



Jamming und spoofing
von GPS/GNSS Signalen
Karen von Hünnerbein



Agenda

Beispiele für Jamming und Spoofing

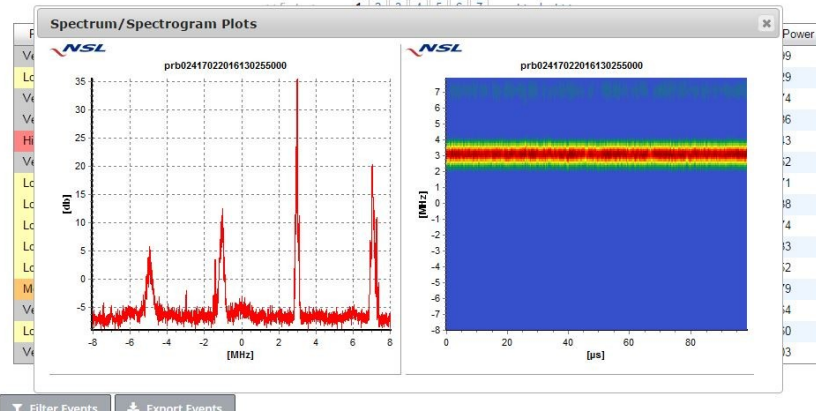
Technische Lösungen:

- Detektion und Monitoring
- Mit RF Simulation Empfänger testen zum Härten
- Intelligentes Vorschaltgerät InVo
Herausfiltern der Störsignale



DETECTOR Monitoring Centre

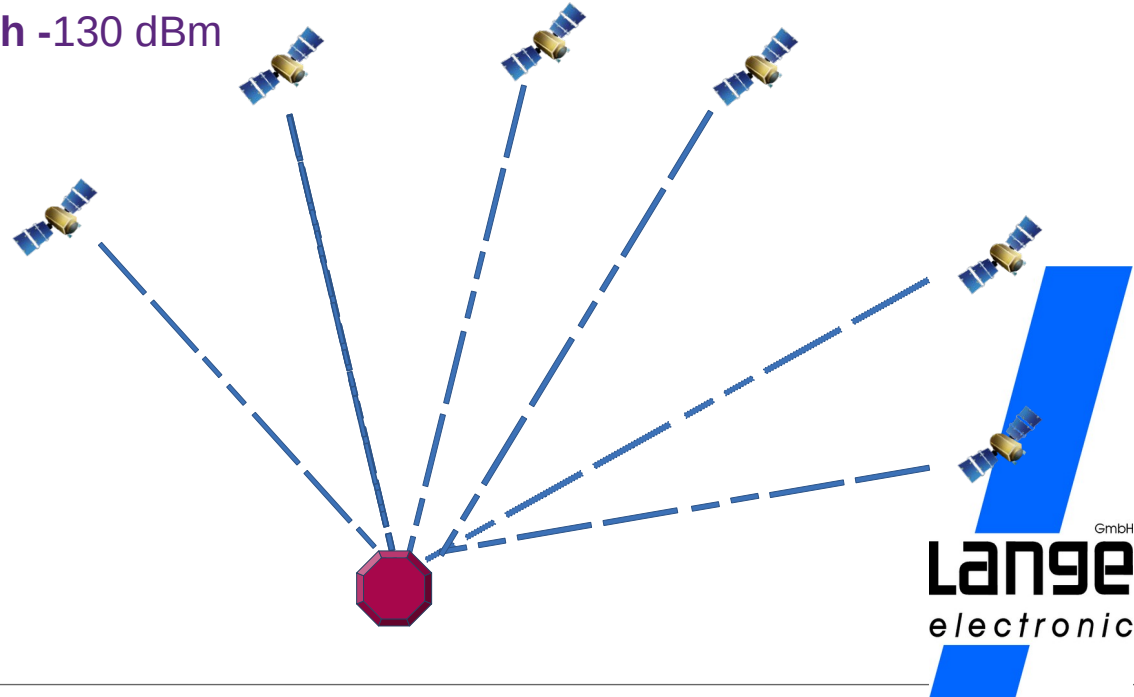
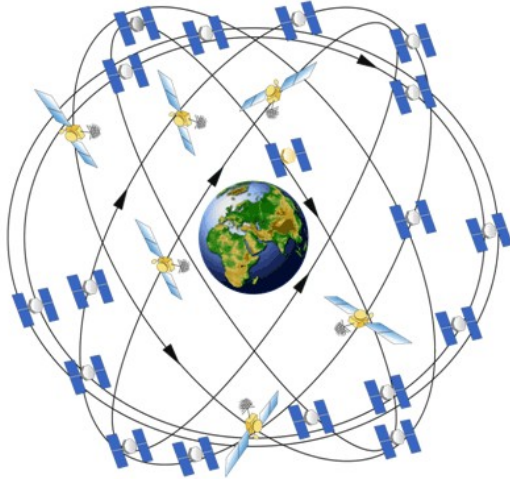
The list below shows the interference events as picked up by the DETECTOR probe(s).



