Sichere, souveräne Satellitennavigationsempfänger „made in Germany“ mit Galileo PRS

OMNISECURE
Berlin, 21. Juni 2022

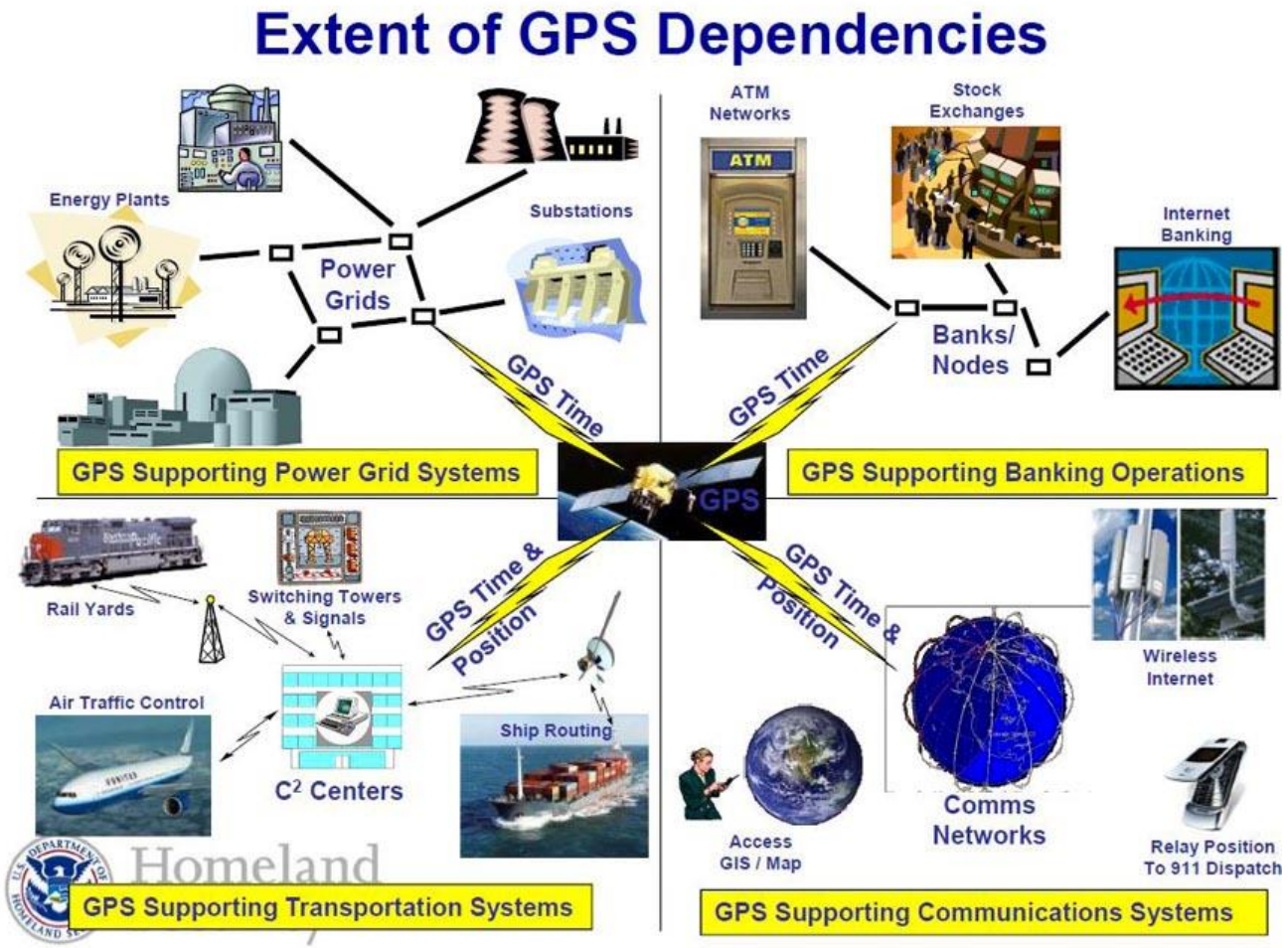
Alexander Rügamer

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

Fraunhofer IIS

Motivation

Vielfältige Anwendungen…. auch in sicherheitsrelevanten Bereichen



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

Fraunhofer IIS

Motivation
Aktuelle Gefährdung 1/2

Finland reports GPS disturbances in aircraft flying over Russia's Kaliningrad

The interference began soon after a meeting between presidents Sauli Niinistö and Joe Biden

Some of Finnair's Asian flights and most of its European ones go past Kaliningrad. Photograph: Lehtikuva Lehtikuva/Reuters

Aircraft flying near the Russian enclave of Kaliningrad and near Finland's eastern border with Russia have noticed interference with their GPS signals, according to Finnish authorities.

The interference began soon after Finland's President Sauli Niinistö met Joe Biden in Washington on Saturday to discuss deepening defense ties between Finland and Nato due to Russia's attack on Ukraine.

https://www.theguardian.com/world/2022/mar/09/finland-gps-disturbances-aircrafts-russia

GPS WORLD GNSS POSITIONING NAVIGATION TIMING

Follow Us

Search the Site...

GNSS | OEM | Autonomous | Survey | Mapping | Transportation | Defense | Mobile

European agency warns of GNSS outages near Ukraine

March 22, 2022 - By Matteo Luccio

Photo: franckreporter/E+/Getty Images

In the current context of the Russian invasion of Ukraine, the issue of GNSS jamming and/or possible spoofing has intensified in geographical areas surrounding the conflict zone and other areas, according to the European Union Aviation Safety Agency (EASA). The agency issued a safety information bulletin on March 17 warning of a GNSS outage leading to navigation / surveillance degradation. According to the

https://www.gpsworld.com/european-agency-warns-of-gnss-outages-near-ukraine/

Science

Mysteriöser Jammer vor Start von bemannter Raummission gefunden

02.06.2022

Der Störsender war in einem Fahrzeug versteckt und hätte das Potenzial gehabt, den Kurs der Rakete zu beeinflussen.

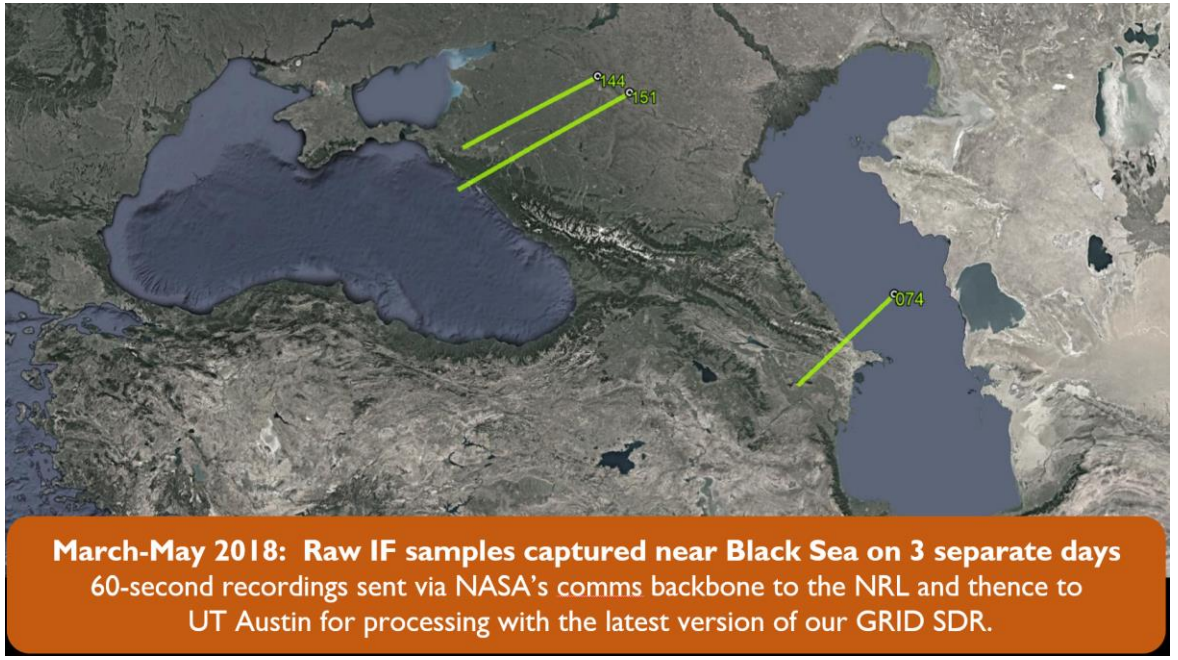
China wird demnächst 3 Raumfahrer*innen zur neuen **Tiangong-Raumstation** befördern. Doch einige Wochen vor dem geplanten Start kam es zu einem ungewöhnlichen Zwischenfall.

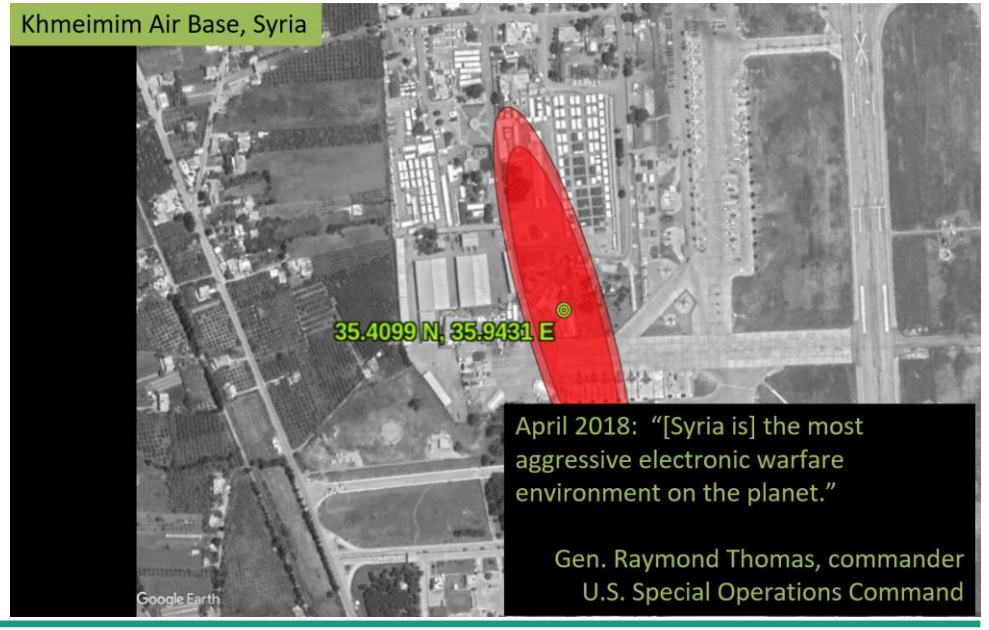
Es wurde ein **mysteriöser Funkstörsender** bei dem Weltraumbahnhof entdeckt. Der Jammer war in einem Fahrzeug versteckt, das sich ganz in der Nähe des **Jiuquan Satellite Launch Center** in der Provinz Gansu befunden hatte.

