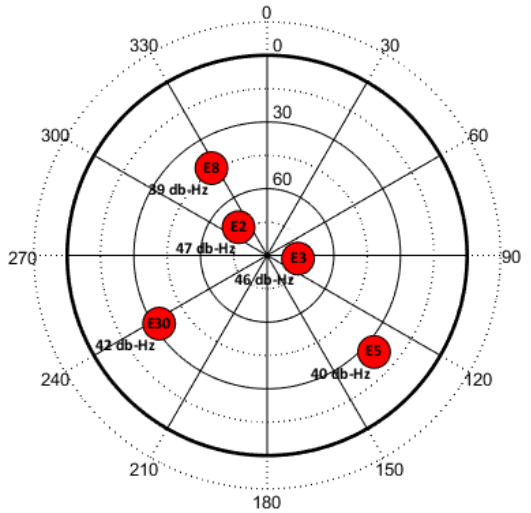


- E1A BPSK(2.5)
  - 10 ms integration time
  - 40.5 MHz @ 1 bit I/Q
    101.25 kByte / snapshot









"Serverbasierte" Galileo PRS-Empfänger

„Sample and Process" – Vor/Nachteile der Technologie

PROS

- Endgerät billig
  (relativ geringe Rechenleistung)
- PRS Algorithmen komplett in geschütztem Server
- Nachträgliche Beweisführung möglich
- „Passive" PRS Benutzung
  (hoher Schutz vor Missbrauch)

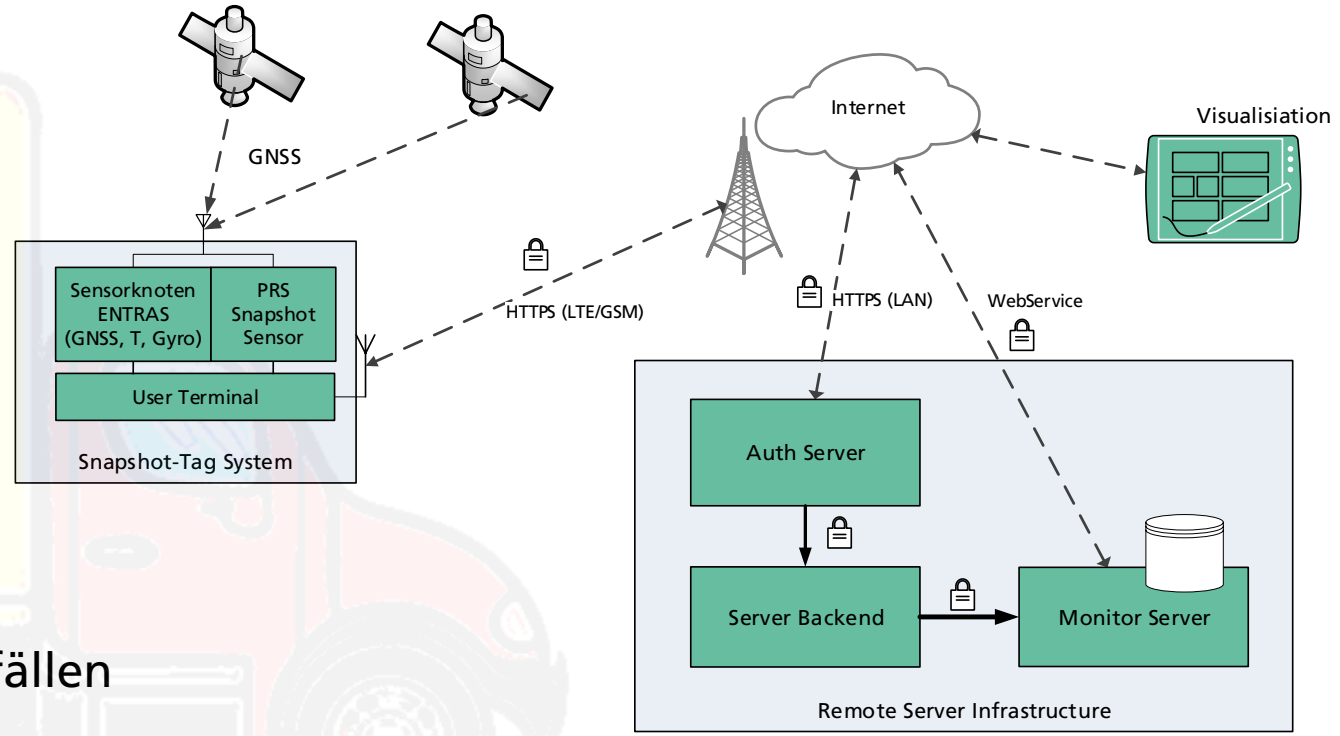
CONS

- Kommunikationskanal muss Rohdaten und ggf. PVT übertragen
- Latenz relativ hoch
- Skalierung / Aufwand
  bei vielen Geräten

- Anwendungen:
  - Authentifizierung von Messungen („PRSauth", Fraunhofer IIS)
  - Nachträgliche Beweisführung / Tracking von Gütern