GPS / GNSS Signale Eigenschaften

- * Die GPS Satelliten bewegen sich ständig
- * Die Signale kommen **aus unterschiedlichen Richtungen**
- * Tiefstehende Signale werden oft blockiert
- * GPS Signale **sind sehr schwach** -130 dBm

- genaue 3D Position
- * überall
- * weltweit
- * unter freiem Himmel



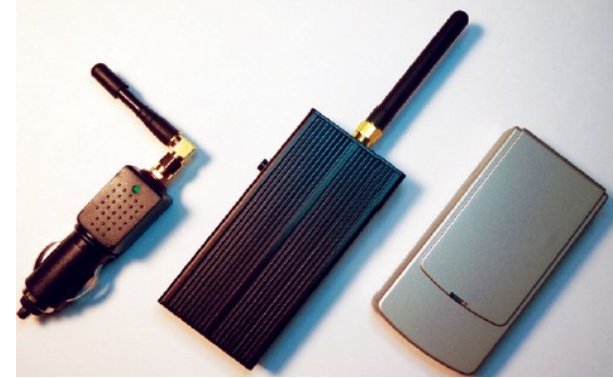
Jamming - Störsignale

Versehentliche Interferenz:

Jeder Sender in demselben Frequenzband L1, L2, L5

Defekte Elektronische Geräte,
die Rauschen senden

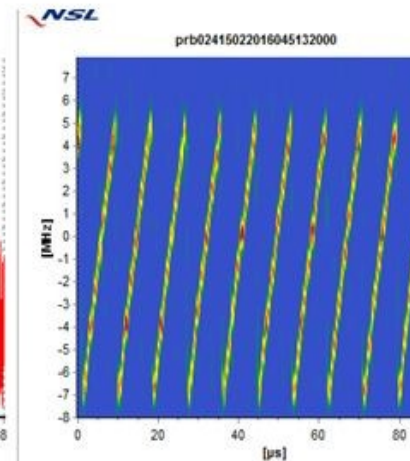
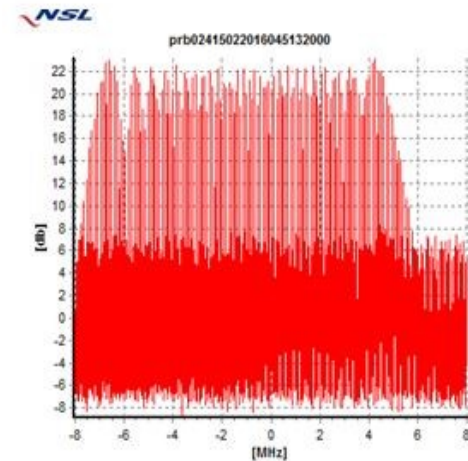
Mehrere Sender gemeinsam können
stören durch Intermodulationseffekte



Absichtliches Jamming:

Senden starker L Band Signale
zum Verhindern von GPS Empfang
Beispiel: Personal Privacy
Devices LKW Fahrer

Das führte zu Ausfällen eines Bodenkorrektur-
Systems am Newark Flughafen vor ca. 13 Jahren
Jammer auf dem nahegelegenen Highway



Beispiele für Jamming 2016 an A2

Event 2: CDMA interference, rating 8.2307

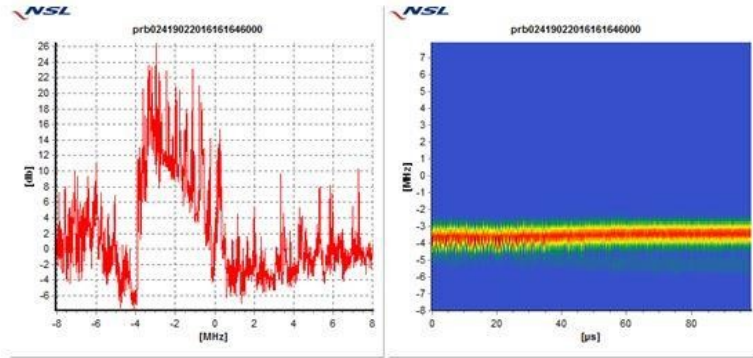


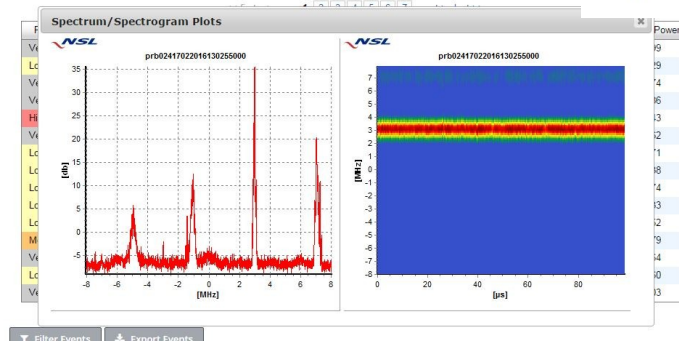
Figure 8: CDMA interference event (Feb. 19 2016, 16:16:46 UTC)



DETECTOR Monitoring Centre

The list below shows the interference events as picked up by the DETECTOR probe(s).