Ob es sich dabei um einen möglichen **Sabotage-Akt** handelt, wollte von offizieller Seite niemand bestätigen, heißt es ***in mehreren Medienberichten***. Mit dem Störsender wäre es allerdings möglich gewesen, die **Navigationssysteme** zu stören und so den **Kurs der Rakete** zu beeinflussen.

https://futurezone.at/science/stoersender-jammer-raketenstart-china-navigation-kurs-flugroute-sabotage/402028928

Motivation
Aktuelle Gefährdung 2/2



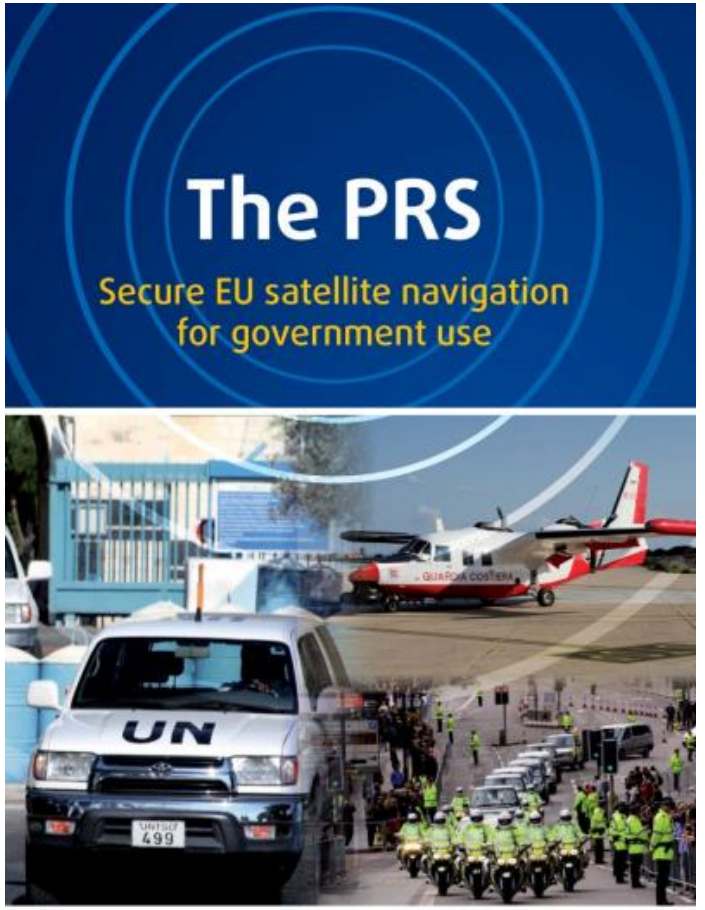


Murrian, MJ, Narula, L, Iannucci, PA, et al. First results from three years of GNSS interference monitoring from low Earth orbit. *NAVIGATION.* 2021; 68: 673– 685. https://doi.org/10.1002/navi.449

Fraunhofer IIS

Galileo PRS
Galileo PRS = Sicherheit

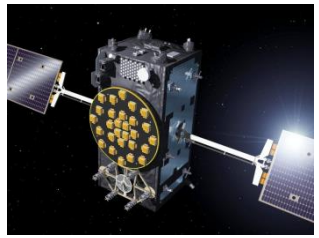
- Galileo ist das EU-“Global Navigation Satellite System“ (GNSS)
  - Akt. 28 Satelliten im All; 24 verfügbar → nahe am Endausbau
- Galileo bietet drei globale SatNav-Dienste:
  - Open Service (OS)
  - Commercial Service (CS)
  - Public Regulated Services (PRS)
- PRS ist verschlüsselter und besonders geschützter SatNav-Dienst
- 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



Galileo PRS
Eigenschaften und Nutzergruppen

- Hohe Verfügbarkeit
  - Insb. wenn offene GNSS-Dienste nicht nutzbar sind
  - Robuster gegen Jamming als offene GNSS-Signale
  - Spoofing durch eingesetzte Verschlüsselung nicht möglich
- Zugang zum PRS nur für autorisierten Organisationen und Nutzer (Beschluss 1104/2011/EU)
  - Competent PRS Authority (CPA) entscheidet
  - „Drittstaaten“ (Schweiz, USA, UK,…) können über Abkommen mit EU ebenfalls Zugriff erhalten
- Beispiele für potentielle PRS-Nutzer sind:
  - Behörden und Organisationen mit Sicherheitsaufgaben (BOS)
  - Betreiber kritischer Infrastruktur (KRITIS), z.B. Energieversorger, Kommunik.-dienste, Banken, etc.
  - Bundeswehr

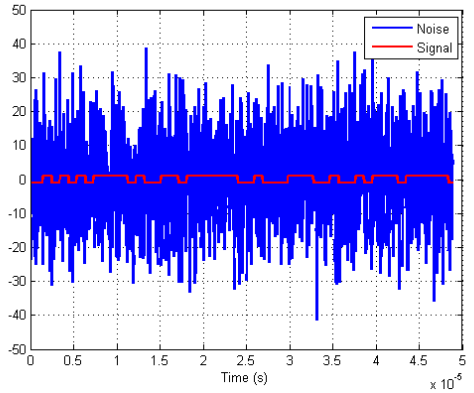
Galileo PRS
Funktionsweise PRS-Empfänger



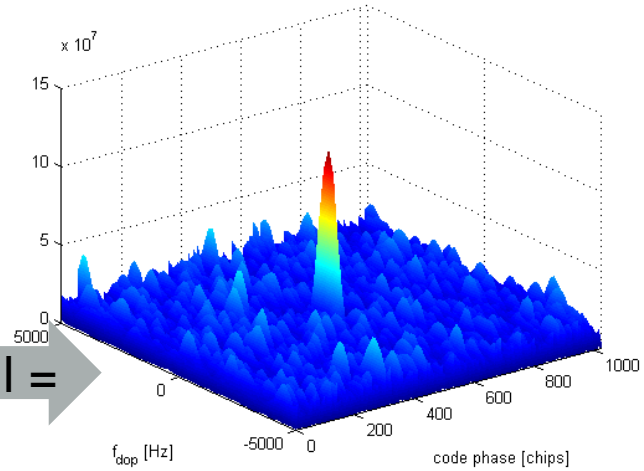
PRS-Signal

- “konventionelle” PRS-Empfänger:

Keying



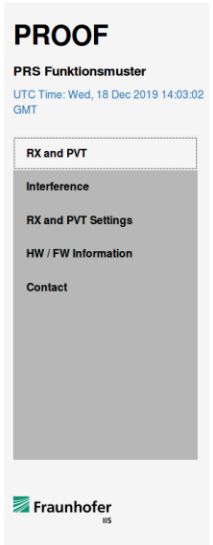
- PRS-Schlüsselspeicherung und -Verwaltung
- PRS-Krypto-Algorithmen
- PRS-Sicherheitsfunktionalitäten
- PRS-Nachricht Entschlüsselung
- PRS-PRN-Generierung x empfangenes Signal =
- ➔ Controlled Item

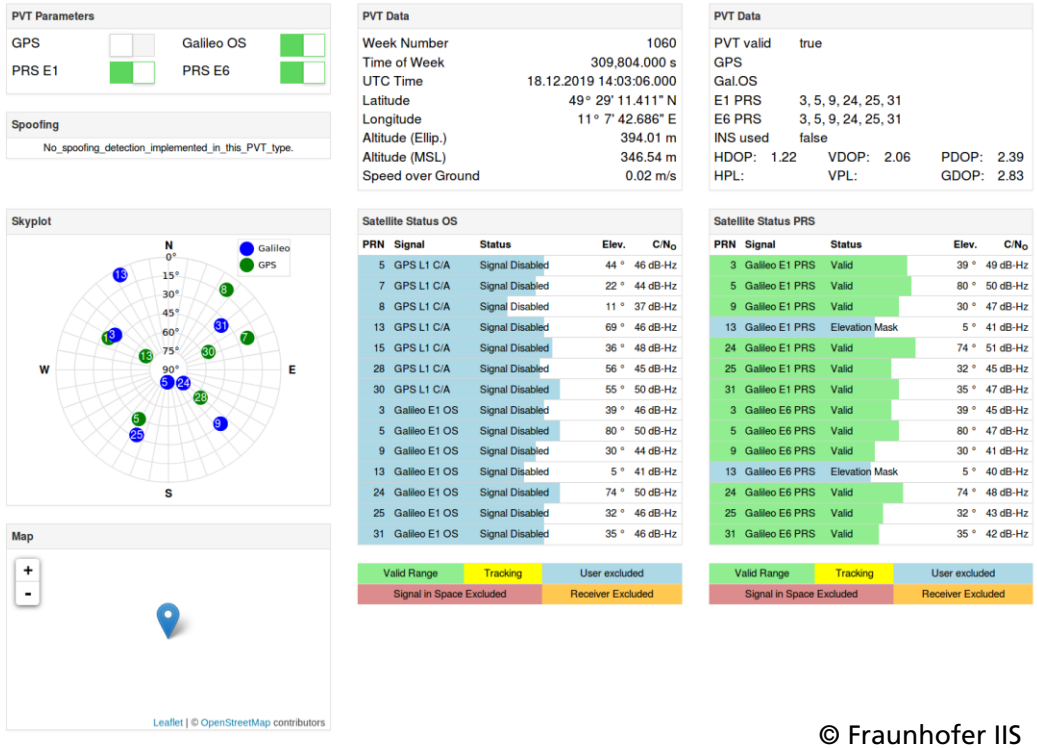


Galileo PRS
Deutscher Galileo PRS-Testempfänger: PROOF

© Fraunhofer IIS

- Bundeswehr / WTD81: PROOF [2015-2017]
  - PRS-Empfänger mit erhörter Störfestigkeit
    - GPS L1 C/A (12 Kanäle)
    - Galileo OS (12 Kanäle)
    - Galileo PRS (je 12 Kanäle E1 und E6)
  - Schnelle Hardware-Akquisition
  - Sensorfusion mit externer IMU
  - Differential GNSS / -PRS Unterstützung
  - Ausgabe: RINEX, Web-Interface
- Sukzessive Erweiterungen aus nat. PRS-Projekten DIRACU, GUARDIAN, HALI, PayOFF,…

