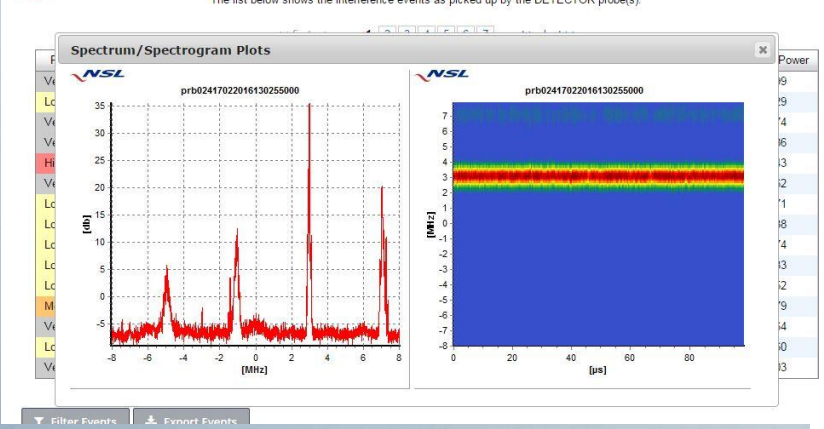




# Jamming und Spoofing von GNSS-Signalen

## Störpotential sowie Ansätze zur Detektierbarkeit

***Karen von Hünerbein***
***Werner Lange***

Lange-Electronic GmbH

Technische Universität Braunschweig

# Gliederung

- Was bedeutet Jamming, Spoofing, Meaconing?
- Woher kommen die Störsignale?
- Beispiele für Störer
- Auswirkungen auf GPS / GNSS Empfänger
- Störreichweiten
- Ansätze zur Detektierbarkeit

*GNSS Global Navigation Satellite Systems*

Lange GmbH electronic

# GPS und andere GNSS

*GNSS Global Navigation Satellite Systems*

GPS / GNSS ist Schlüsselsystem
in Hunderten von Applikationen

- *u.a. im Autonomen Fahren*
- *kritische Infrastruktur*
- *Luftfahrt*

nicht nur bei Ortung und Navigation sondern auch bei präzisem Timing

zeichnet sich aus durch sehr geringe Signalstärken von um die -130 dBm
→ liegt damit im thermischen Rauschen

und ist dadurch leicht störbar

Lange GmbH electronic

# GPS Timing in kritischer Infrastruktur

- Mobilfunk-Basisstationen
- Telekommunikations- und TV Netzwerke

- Banken und Geschäfte nutzen Zeitstempel
  - Verwalten zeitkritischer Transaktionen
  - Währungs- / Aktiengeschäfte korrekte Zeit = korrekter Kurs

- Synchronisieren von Computer Netzwerken

  (Driften der internen Computeruhren)

- 

  Stromnetzbetreiber

  Synchronisieren der Phasen des Wechselstroms

Lange GmbH electronic

# Was bedeutet Jamming, Spoofing, Meaconing

Jamming – wird verursacht durch Sender und Störsender,

die in demselben Frequenzband L1, L2, L5 senden,
z.B. DME -- Distance Measuring Equipment in der Luftfahrt

Unabsichtlich: z.B. Defekte Elektronische Geräte, Zigarettenanzünder

Absichtlich: Senden starker L-Band Signale zum Verhindern von GPS Empfang

[Bauernfeind et.al. 2012, "Analysis, Detection and Mitigation of In-Car GNSS Jammer Interference in Intelligent Transport Systems"]

Meaconing

Wiederabstrahlen empfangener GPS Signale

→ verzerrt Zeitinformationen oder Empfangsposition

Spoofing Senden von Täuschsignalen, die den realen GPS/GNSS Signalen sehr ähnlich sehen

→ und dem Empfänger eine falsche Position oder Zeit vorgaukeln

# Beispiel für Spoofing

Global fishing watch project - 2014
Satellite AIS Receiver – Reception footprint shown (Atlantic Ocean)


Two ships observed definitely spoofing their position – either spoofing GPS or inserting false data into the AIS transponder

AIS: Automatic Identification System

Vermutlich ein Fall von Selbst-Spoofing

Mehrere Erfolgreiche Spoofing Demos als Test z.B. Uni Texas 2012

Einfach realisierbar mithilfe GNSS Signalgenerator oder SW Defined Radio

Lange GmbH electronic

# Hannover Flughafen 2010 - Meaconing

Ein GPS Repeater im Hangar war in Betrieb
weniger als 1000 m von der Landebahn entfernt


Flugzeuge erhielten Bodenähe -Warnungen
und Landebahn- Abweichungs-Warnungen

**ein Flugzeug hob ab mit nomineller GPS Position im Hangar**

Es stellte sich heraus

- Zu hohe Signalstärke des Repeaters
- Die Hangar Tür blieb manchmal
  offen bei laufendem Repeater-Betrieb

Lange GmbH electronic

# Newark Airport gestört durch LKW Jammer

FIGURE 7 Overview map of Newark Airport

GBAS System stürzte wiederholt ab durch LKW Privatjammer auf nahegelegener Autobahn

Mehrere GBAS Antennen wurden gleich-zeitig gejammt

FIGURE 8 LAAS Ground Facility site at Newark Airport showing GBAS antenna locations