Institute of Flight Guidance

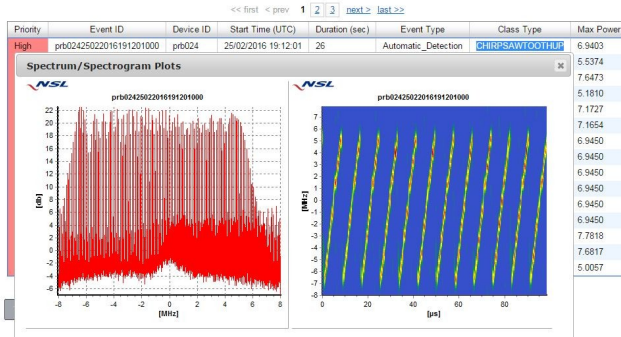


N=238
Alarm= 35



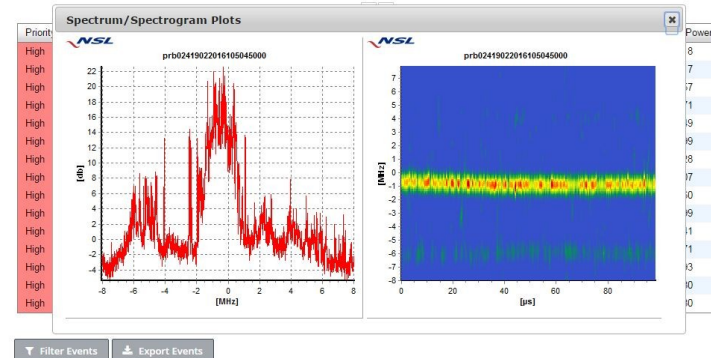
DETECTOR Monitoring Centre

The list below shows the interference events as picked up by the DETECTOR probe(s).



DETECTOR Monitoring Centre

The list below shows the interference events as picked up by the DETECTOR probe(s).



Auswirkungen von Jamming

Institute of
Flight Guidance



Jammingsignale

Event 2: CDMA interference, rating 8.2307

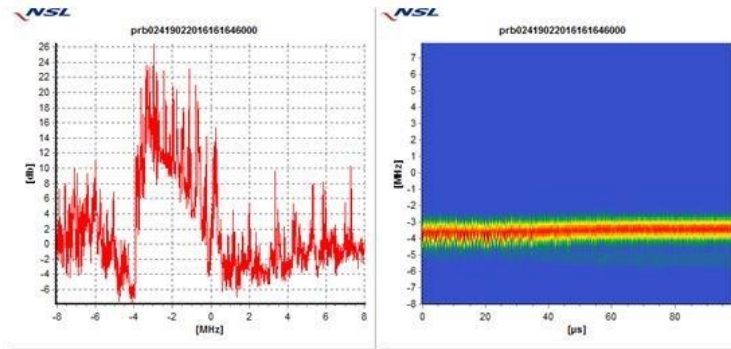
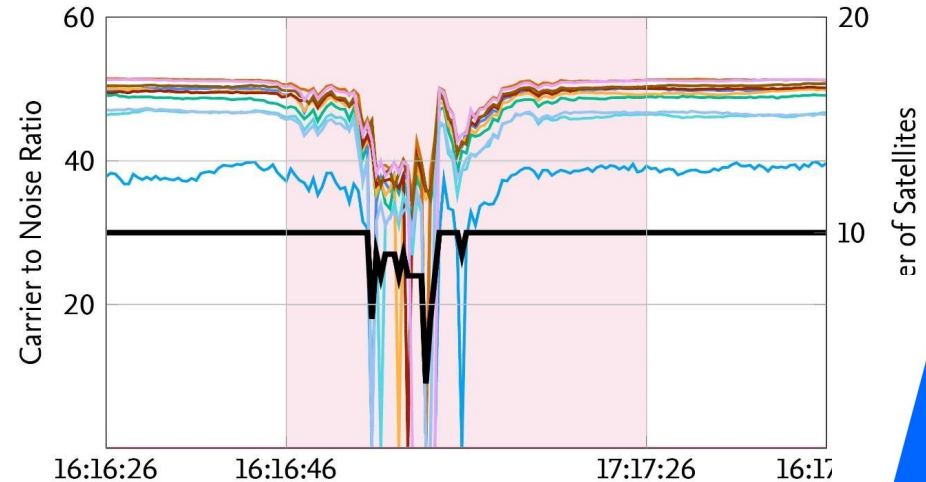


Figure 8: CDMA interference event (Feb. 19 2016, 16:16:46 UTC)