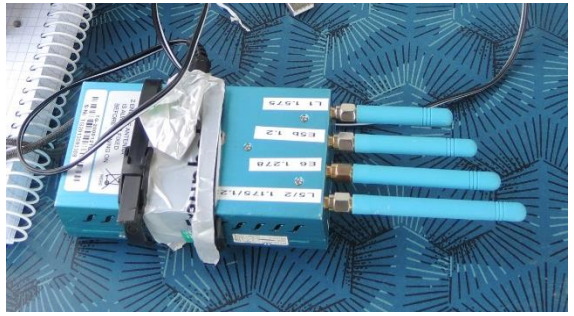




© Fraunhofer IIS

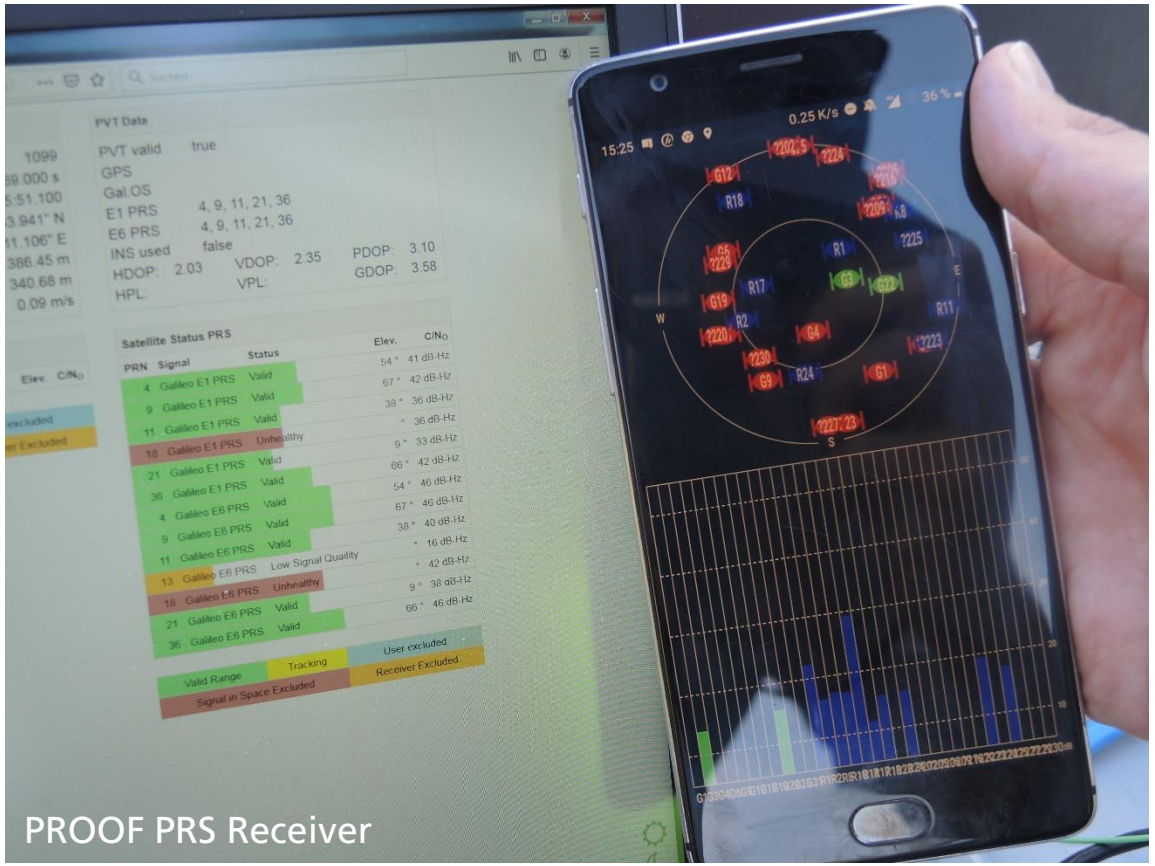
Testkampagne – Jamming

Jamming-Angriff mit einer Drohne (unter kontrollierten Bedingungen, mit Erlaubnis der BNetzA)



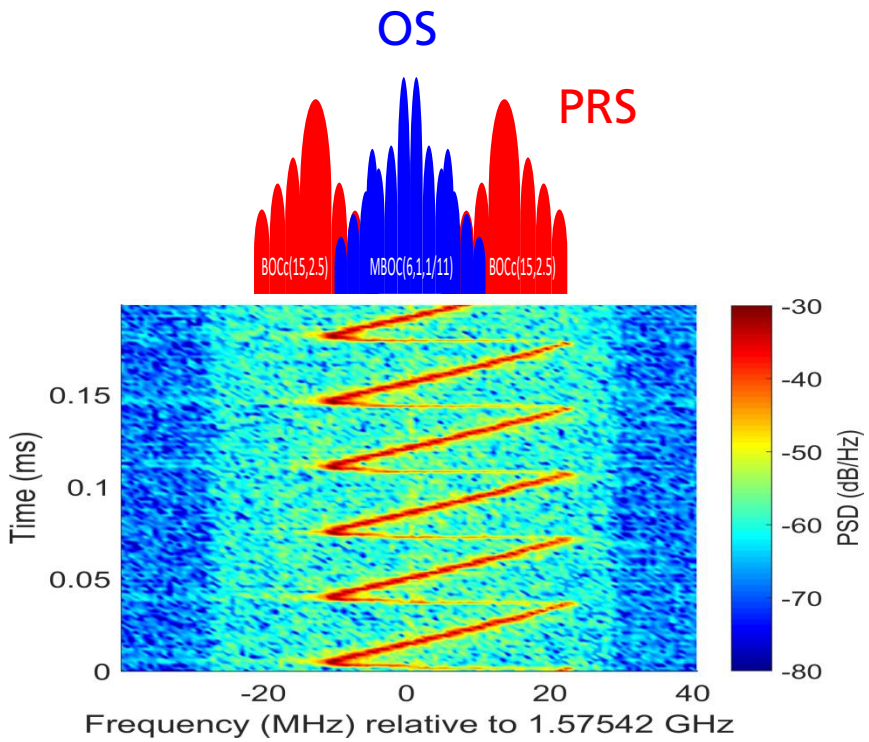
Testkampagne – Jamming

Jamming-Angriff mit einer Drohne (unter kontrollierten Bedingungen, mit Erlaubnis der BNetzA)

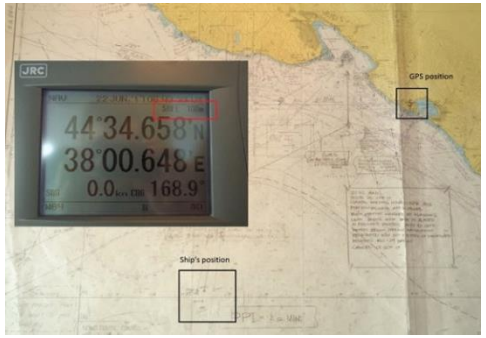


PROOF PRS Receiver

- PRS funktioniert weiterhin, obwohl GPS / Galileo OS auch auf PROOF nicht mehr verfügbar sind
- Bandbreite PRS erhöht Robustheit!



Täuscher (Spoofer) – Spoofing
Vorfälle



- Spoofing: Übertragung eines gefälschten GNSS-Signals
  - Vortäuschen einer GNSS-Empfänger Positions- bzw. Zeitlösung
  - Potentiell größere Gefahr als Jamming!
- „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“

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.

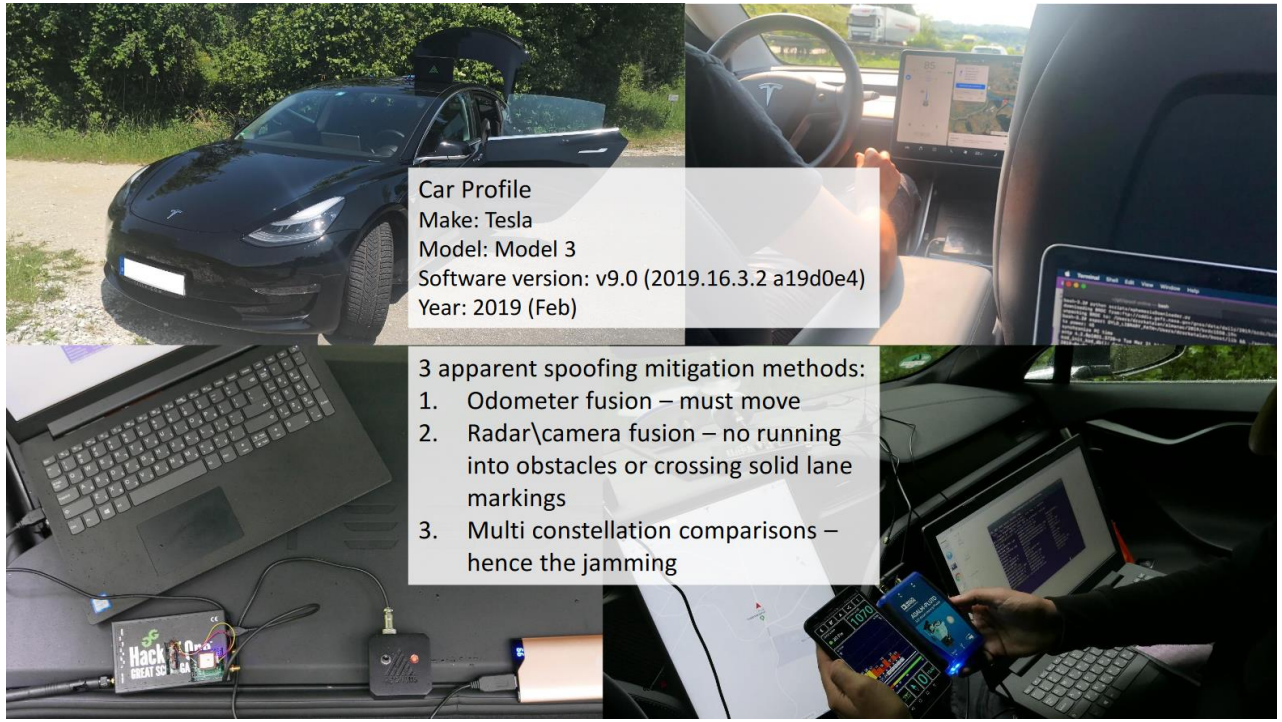
https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea

Täuscher (Spoofer) – Spoofing
Autopilot

Bogus Satellite Nav Signals Send Autonomous Cars Off the Road

At the Black Hat security conference, a researcher demonstrated how making tweaks to navigation signals could send a self-driving car careening off the road.