Sam Pullen & Grace Gao
Inside GNSS March/Apr 2012

Lange GmbH electronic

# Aktuelle Beispiele

Derzeit findet im östlichen Mittelmeer ein großes Jamming Event statt

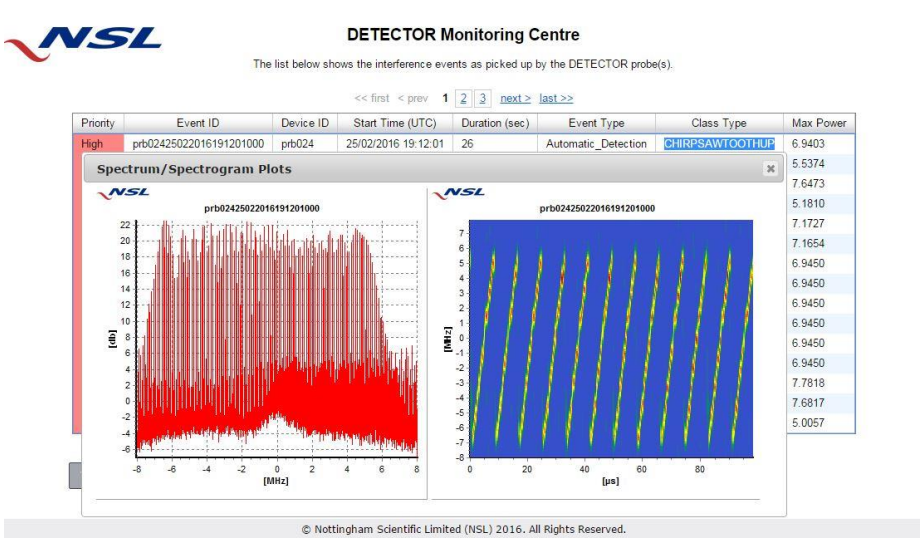
- Linienflugzeuge melden weiträumige GPS Ausfälle
- Der Störer wird in Syrien  vermutet

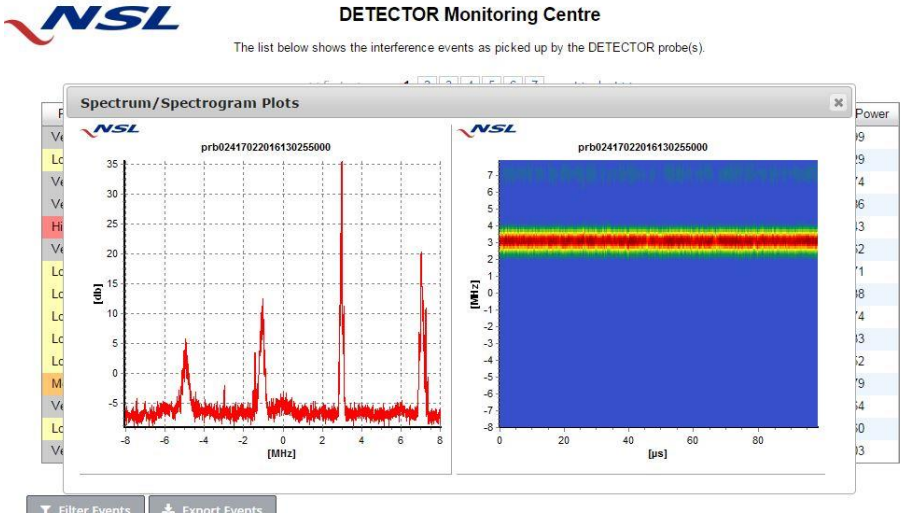
Quelle: Dr. Butsch, DFS

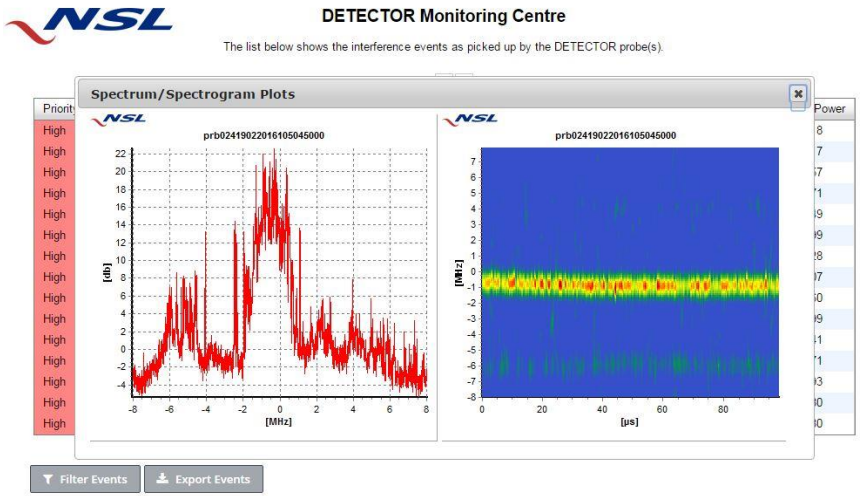
Vor kurzem sind bei großer Drohnenflugshow in Hongkong