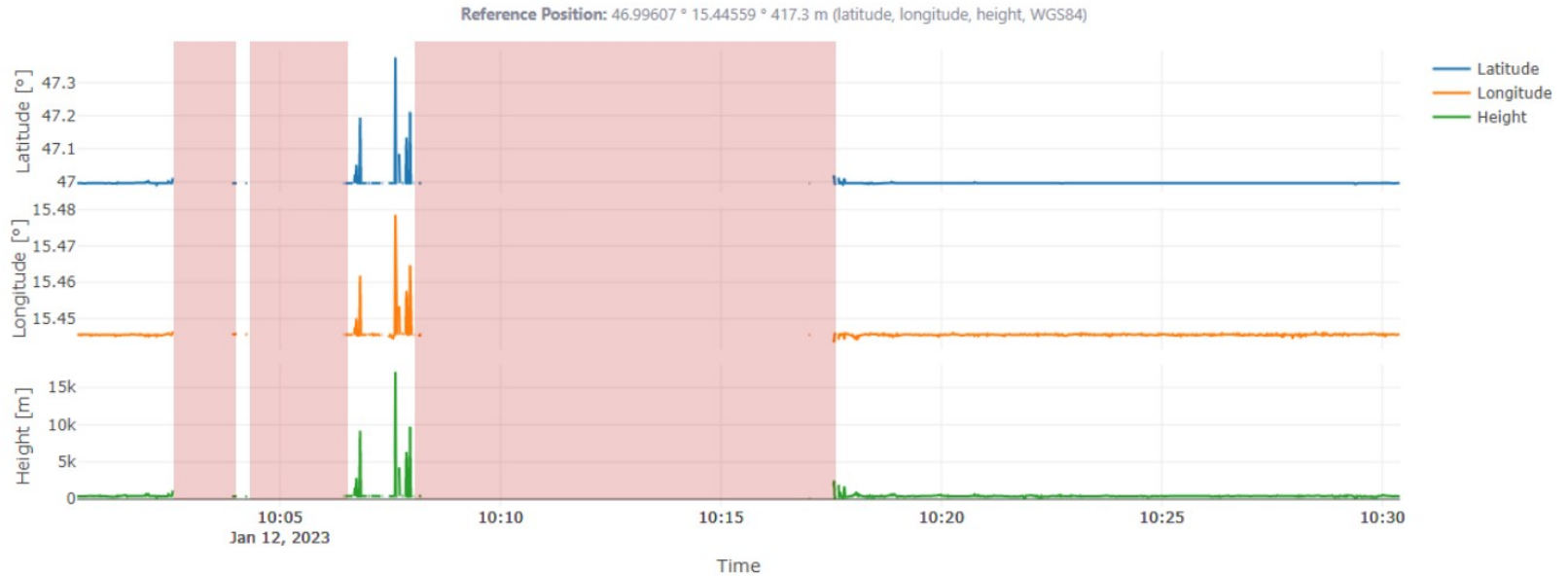
Empfangene Satellitensignale



Auswirkungen von Jamming 2

JAMMER – EXAMPLE 2

MS1 - LOCAL PVT DISRUPTED FOR MINUTES



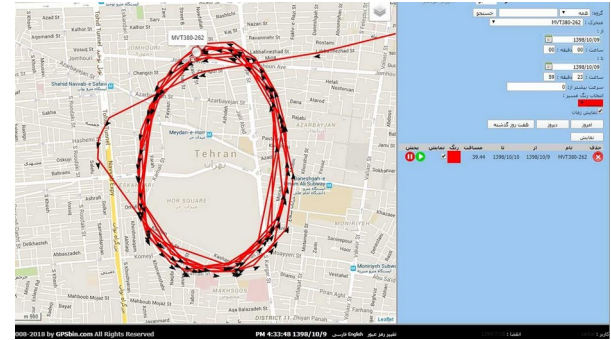
Spoofing - Täuschsignale

Von Unbefugten gesendete,
GPS/GNSS Signale

Die dem Empfänger eine falsche

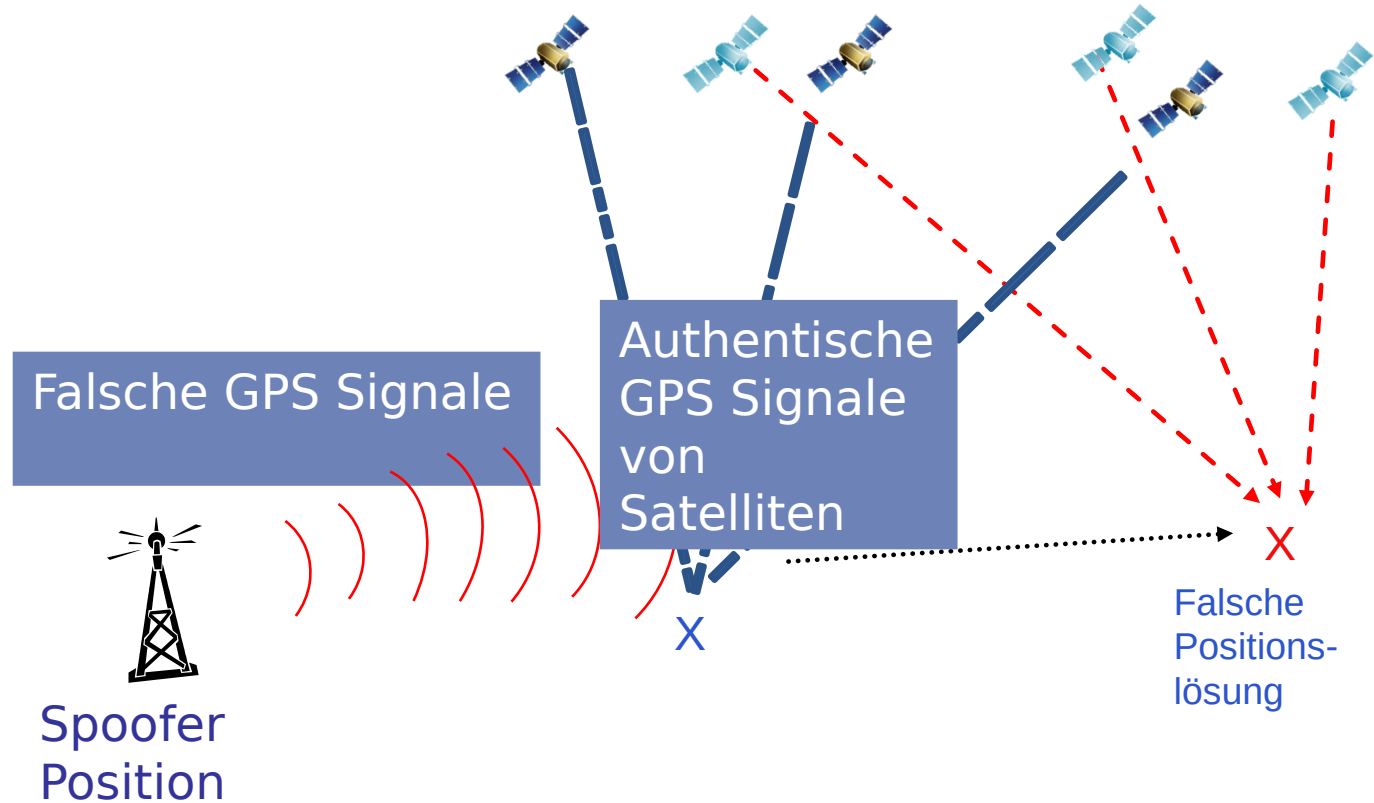
- * **Position** oder
- * **Uhrzeit**

vorgaukeln



Teheran 2020 Crop Circle
Spoofing
Screenshot Dana Goward