By Max Eddy August 8, 2019 2:12PM EST

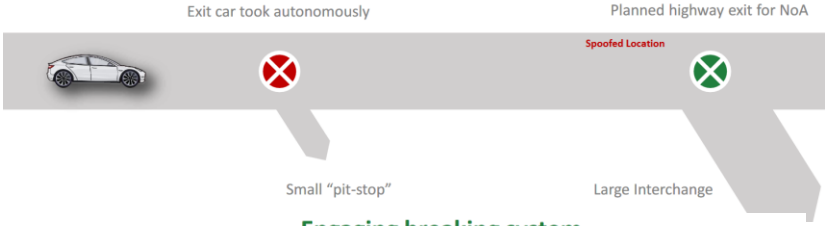


REGULUS

Diverting the vehicle off the highway

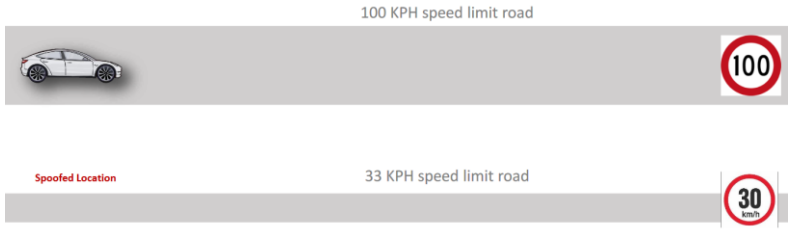
- Car autonomously driving on NoA, planned to exit at a main interchange ahead
- Attacker spoofed car location, changing it to the interchange, while car is actually still 3 miles away
- Car identifies a small pit stop as the designated exit, drifts right into the pit stop at high-speed

*No driver approval required at any point



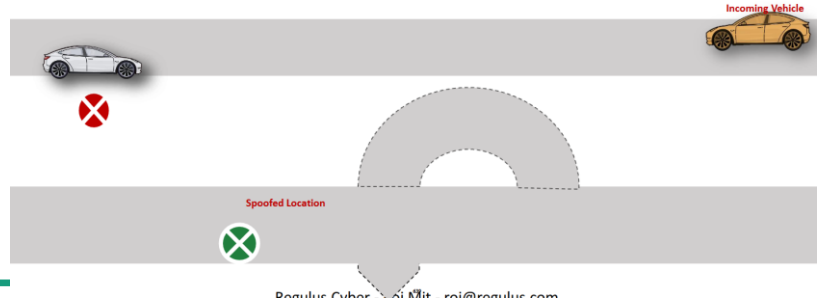
Engaging breaking system

- Car autonomously driving on Autopilot on highway with a 100 KPH speed limit (62 MPH)
- Attacker spoofs car to a nearby town road with 33 KPH speed limit (20 MPH)
- System engages the breaks and eforces a new speed limit for the autopilot system



Changing to opposite lane into incoming traffic

- Car physically driving in a small town road with two opposite lanes and a dotted seperation line
- Attacker spoofed vehicle location, changing it to a highway with an interchange that requires a left exit
- Vehicle activates left blinker and autonomously changes to the left lane into incoming traffic

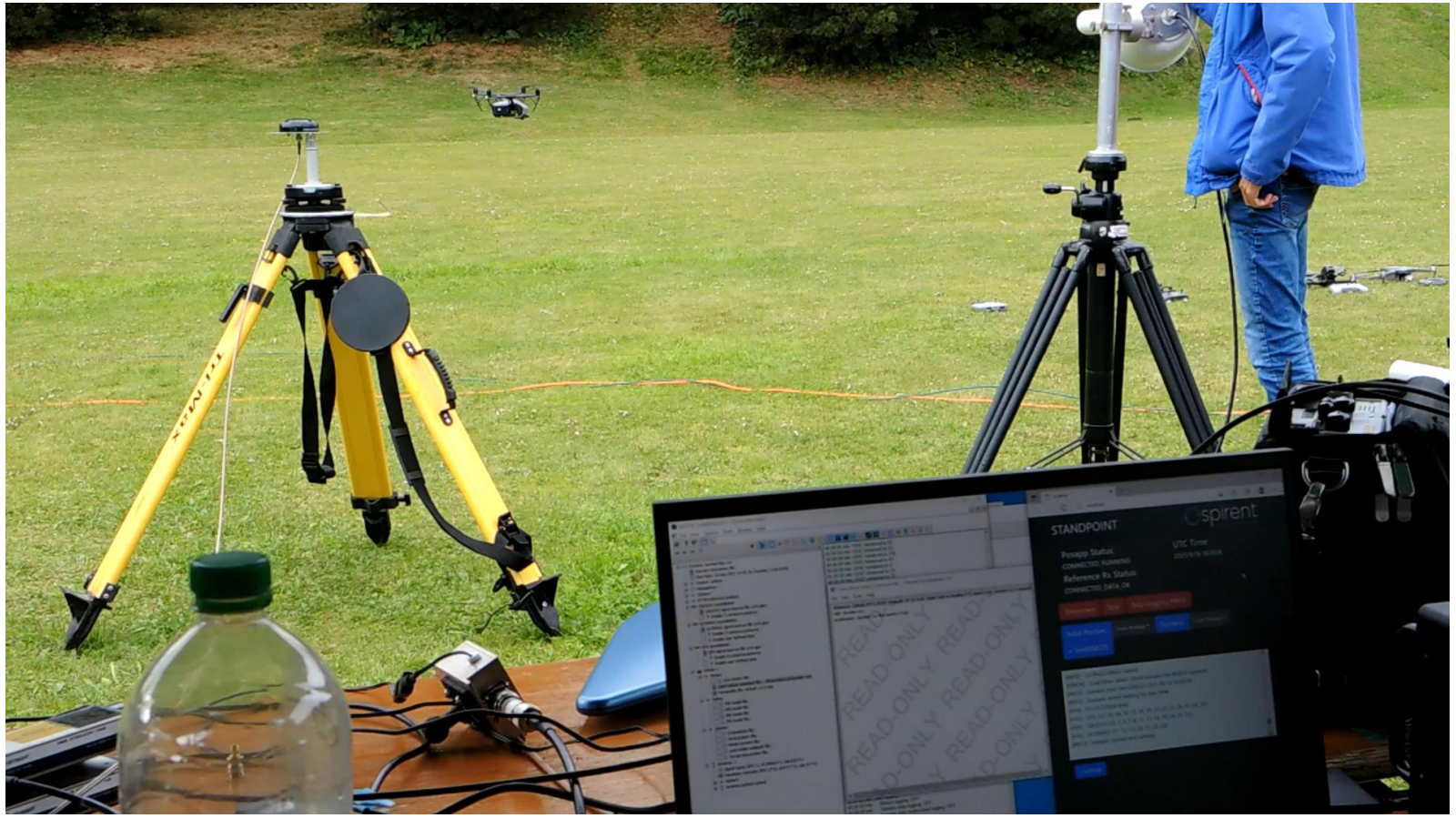


Mit et al., „Analyzing Tesla's Level 2 Autonomous Driving System Under Different GNSS Spoofing Scenarios and Implementing Connected Services for Authentication and Reliability of GNSS Data", ION GNSS+ 2020

Fraunhofer IIS

Testkampagne – Spoofing

Drohnen (Truppenübungsplatz mit Genehmigung, Sep 2021)



- Scenario: Hovering, 1 m Höhe
  - 10 s static positioning spoofing (E1, L1, G1);
  - Beschleunigung 5 s Endgeschwindigkeit 0.5 m/s

Testkampagne – Spoofing

Spoofing-Angriff (unter kontrollierten Bedingungen, mit Erlaubnis der BNetzA)

Entfernung 50m

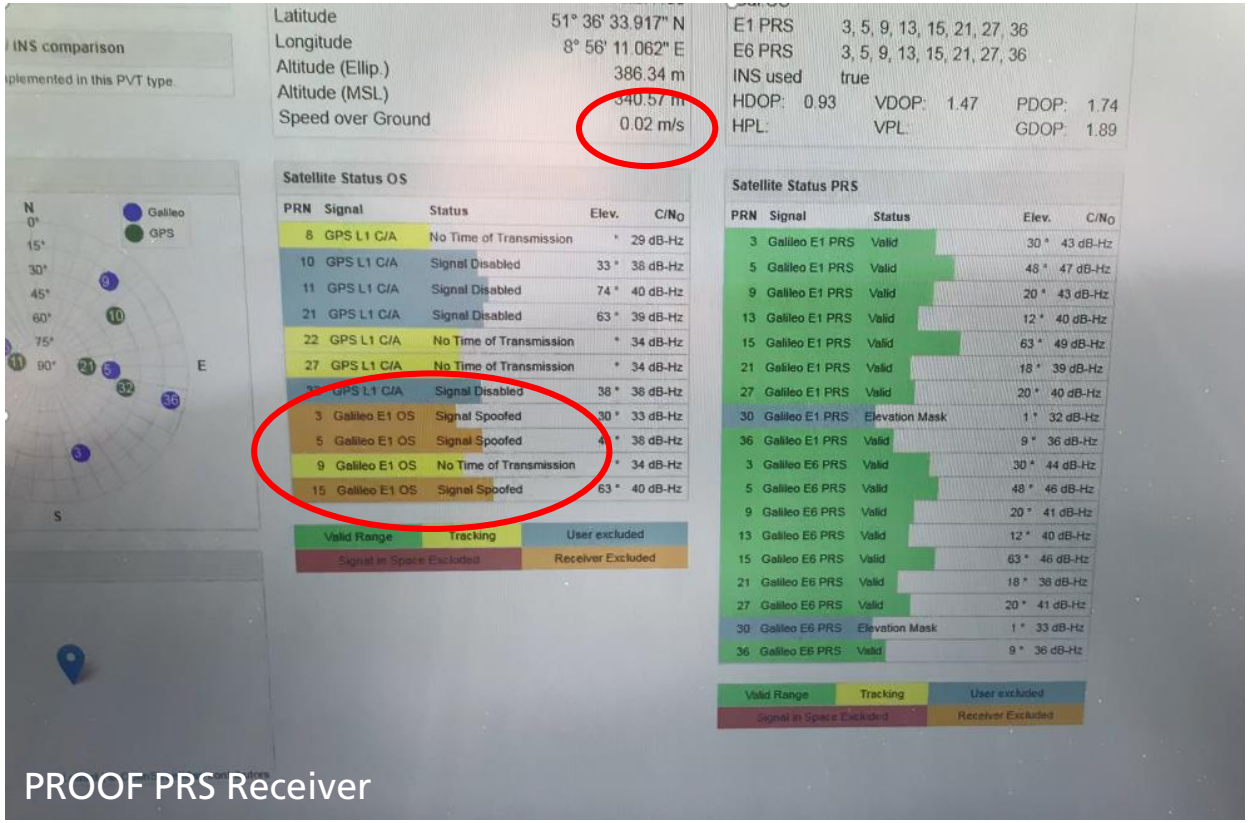
Smartphone + Navi vs. PRS-Empfänger

Testkampagne – Spoofing

Spoofing-Angriff (unter kontrollierten Bedingungen, mit Erlaubnis der BNetzA)

Geschwindigkeit: 13 km/h

Geschwindigkeit: 0 km/h



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)

ETB PRS-AM
(2020 – 2023)