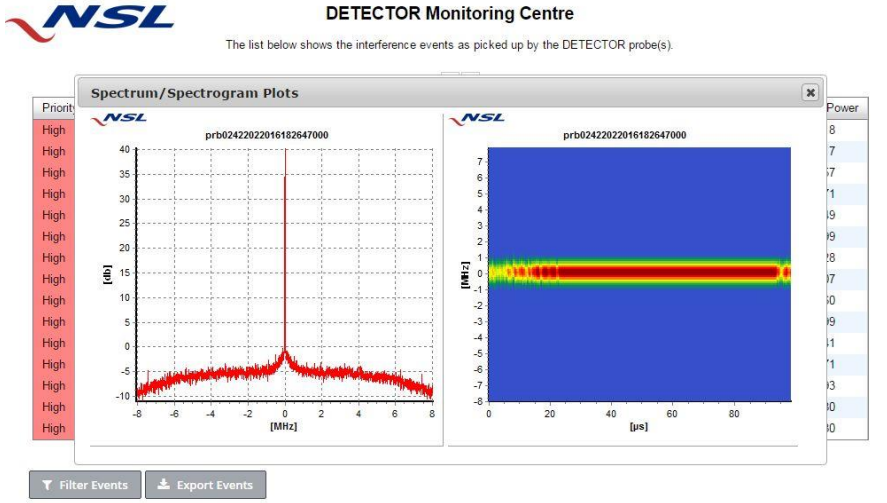
- 40 Drohnen abgestürzt wegen Jamming
- 1 Mio $ Schaden

# Beispiele für Störereignisse




Technische Universität Braunschweig

electronic

# Auswirkungen auf GNSS Empfänger

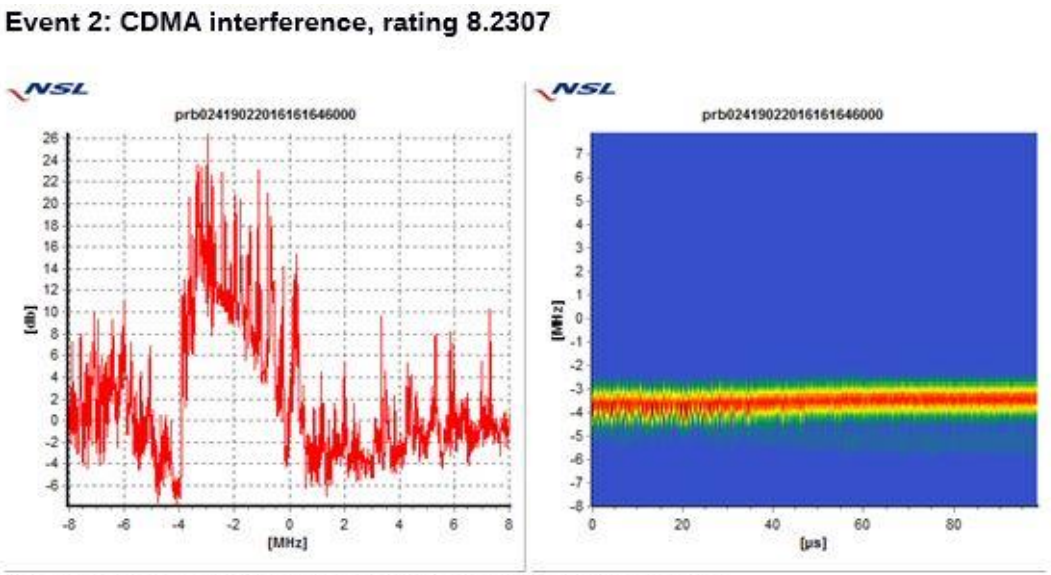
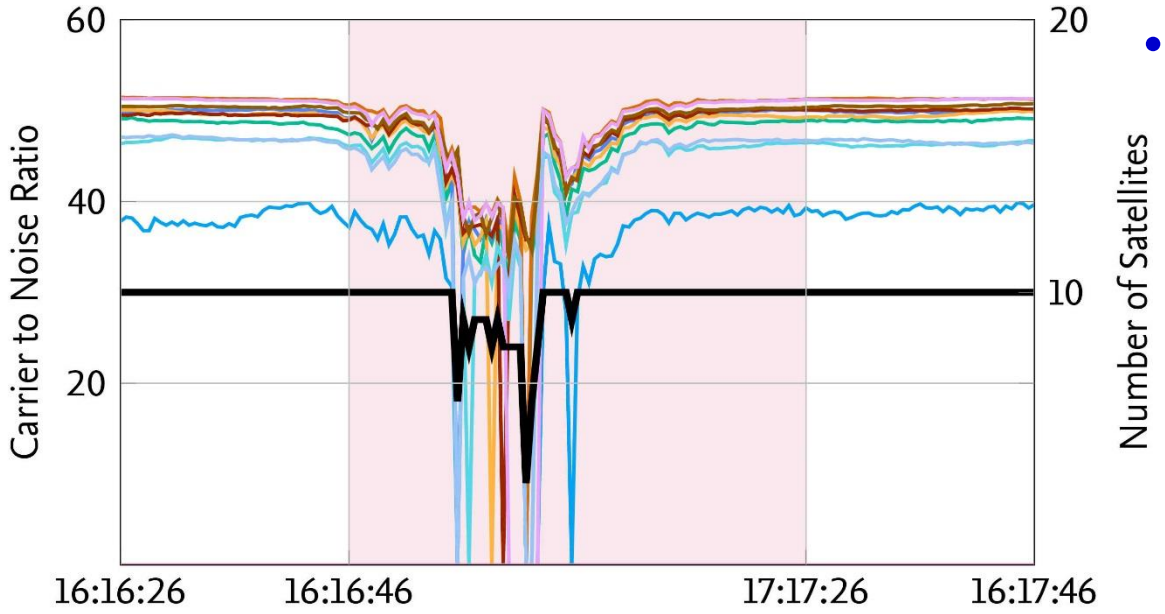