Spoofing - Täuschsignale



Spoofing ist oft schwieriger zu detektieren als Jamming

Technische Lösungen

Monitoring



Test und Validierung

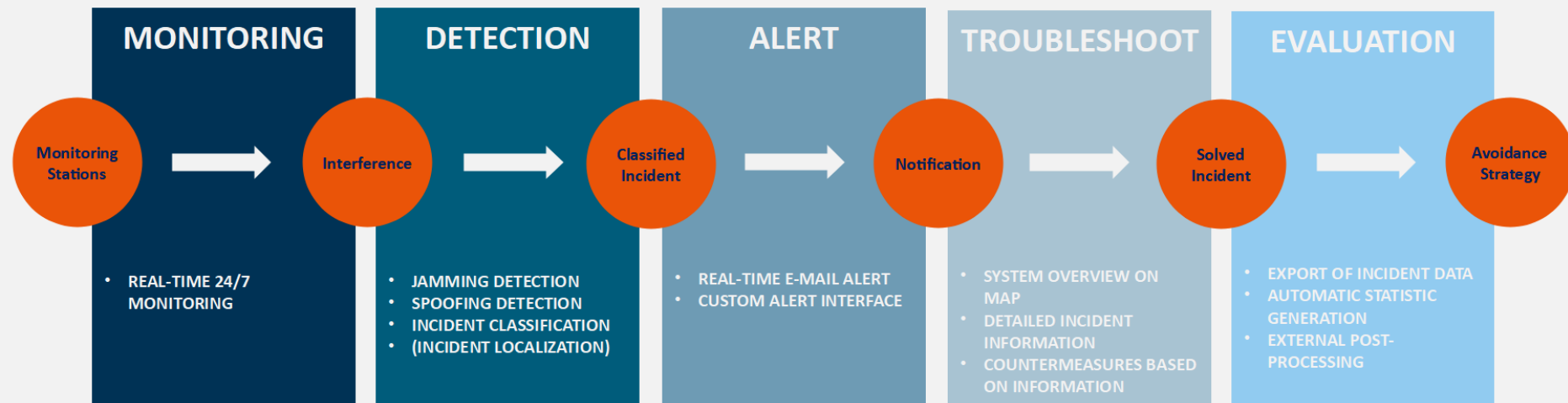


Abwehr



GIDAS - GNSS QUALITÄTSSICHERUNG

Monitoring der Signal Umgebung - Signalaufklärung



GNSS INTERFERENCE DETECTION AND ANALYSIS SYSTEM MONITORING UND ANALYSE VON STÖRSIGNALEN

STATIONÄR - drei oder mehr **MONITORING SENSOREN**
und ein **MONITORING CENTER**
für **kritische Infrastruktur**