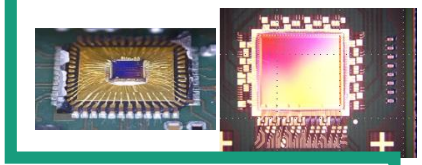
Objective:

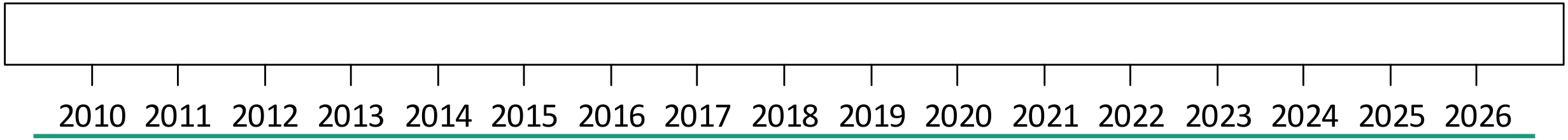
Product
PRS-AM

Objective:

PRS Chipset
PASCAL
GUARDIAN
SM-ASIC

Development of PRS
Security Module ASIC

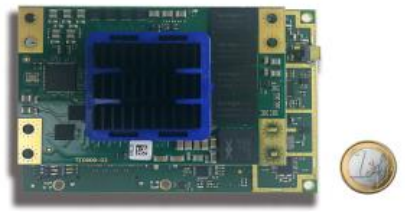




Fraunhofer IIS

Aktuelle Evaluierung Galileo PRS-Technologie in Deutschland
Bundeswehr

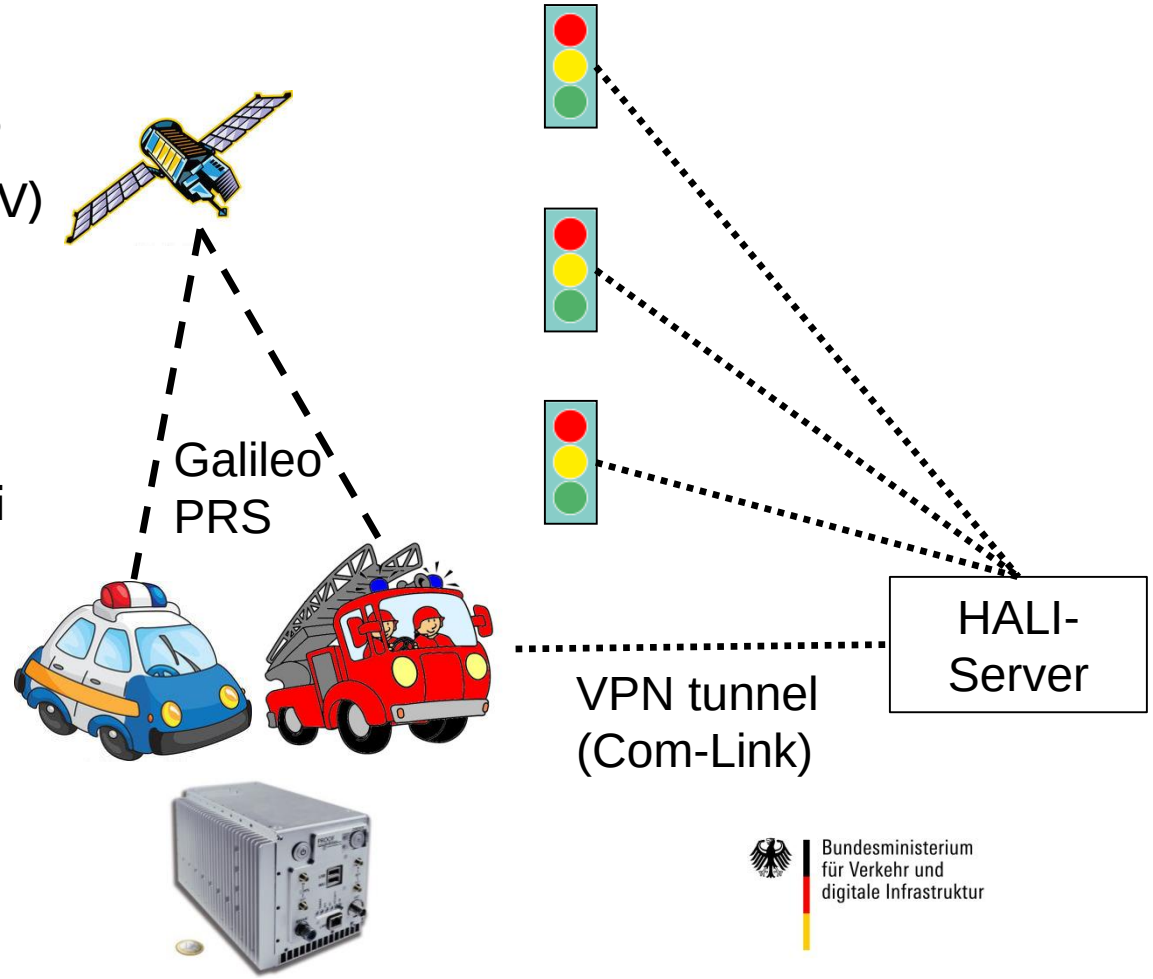
- Souveränität und dual-System-Lösung
  - Integration von Galileo PRS in allen Navigationsanwendungen
  - Start mit land- und seebasierten Vehikeln
  - Kombination mit militärischer GPS-Karte
  - ➔ „doppelte“ Sicherheit:
    - Militärisches GPS mit P(Y) / M-Code
    - Galileo PRS



Aktuelle Evaluierung Galileo PRS-Technologie in Deutschland

HALI-Berlin (1/3)

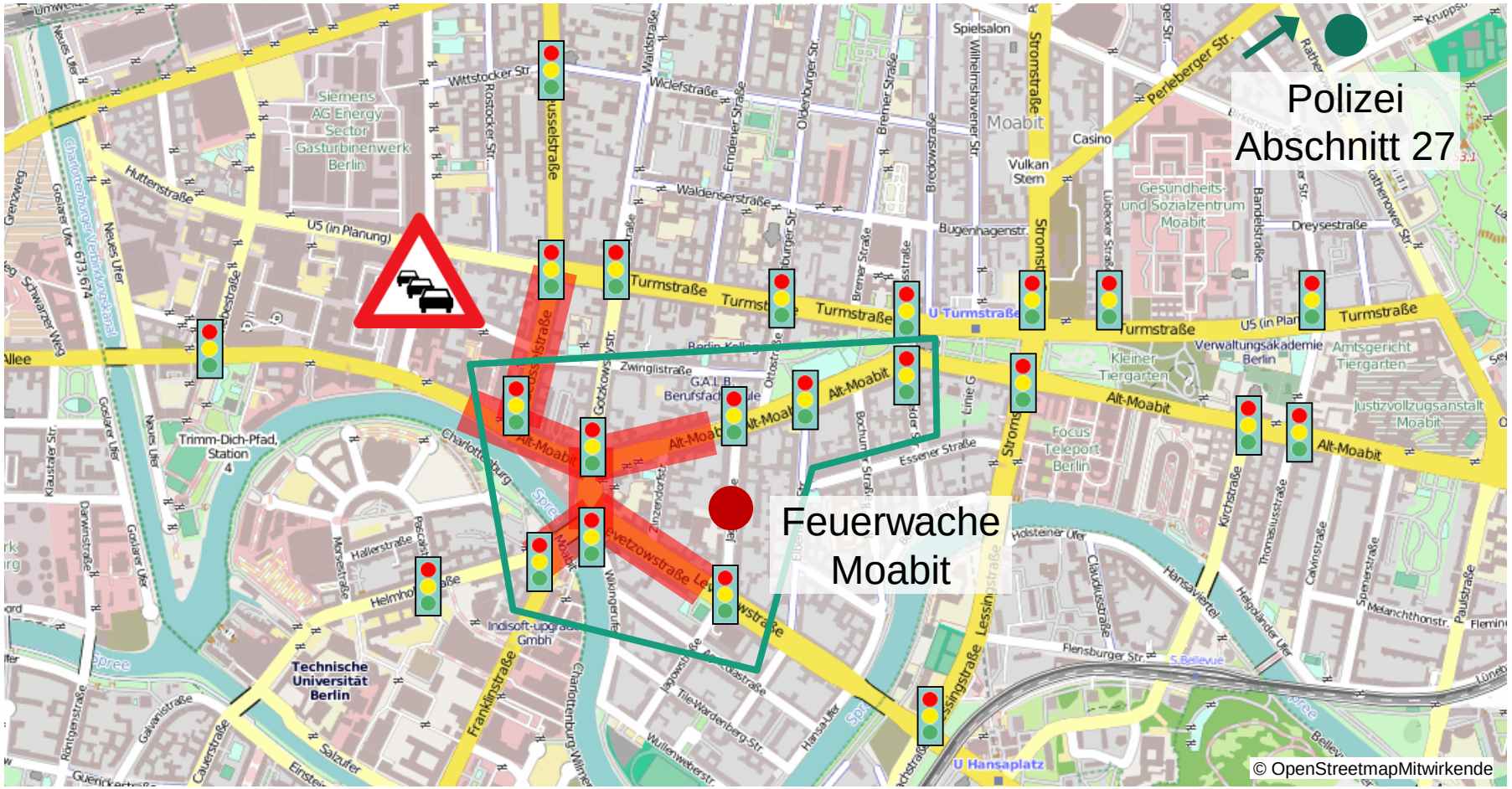
- Always Green for Emergency Vehicles with Galileo PRS
  - Gefördert über das nationale PRS-Programm (BMDV)
- Ziele
  - Nutzung von PRS zur LSA-Bevorrechtigung von Sondereinsatzfahrzeugen
  - Demonstration in 6 Fahrzeugen der Berliner Polizei und Feuerwehr
  - Optimierung der PRS-Signalverarbeitung im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



Bundesministerium für Verkehr und digitale Infrastruktur

Aktuelle Evaluierung Galileo PRS-Technologie in Deutschland

HALI-Berlin (2/3)