*Figure 8: CDMA interference event (Feb. 19 2016, 16:16:46 UTC)*

Institute of Flight Guidance

- Geringeres Carrier to Noise Ratio
- Weniger Satelliten werden getrackt




Lange GmbH electronic

# Störpotential ist erheblich

- Weniger getrackte Satelliten,
- Totalausfall GPS/GNSS Signale
- Ungenaue Position
- Falsche Position
- Abstürzende Drohnen und Flugzeuge
- Totalausfall Kommunikationsnetzwerke

- Die Reichweiten der Jammer sind oft größer, als der Störer denkt

Jammer power: 21 dBm (125 mW)

Jammer power in 100 m distance: -55 dBm

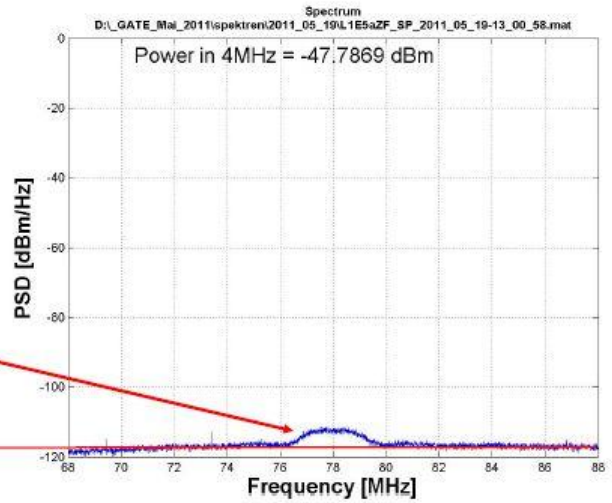
GNSS Signal: -127 dBm

J/S = 72 dB = 16 000 000 : 1

Lange GmbH electronic

# Einfluß Störsignal am analogen Front End

## Spectrum at Analog Front End Output without RFI



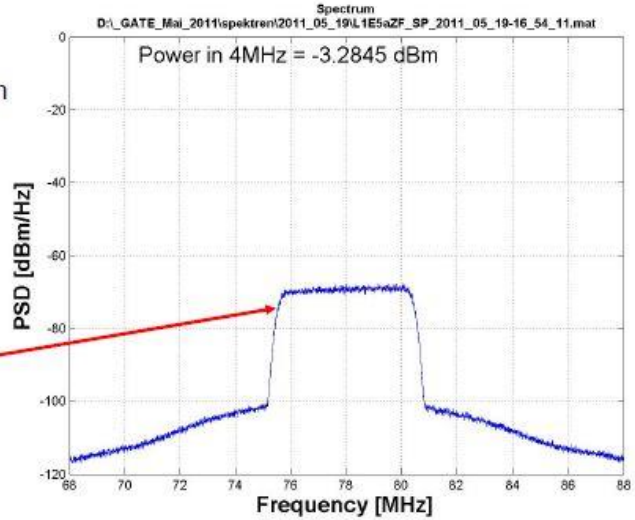

GPS + Galileo signals

Noise power density =
N0 = -116 dBm/Hz



## Spectrum at Analog Front End Output with RFI

I/N0 = -3,3 dBm + 116 dBm
I/N0 = 112,7 dB




BBN interference
(Tx power = -10 dBm)

# Ansätze zur Detektierbarkeit

- externe Messsysteme
  - Spectrum Analyzer
  - eigens dafür gebaute Detektor-Geräte

- Interne Prüfung im Empfänger:
  - Abnahme C/No - Satellitensignalverluste unspezifische Phänomene
  - Automatic Gain Control – höhere Rauschstärke
  - Spoofing + Meaconing – alle Satelliten sind mindestens doppelt vorhanden

- Zusatz-Systeme:
  - Vergleich mit anderen Sensoren
  - Antennenarrays – CRPA
  - verbesserte Algorithmen
  - SBAS und andere externe Korrekturdaten

Lange GmbH electronic

# Externe Messsysteme zur Detektion

Spektrum Analysator zeigt Störereignisse in einem Band an

* Rohdaten können gespeichert werden
* dann aufwendiges post processing


ITK Interference Toolkit mißt Signalstärken an mehreren Orten – rechnet daraus eine Störerkarte

DETECTOR erkennt Störereignisse

* speichert kurze Signalschappschüsse
* Sendet Alarm bei starken Events

Lange GmbH electronic

# Externe Messsysteme zur Detektion

JammerCam™ in situ at motorway services

Jammer Cam misst Interferenz
* macht ein Foto vom Fahrzeug,
* Versendet es per Mail mit Positionsdaten

GPS L1 Signalstärkemessung zeigt Störereignisse – Signalstärke per 8 LEDs an
Bandbreite 20 MHz auf L1

Lange GmbH electronic

# Interne Prüfung im Empfänger

- höhere Gesamtsignalstärke
  - AGC Control liefert geringere Verstärkung
  - C/No sinkt unspezifisch, kann viele Ursachen haben
  - Verlust an getrackten Satelliten

- Vector Tracking - andere Empfängerarchitektur,
  kombiniert Signaltracking und Positions-Geschwindigkeitsbestimmung
  - Funktioniert bei geringerem C/No und
  - überbrückt Signalunterbrechungen

Quelle: Inside GNSS, 2009

- Direct Positioning - andere Empfängerarchitektur
  Ableitung der **Navigationsparameter** direkt aus den GPS Rohdaten
  - Mithilfe eines **Vektorkorrelators**,
    der die **zusammengesetzte Signalkopie** ermittelt,
    die am besten zum beobachteten GPS Rohsignal passt
  - Testergebnis: widerstand Jamming und Meaconing Angriff