PORTABLE - ein Koffer mit allem was nötig ist
für **Feldtests** - MOBIL UND FLEXIBEL

EMBEDDED - Detektor-Algorithmen integriert
in Anwender-Systeme

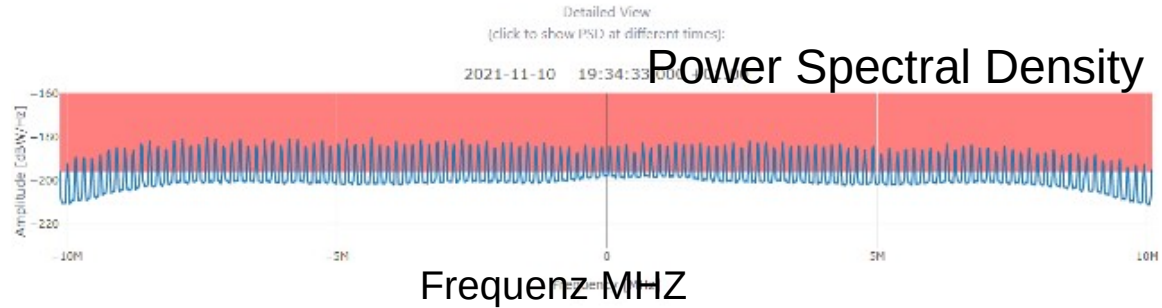


Jamming Ereignis

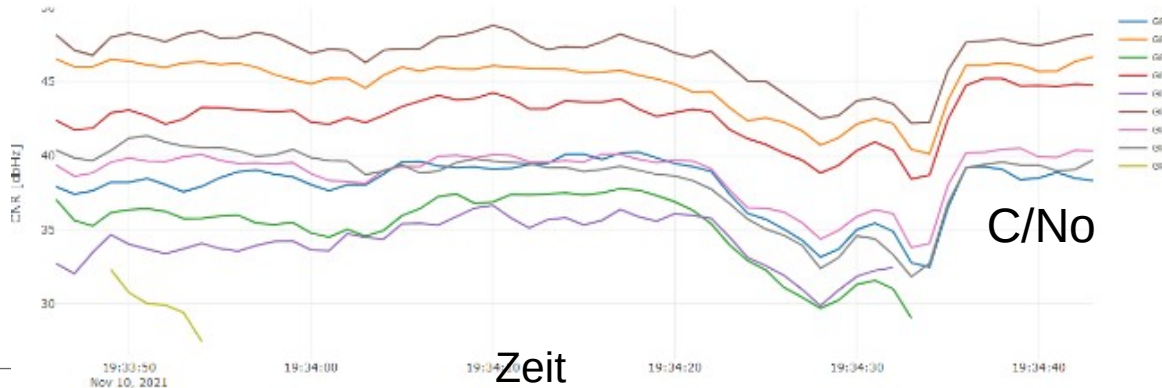


Wasserfall Diagramm für Signalstärke

- Starker Alarm in Tallin
- 10th Nov 2021
- 3 min Gesamtdauer
- 45 sec Alarm
- Viele Peaks über den gesamten Frequenzbereich



Power Spectral Density



C/No

Test mit GPS Satellitensignalsimulator

Realistische Emulation von

- * GNSS Signalen
 - * Jamming Signalen
 - * Spoofing Signalen
- gleichzeitig



 Introducing PNT X

Testumfang



- GNSS Signale: Multi GNSS und Multi Frequenz
- **Jamming Signale:**
 - CW, FM, AM, PM,
 - Breitbandiges AWGN, BPSK,
 - CW Pulse, Chirp und gematchtes Spectrum

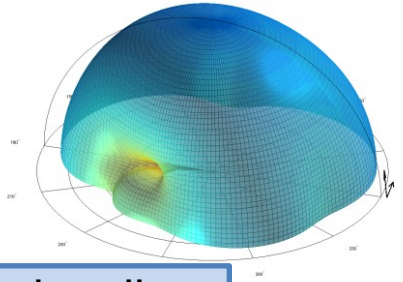
Spoofting Signale

- Mehrere Spoofsender
- Navigationsdaten-Attacke
- Meaconing Attacke
- Timing Fehler Attacke





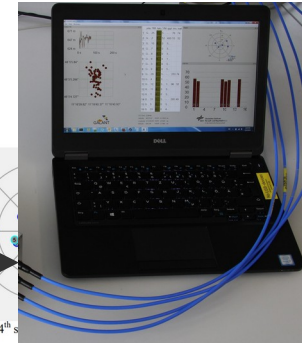
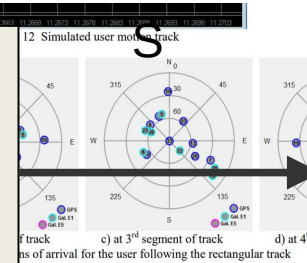
Vorhandenes
Antennenkabel