Traffic lights

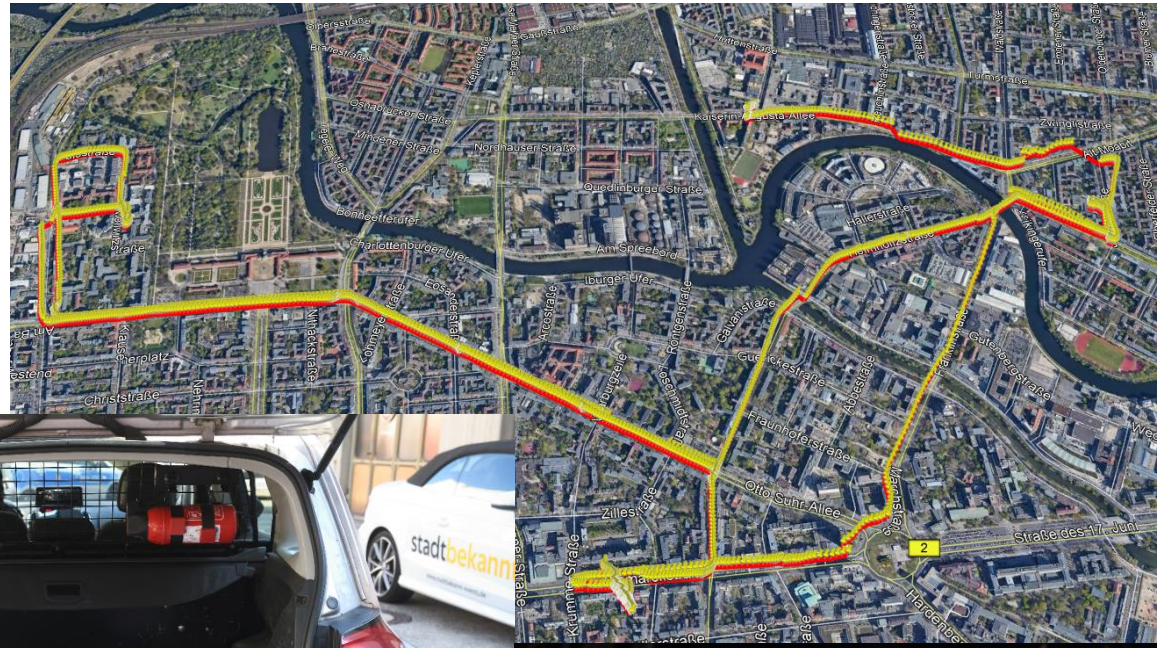
Areas subject to traffic jams

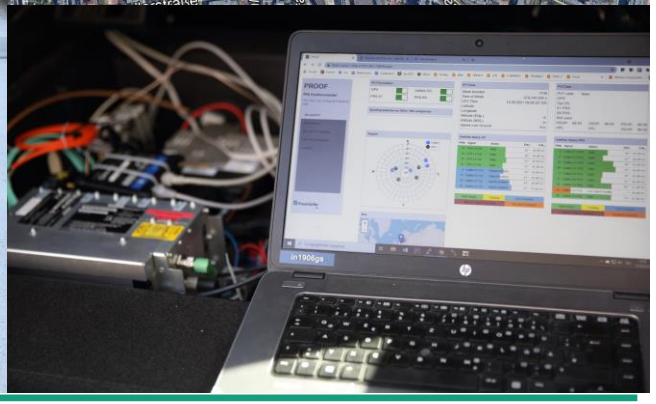
Test field

Aktuelle Evaluierung Galileo PRS-Technologie in Deutschland

HALI-Berlin (3/3)

- Live Demonstration “echtes PRS”
  11.8.2021, Berlin
  - Weltweit erstmalige PRS-Demonstration mit hoheitlichen Anwendern
  - Sensor Fusion
    PRS + INS + Odometer
  - 3x Polizei, 3x Feuerwehr
  - Langzeitevaluierung
    ab Q3/2022 geplant

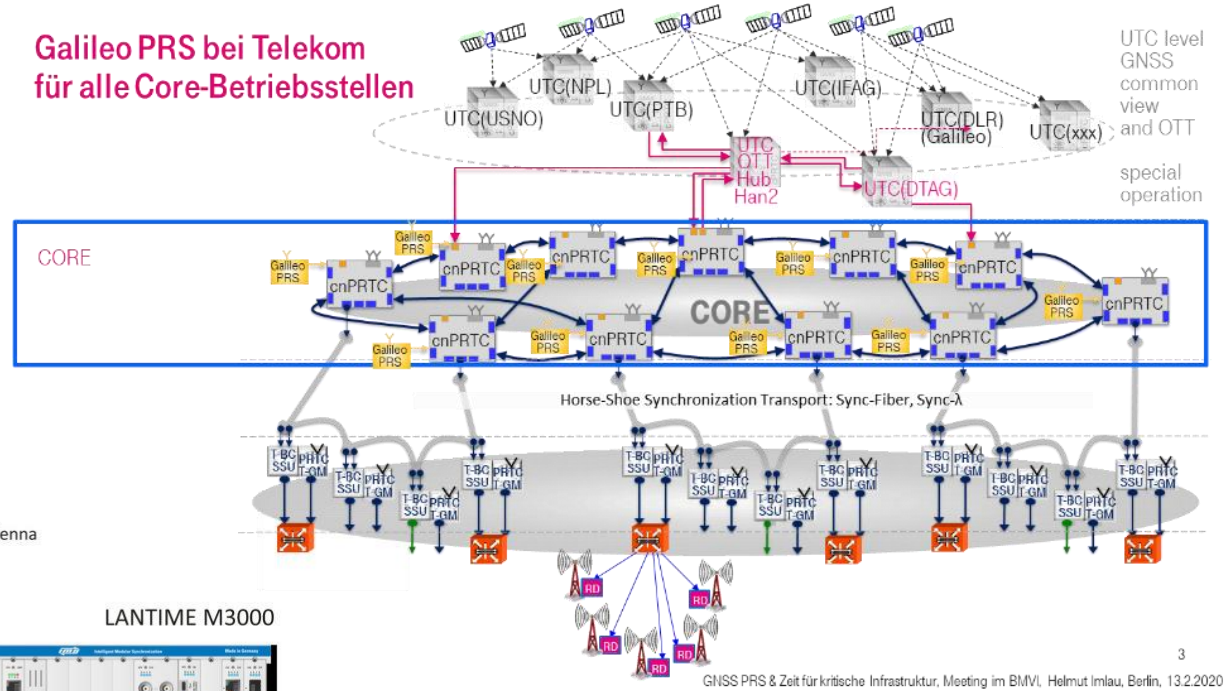


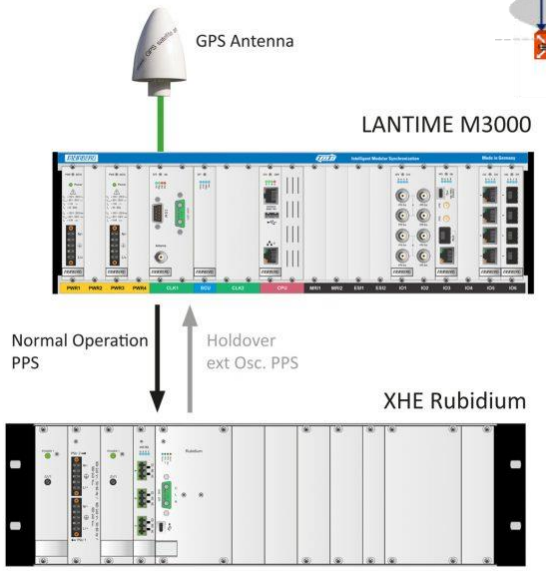


Aktuelle Evaluierung Galileo PRS-Technologie in Deutschland

SIZE – Sicherer Zeitempfänger

- Sicherer Zeitempfänger
  - Gefördert über das nationale PRS-Programm (BMDV)
- Kooperation mit Deutscher Telekom und Meinberg
  - Anbindung PRS-Empfängertechnologie an Meinberg Zeitempfänger
  - Evaluierung für potentiellen Einsatz im Zeit-Backbone der Deutschen Telekom
  - Optimierung der PRS-Technologie für Zeitgenauigkeiten <30 ns





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
- Neben Technologieentwicklung auch erste Anwendungsprojekte:
  - HALI-Berlin: Integration PRS in Feuerwehr- und Polizeifahrzeuge
  - Sichere Zeitempfänger, Drohnennavigation, Gefahrgutüberwachung
- Große Chance für Europa und Deutschland!

© Fotolia / Fraunhofer IIS

Fragen?

Alexander Rügamer

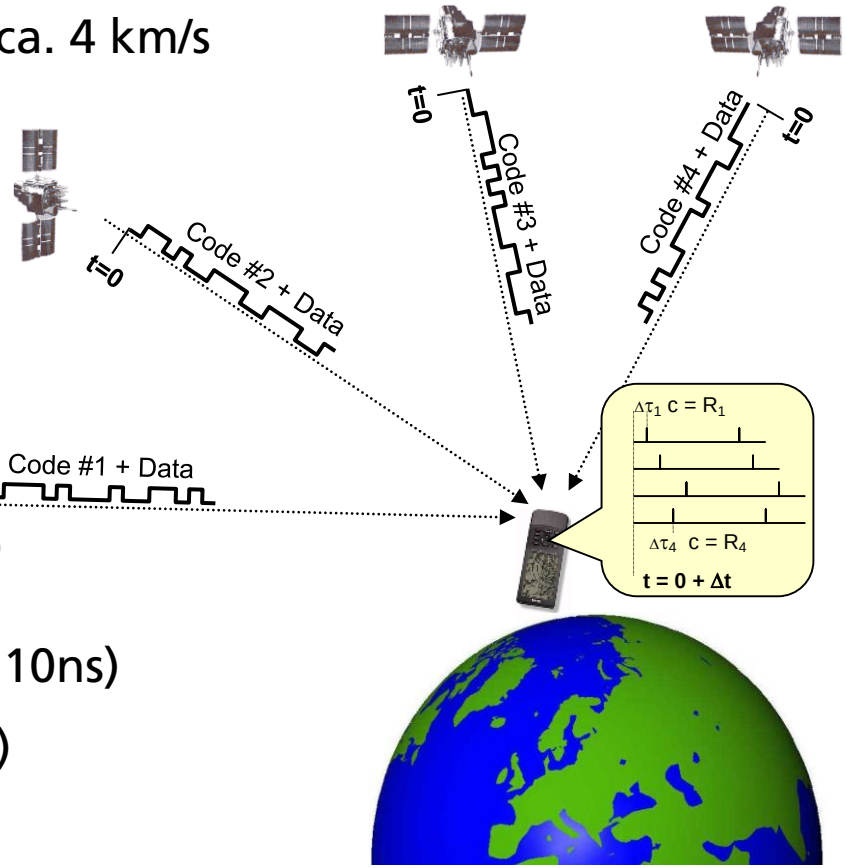
Group Manager Specialized GNSS Receivers
Satellite Based Positioning Department
Fraunhofer Institute for Integrated Circuits IIS
Nordostpark 93, 90411 Nuremberg, Germany
Phone + 49 911 58061-6379 | Fax +49 911 58061-6398

alexander.ruegamer@iis.fraunhofer.de

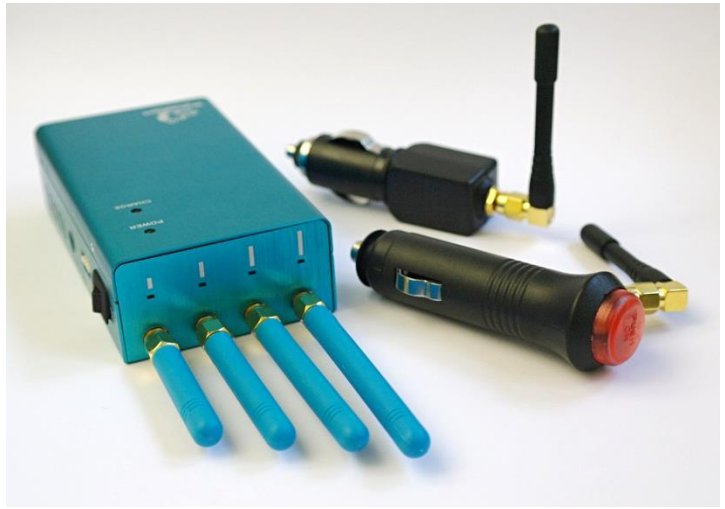
Backup

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 ?!