Quelle: Ng und Gao, PLANS 2016

# Interne Prüfung im Empfänger -2-

- Bei Spoofing und Meaconing liegen alle Satellitensignale doppelt vor
  - Dann kann man mithilfe vieler Suchkanäle im Empfänger doppelte Korrelationspeaks finden, und die falschen ausschließen
  - Wenn alle Signale korrumpiert sind
    → Alarm und Einsatz alternativer Ortungstechnologie
  - Javad hat 200% größeren Rauschpegel bei Spoofing gemessen

SPIRENT

Frequency Domain Adaptive Filtering
Herausfiltern von Frequenzpeaks im Nutzband

Lange GmbH electronic

# Interne Prüfung im Empfänger

- **RAIM Receiver Integrity Autonomous Monitoring**
  - Wenn genügend Satelliten sichtbar sind kann man Subsets aus den Satelliten bilden und mit jedem Subset Positionen rechnen

  → bei größeren Ausreißern in der PVT Lösung gibt es ein Problem

  - Das funktioniert in der Luftfahrt, weil es in der Luft freie Himmelssicht gibt
  - Weniger gut in urbanen und bergigen Gegenden – wegen anderen Störquellen u.a. Multipath

- **Geplant Authentifizierungssignale bei Galileo mit Verschlüsselung**

SPIRENT

Lange GmbH electronic

# Zusatzsysteme

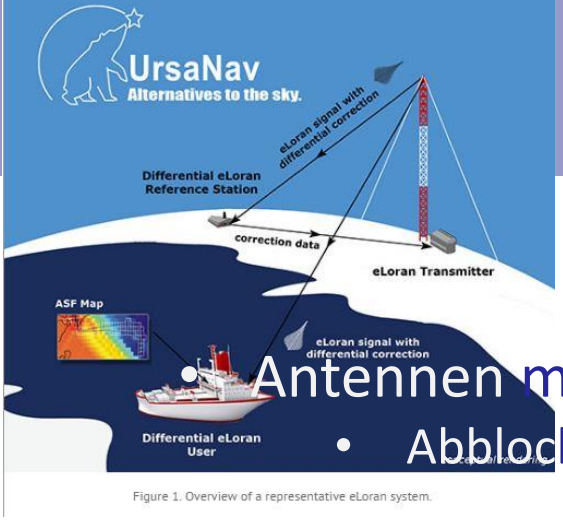
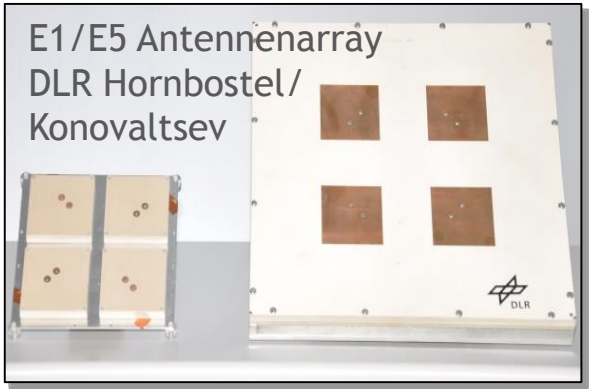


Figure 1. Overview of a representative eLoran system.


- Antennen mit geeigneter Empfangscharakteristik wählen
  - Abblocken niedriger Elevationen via Choke Ring

- Externe Korrekturdaten
  - SBAS
  - Integritätsinformationen




- Antennen-Arrays:
  - Digitales Beam-Forming

- Vergleich mit den Ergebnissen anderer Sensoren und Systeme
  - inertiale Sensoren
  - Andere Funktortungsverfahren, z.B. DME, e-LORAN
  - Stabile Crystal Oszillatoren oder Mobilfunkzeit für Timing

Lange GmbH electronic

# Technische Lösung:
# Frequency Domain Adaptive Filtering

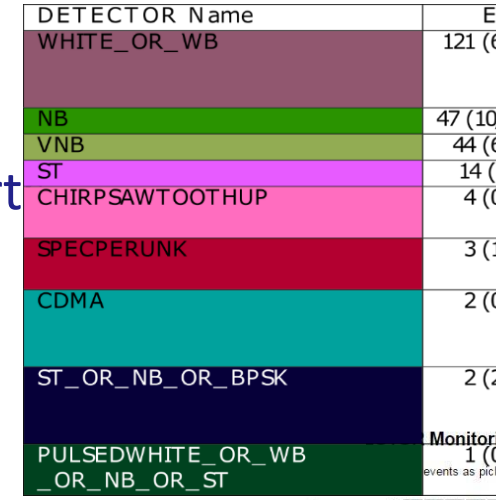
FDAF wird vor dem Korrelationsprozeß angewendet

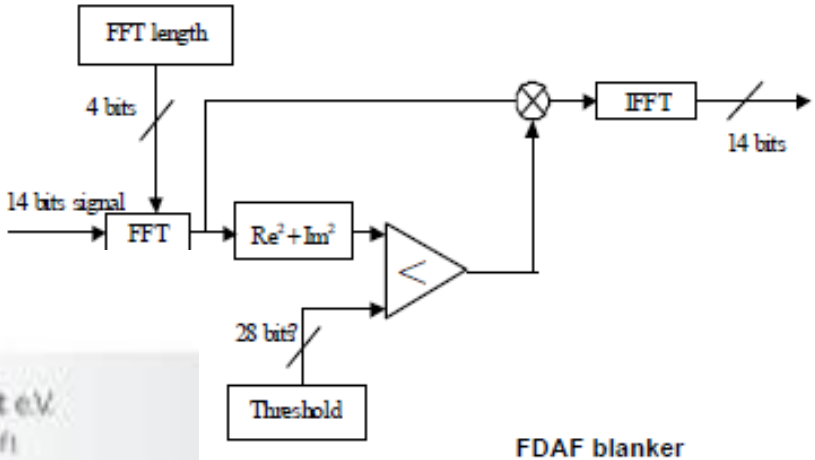
ZF Daten des Frontends werden per FFT konvertiert in Frequenzdomäne für jedes Antennenelement