Konventionelle
L1/L5 GNSS
Empfänger

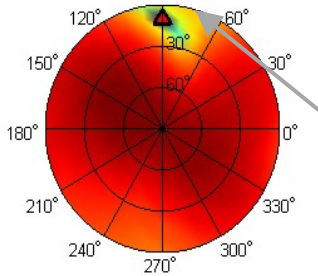
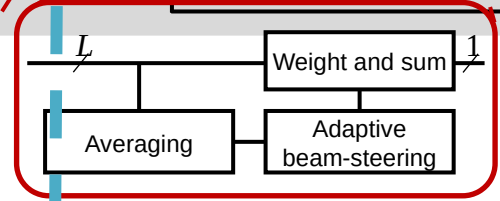
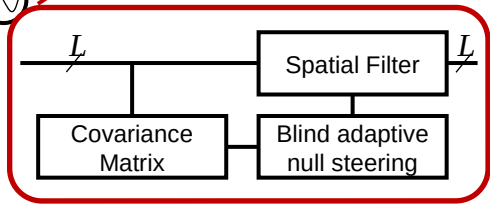
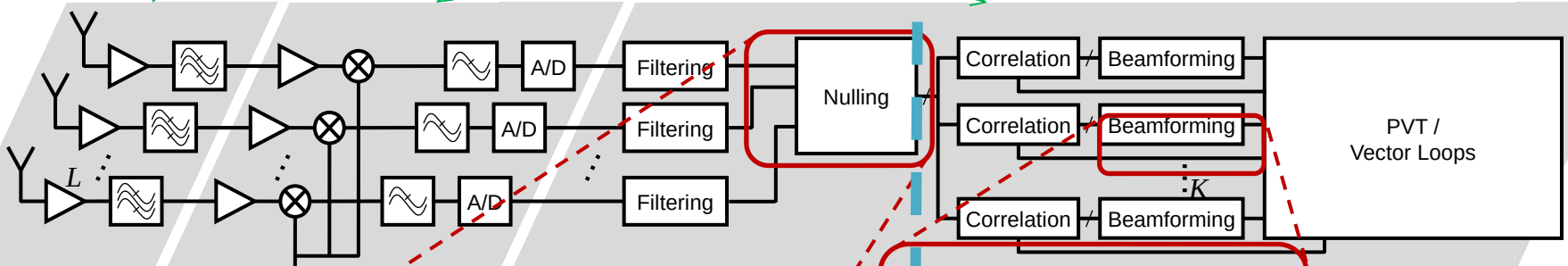
Ant-Out
MMI-Out
Power-In

Power-Input



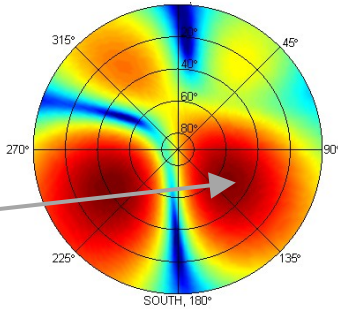
Darstellung von
Zusatz-
Informationen

Korrektoren

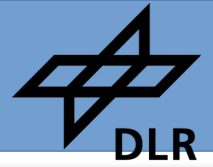


Räumlicher Nullpunkt in Richtung des Störsenders (gemeinsam für alle Signale)

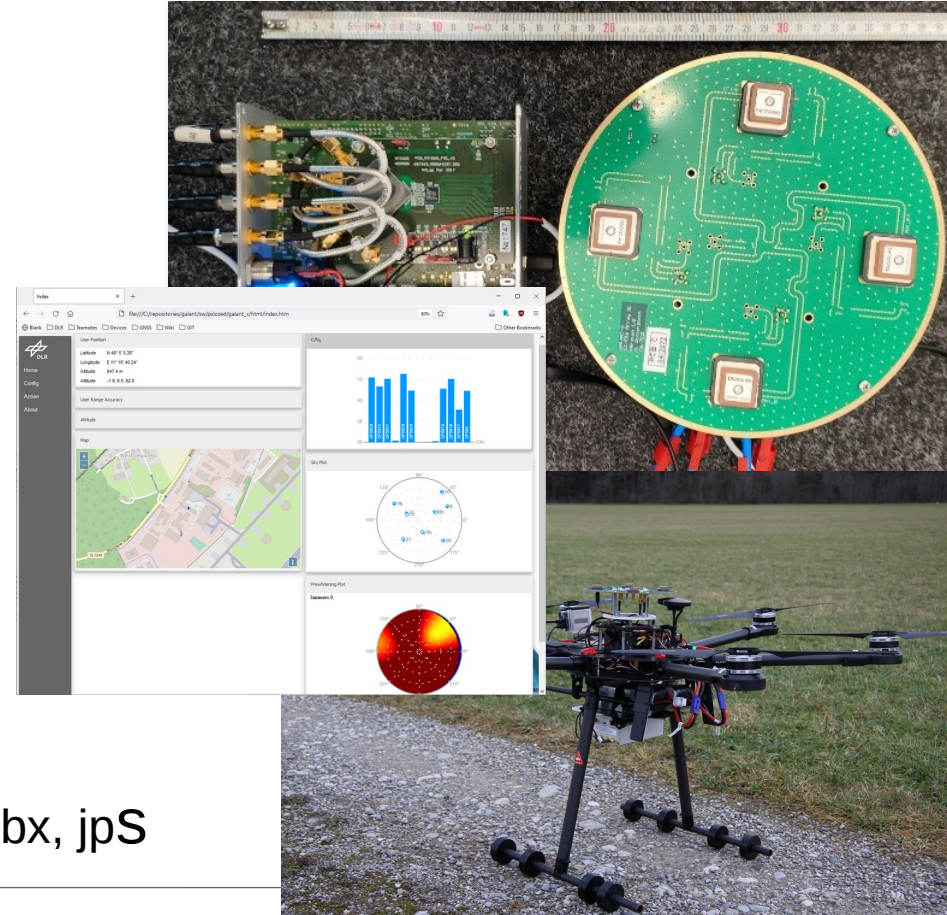
Maximale Verstärkung in Richtung des Satelliten (individuell für jedes Satellitensignal)