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…

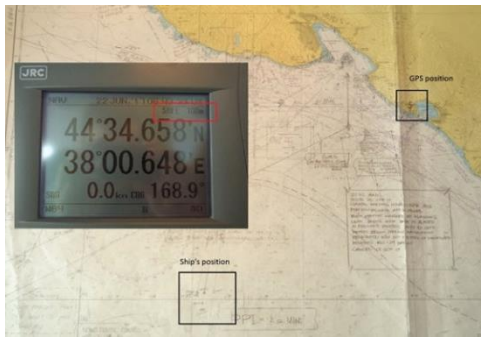
GNSS Störungen und Vorfälle
Jamming

- 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.

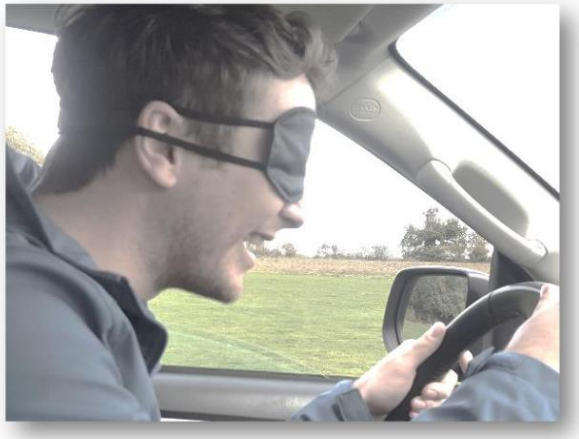
https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea

https://insidegnss.com/sinister-spoofing-in-shanghai/

Fraunhofer IIS

Täuscher (Spoofer)
Definition

Jamming



Spoofing

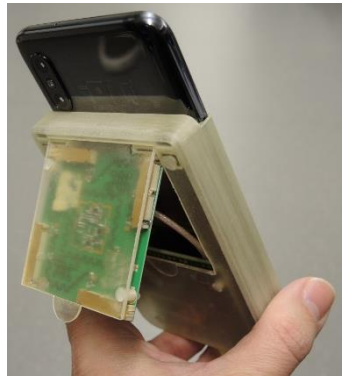
- Definition:
  - Übertragung eines gefälschten GNSS-Signals
  - Vortäuschen einer GNSS-Empfänger Positions- bzw. Zeitlösung
  - Potentiell größere Gefahr als Jamming!

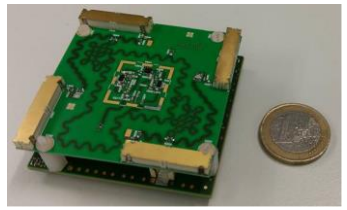
- Grundsätzliche Klassifizierung:
  - Manipulation am Gerät
  - Meaconing (Wiederaussenden eines authentischen Signals)
  - Spoofing (Generierung eines gefälschten Signals)

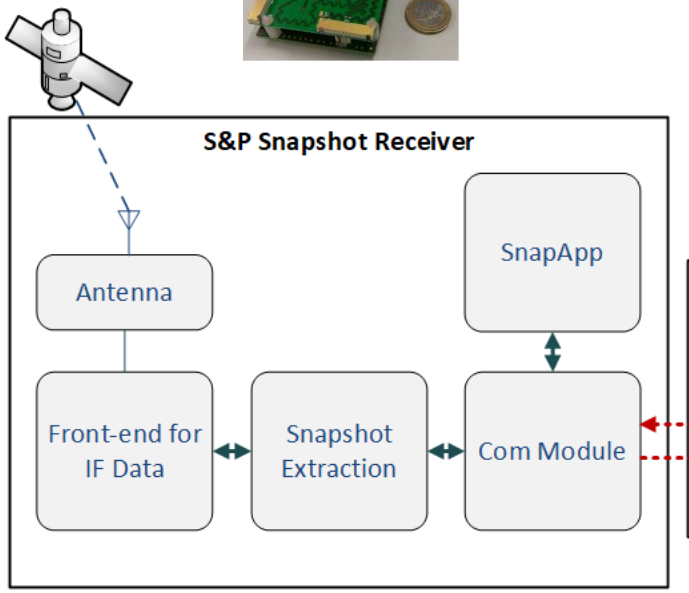
Mit et al., „Analyzing Tesla's Level 2 Autonomous Driving System Under Different GNSS Spoofing Scenarios and Implementing Connected Services for Authentication and Reliability of GNSS Data", ION GNSS+ 2020

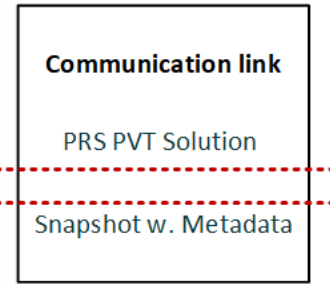
“Serverbasierte” Galileo PRS-Empfänger

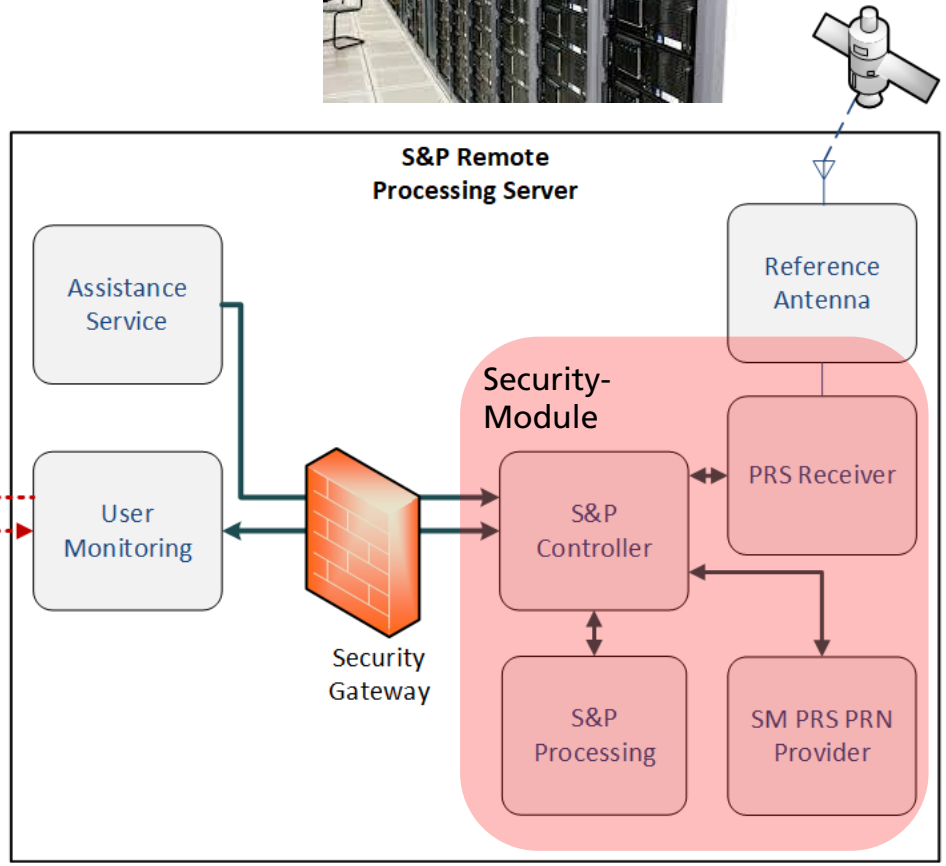
Server-based PRS “Sample & Process”







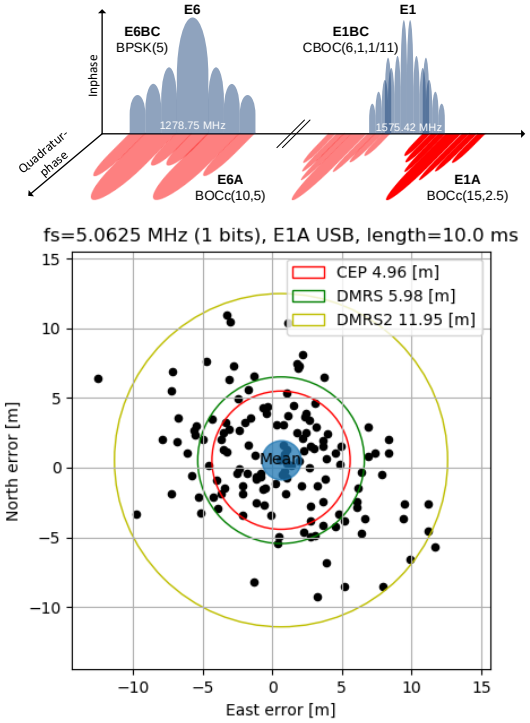




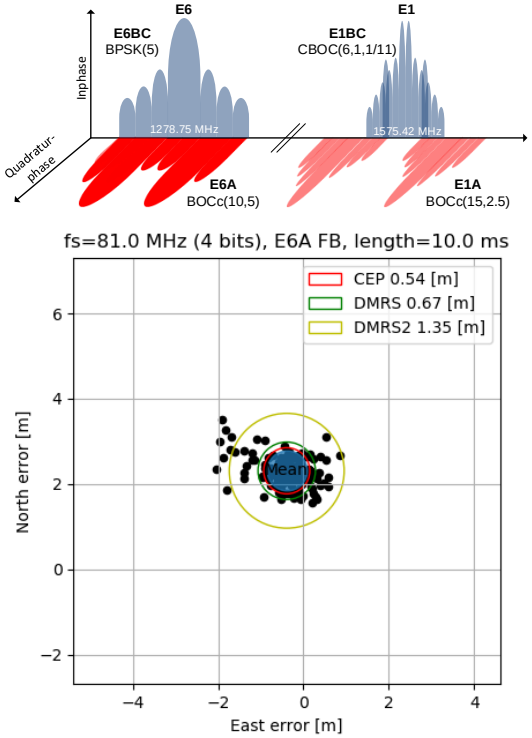
- Idee: ausgelagertes Sicherheitsmodul
  - Kein Keying des Endgerätes; einfache Handhabung
  - Günstige, kleine, energiesparsame Endgeräte möglich
- Allerdings anderweitige Einschränkungen / Trade-offs wie Latenz, Abhängig vom Use-Case