Alle Frequenzen oberhalb eines gewissen Schwellenwert werden annulliert

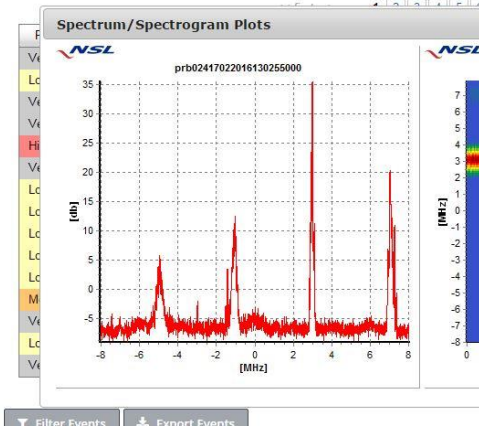
Rückwandlung der Signale mit inverser FFT

Echtzeitverarbeitung > 1,4 GHz




FDAF blanker




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

# Technische Lösung: Adaptive Beamforming
# CRPA - Controlled Reception Pattern Antenna

Mehrere Antennenelemente
empfangen dasselbe Signal

Die Signale kommen an jeder Antenne
zu einem etwas anderen Zeitpunkt an

Die Signale der Antennen werden
aufsummiert

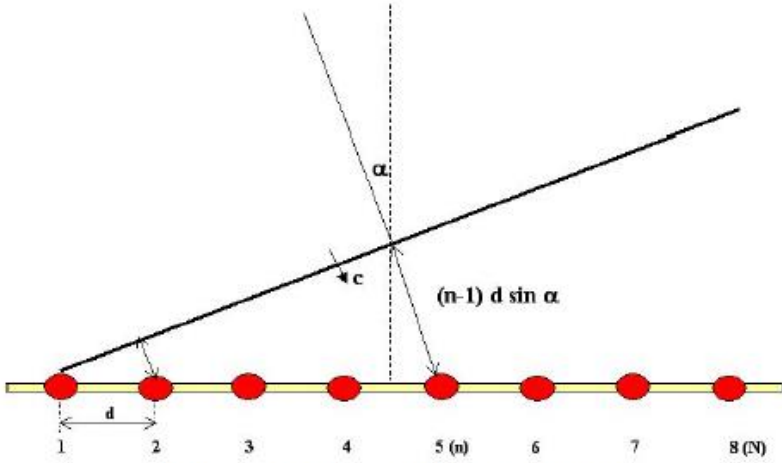
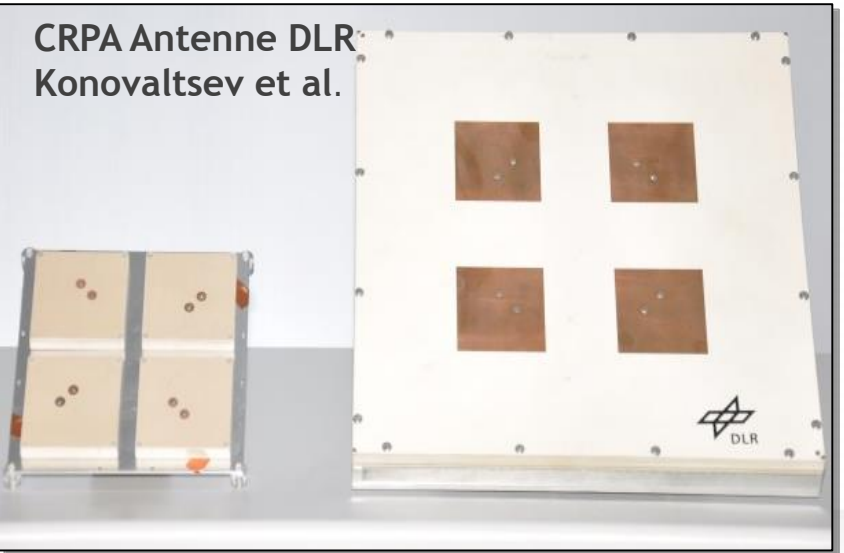
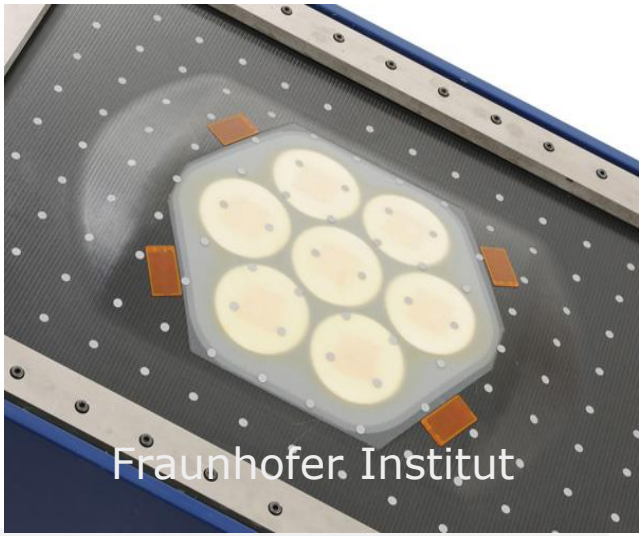