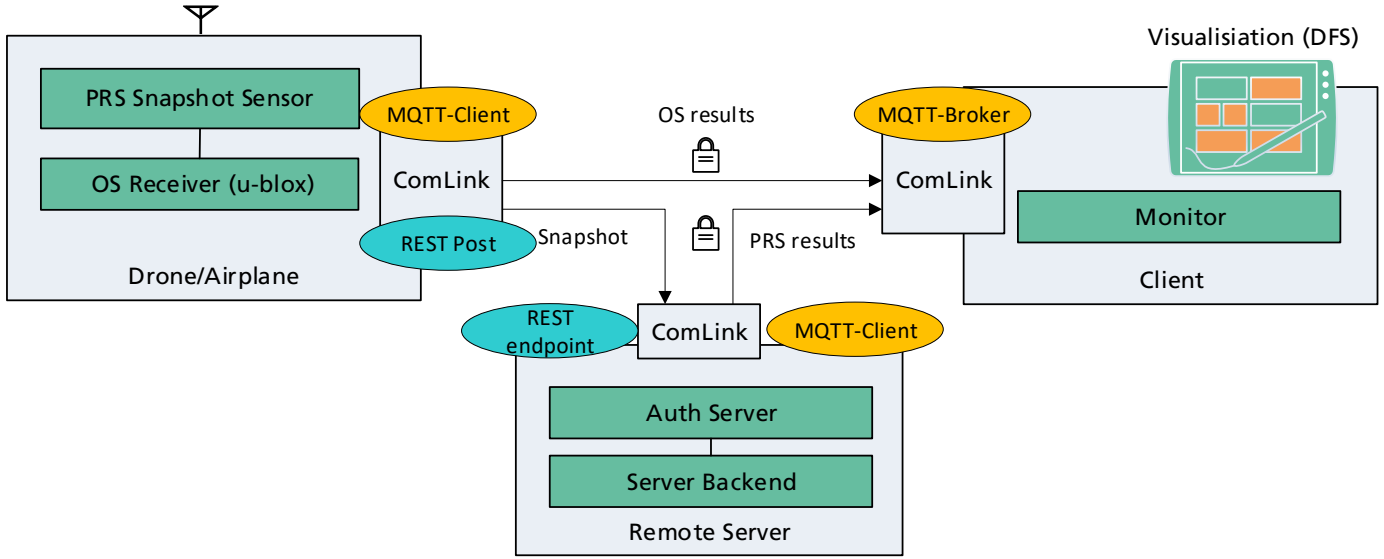
Demonstratorprojekt
Gefahrgutverfolgung

- Fraunhofer Initiative:
  “Cluster of Cognitive Internet Technologies”
- Überwachung des Gefahrguts während dem Transport (Position, Beschleunigung, Temperatur, Luftfeuchtigkeit, etc)
  - Automatische Alarmierung bei Zwischenfällen
  - Unterstützung elektronische Frachtpapiere
  - Nachweis der Lieferung
- Einbindung von GNSS-Rohdaten zur nachträglichen Auswertung
  - Nachweisführung Position und Zeit durch serverbasiertes Galileo PRS



Demonstratorprojekt
Registrierung von Drohnen im Luftraum

- „Beyond-line-of-sight“ Drohnen müssen im Luftraum registriert werden
  - anders als Verkehrsflugzeuge werden Drohnen nicht vom Radar erfasst, weshalb ihr Potenzial aktuell nur eingeschränkt nutzbar ist
- Verwendung von serverbasierter PRS-snapshot-Technologie
  - Absicherung des Ortes
  - Erkennung von Spoofing-Versuchen durch Vergleich OS- und PRS-Lösung
- Demonstrator mit WTD61/Bundeswehr und Droniq



Galileo PRS
Zusammenfassung

- Risiko der Verwendung von ungeschützten GPS L1 C/A oft nicht bekannt oder wird ignoriert, obwohl Zahl der Vorkommnisse steigt!
- Galileo PRS bietet Möglichkeiten und Sicherheit, wie bisher nur für militärische Anwendungen verfügbar
- Galileo PRS Empfängertechnologie wird aktuell in Deutschland entwickelt
  - Klassische PRS-Empfänger für höchste Genauigkeit und Verfügbarkeit
  - Server-basierte Ansätze für neuartige Applikationen
- Galileo ist verfügbar!
  - 26 von 30 geplanten Satelliten im Orbit!
  - Einsatz (zusammen mit GPS, GLONASS,…) in mehr als 1 Mrd. Geräten
  - Endausbau bis 2021
- Große Change für Europa und Deutschland!

© Fotolia / Fraunhofer IIS

Fragen?

Alexander Rügamer

Group Manager Specialized GNSS Receivers
Satellite Based Positioning Department
Fraunhofer Institute for Integrated Circuits IIS
Nordostpark 93, 90411 Nuremberg, Germany
Phone + 49 911 58061-6379 | Fax +49 911 58061-6398

alexander.ruegamer@iis.fraunhofer.de

Galileo PRS
Eigenschaften und Nutzergruppen

- Europäisches System, daher keine externen Abhängigkeiten zu Design, Betrieb, Weiterentwicklung
- Hohe Verfügbarkeit, wenn offene GNSS-Dienste ggf. nicht nutzbar sind
  - Robuster gegen Jamming als offene GNSS-Signale
  - Spoofing wegen Verschlüsselung nicht möglich
- Zugang zum PRS ist nur staatlich autorisierten Organisationen und Nutzern möglich
  - Competent PRS Authoritiy (CPA) entscheidet über Nutzer und Nutzung
  - „Drittstaaten“ (Schweiz, USA, UK(?),…) können über Abkommen mit EU ebenfalls PRS-Nutzer mit eigener CPA werden, allerdings nicht PRS-Empfänger-Hersteller
- Beispiele für potentielle PRS-Nutzer sind:
  - Behörden und Organisationen mit Sicherheitsaufgaben (BOS)
  - Betreiber kritischer Infrastruktur (KRITIS), z.B. Energieversorger, Kommunik.-dienste, Banken, etc.
  - Bundeswehr