“Serverbasierte” Galileo PRS-Empfänger

Beispiel „Nürnberg“

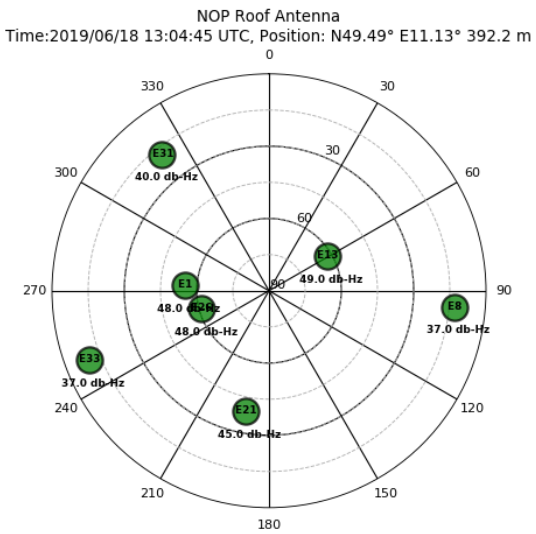


- Low snapshot size: E1A USB / BPSK(2.5)
  - 12.7 kByte / Snapshot for single PRS PVT



- 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

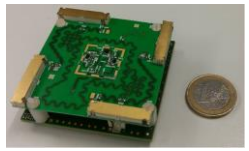


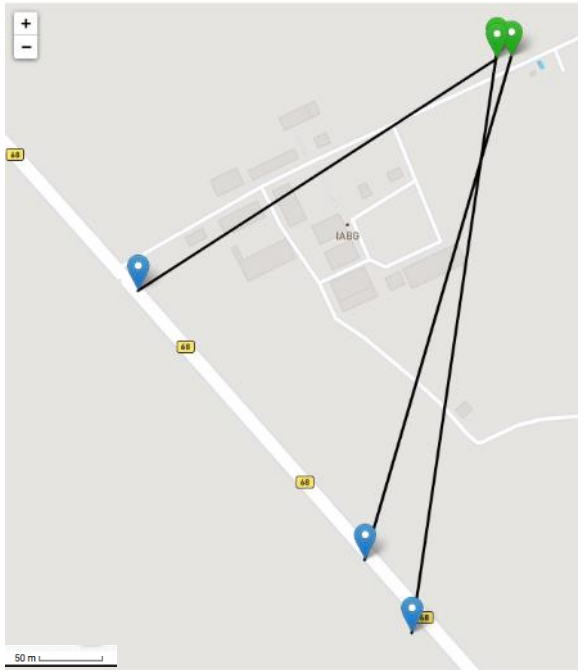
GDOP: 1.86
PDOP: 1.67
HDOP: 1.06
VDOP: 1.29

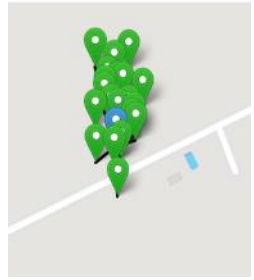
Fraunhofer IIS

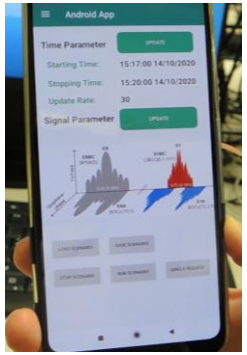
“Serverbasierte” Galileo PRS-Empfänger

Test-Kampagne









- Server-based PRS „Sample&Process“ withstands spoofing attack
  - OS-S&P solution spoofed; PRS-S&P solution secure
  - Both post processing results

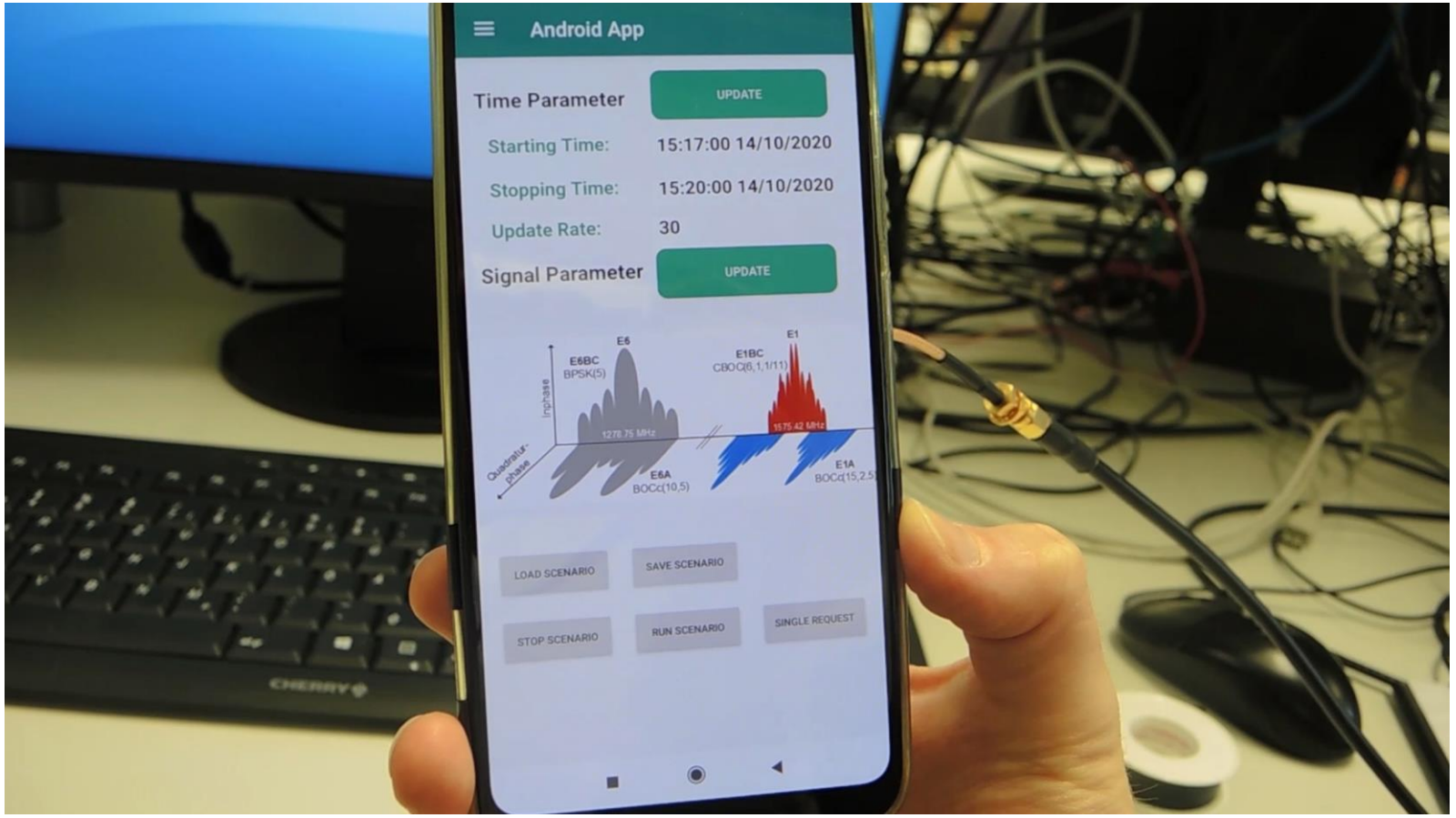
S&P solution PRS

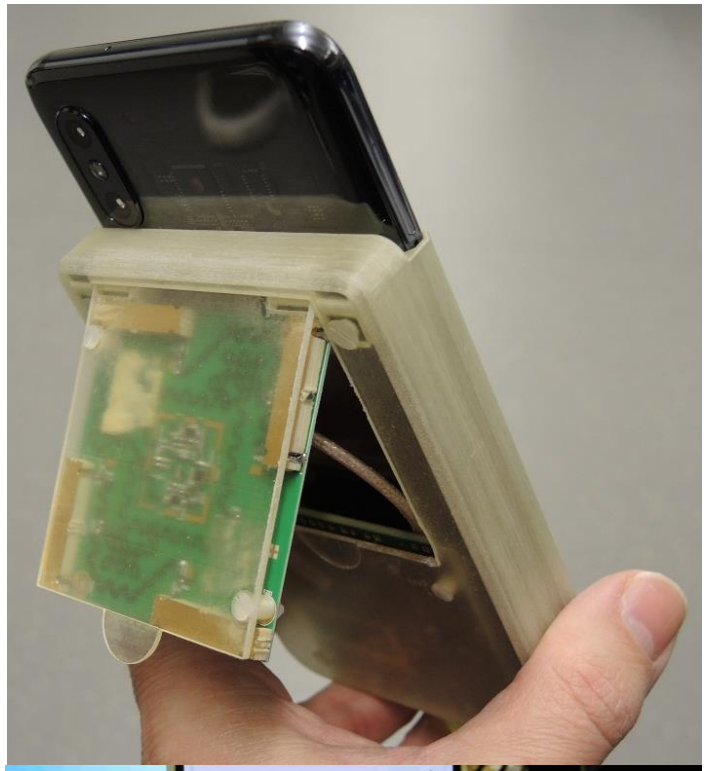
S&P solution OS

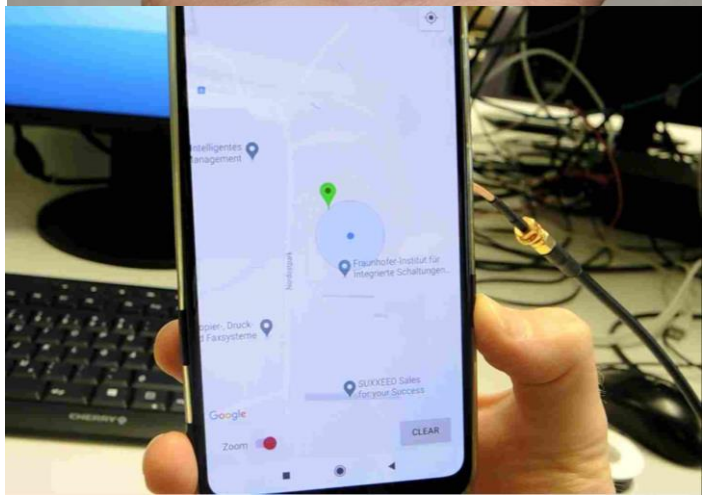
Fraunhofer IIS

“Serverbasierte” Galileo PRS-Empfänger

Snapshot-Rx PRS with Smartphone







Fraunhofer IIS