Fig.1.1: Linear equally spaced array




Lange GmbH electronic

# Technische Lösung: Adaptive Beamforming
# CRPA - Controlled Reception Pattern Antenna

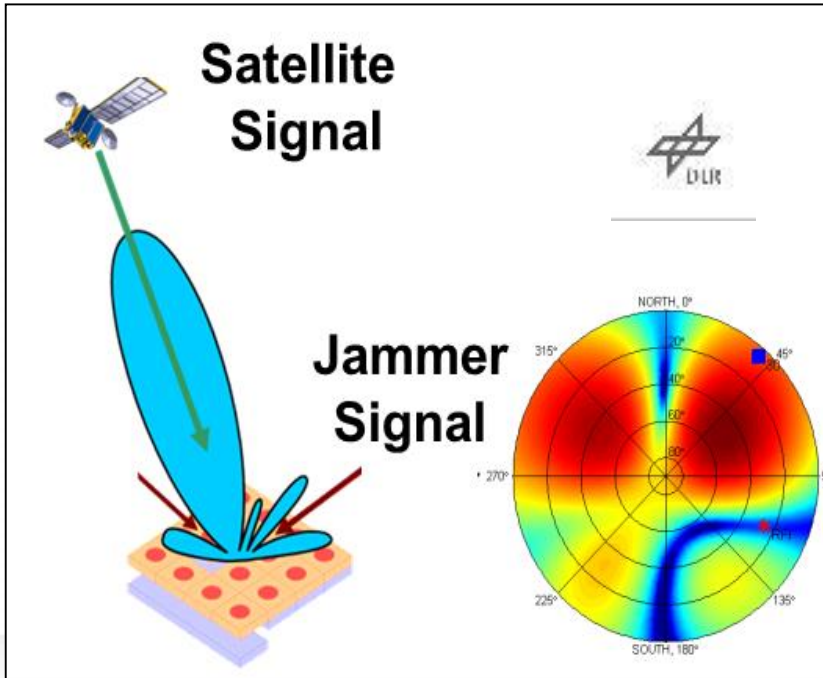
Der Unterschied in den Ankunftszeiten und Phasen wird verwendet um

Signale **konstruktiv** zu addieren

- ➢ größeres Signal ➢ mehr Antennengewinn
- ➢ Erzeugen mehrerer Empfangskeulen, die stark richtungsgebunden sind – Digital Beam Forming DBF

Signale **destruktiv** zu addieren

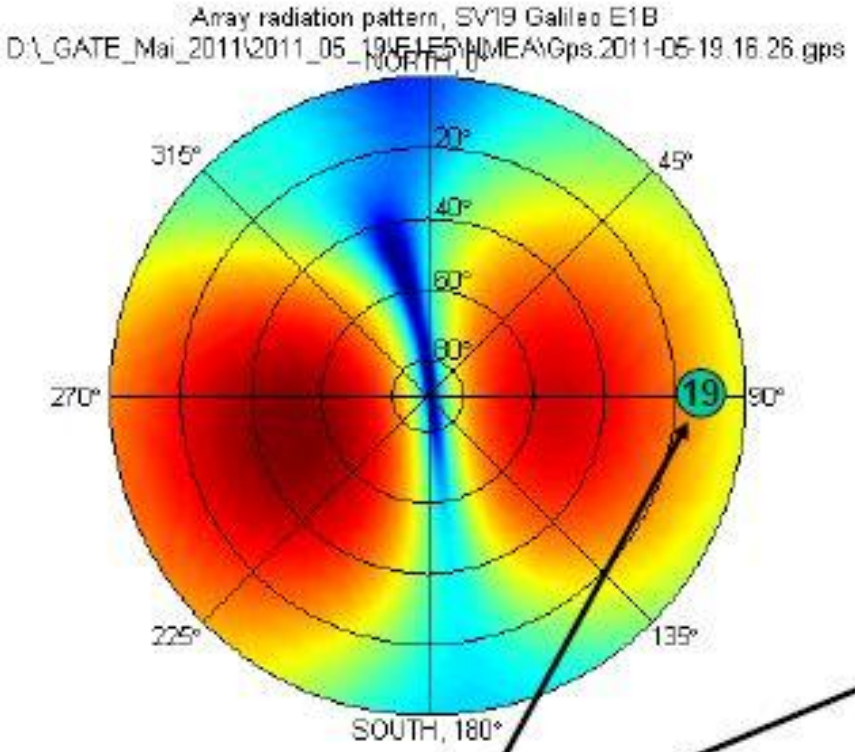
- ➢ kleineres Ausgangssignal = Nullbildung
- ➢ Erzeugen von Nullempfang in Richtung Störer