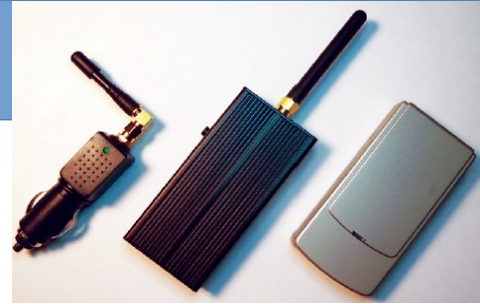
Robuster Navigationsempfänger auf UAS



- Jamming Unterdrückung (CRPA)
- Digitale Antennendiagrammsteuerung
- Richtungsschätzung für GNSS-Signale
- Peilung von Störsignalen
- Lagebestimmung
- INS coupling
- RTK Positionierung
- Blinde Kalibrierung für hochgenaue Richtungsschätzung
- GPS L1/L5, Galileo E1/E5a
- Webserver GUI, RTCM, Rinex, NMEA, ubx, jps



Was bringen diese Lösungen?



1. **GIDAS:** Man weiß Bescheid, welche Störsignale vorhanden sind

- Man kann nach den Quellen suchen zum Entfernen / Abschalten

2. **GNSS/Jamming RF-Simulation im Labor**

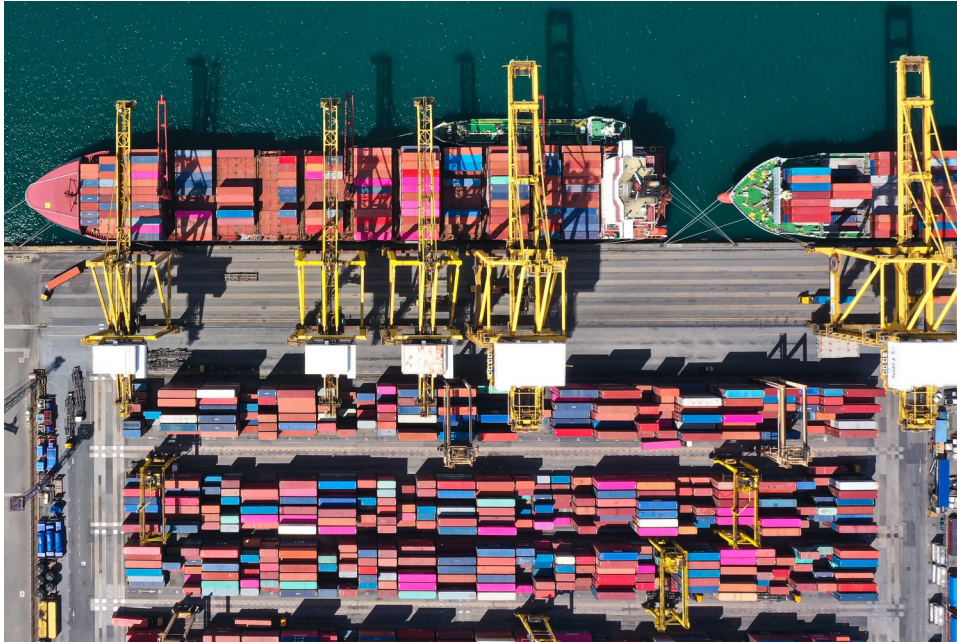
- Kontrolliertes und wiederholbares Testen
- bedeutet viel weniger Aufwand, spart Material und Zeit, Grenzfälle sind testbar

3. **Intelligentes Vorschaltgerät:**

- Störsignale entfernen im Betrieb
- Besseres Lagebild: Erkennen von Spoofing und Jamming

Lagebild: Störsignale
robustere Avionik
Mehr Resistenz des
Navigationssystems an
Bord und Lagebild

Mein Dank geht an



- ❖ Manuel Cuntz, DLR
- ❖ Mirko Stanisak IFF, TU Braunschweig
- ❖ Hafenbilder Adobe Stock