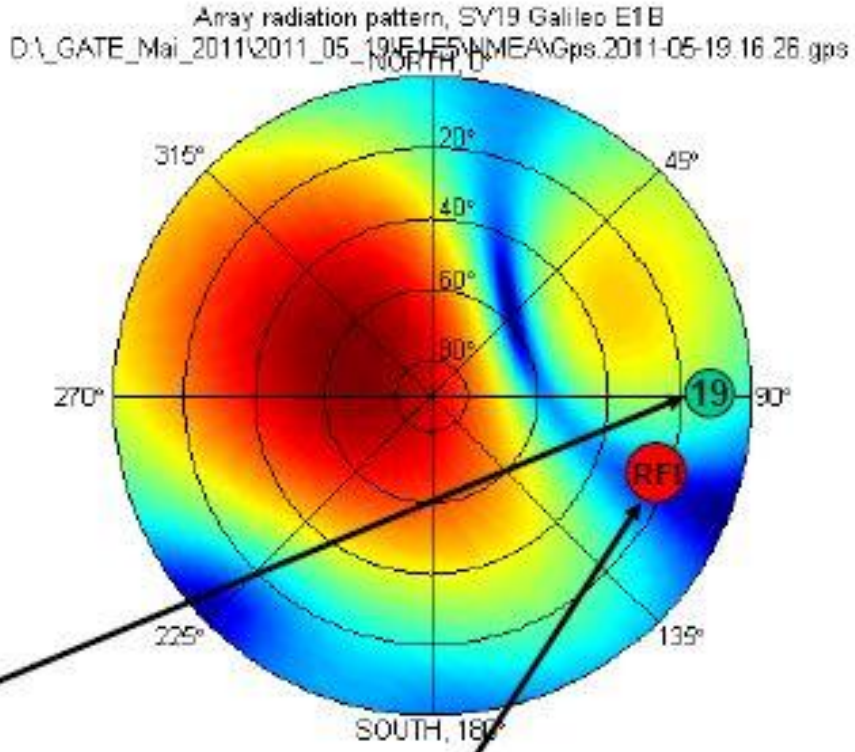
# Ergebnis einer Messung mit **Digital Beamforming DBF**

## DBF Interference Suppression Galileo PRN 19

### No RFI




### RFI




Approx PRN Position

Approx RFI Position

# Technische Lösung: INS Inertialsensoren

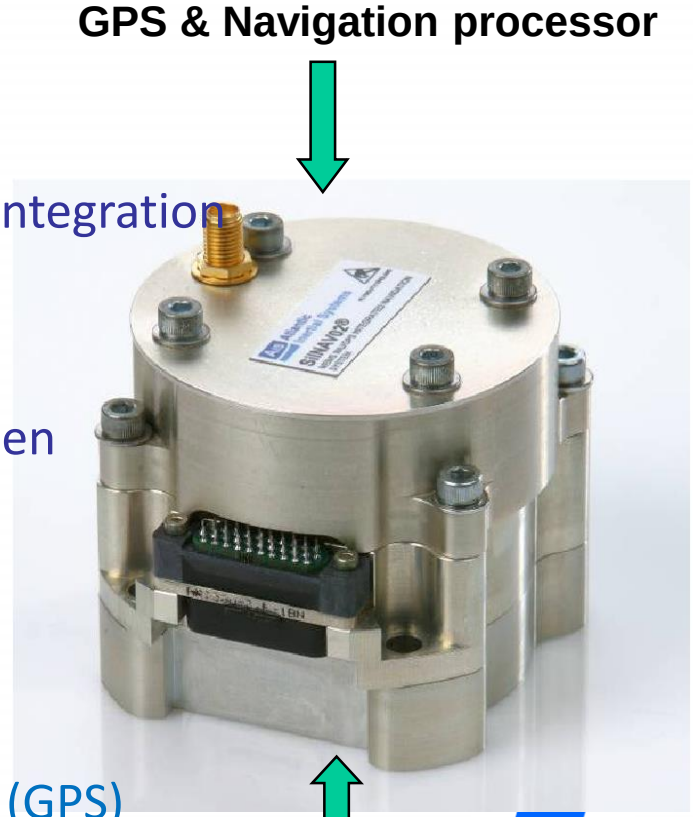
Inertialsysteme bestehen aus mindestens
3 Beschleunigungssensoren und 3 Gyroskopen

Inertialsysteme bieten

- Eine eigene Positionslösung durch mathem. Integration
- Unabhängigkeit von externen Signalen
- Nachteile:
  starke Langzeitdrift, müssen initialisiert werden

GPS/INS kombiniert Vorteile beider Systeme

- geringe kurzzeitige Fehler (Inertial)
- Keine Langzeitdrift und absolute Position (GPS)
- Kontinuierliche Positionslösungen
- Robusteres Navigationssystem
  Möglichkeit des Integritätsmonitoring



# Weitere Technische Lösungen:

- Spezielles AntennenDesign: halbkugelförmige spiralige Antenne

  Uni Illinois in Navigation 2017

- Verwendung besserer HF und ZF Filter,
  zur Unterdrückung von Out of Band Interference

- Lineare Prädiktion:

  prädiziertes Störsignal wird von aktuellem Signal abgezogen

  nur für kontinuierliche Narrow Band Störsignale

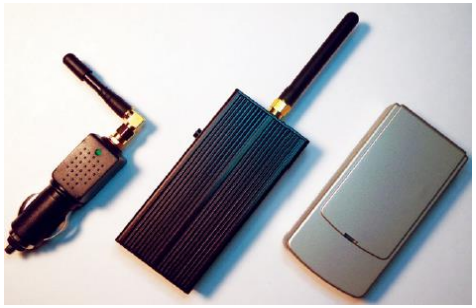
  Quelle: Felix Butsch 2001

- Mechanische Barrieren

# Fazit

Erkennen und Abwehr von GNSS Störereignissen erfordert

- Mechanische Barrieren
- Filterung
- zusätzliche Algorithmen
- zusätzliche Sensoren
- komplexere Antennen



und bedeutet mehr Aufwand

# Empfehlungen

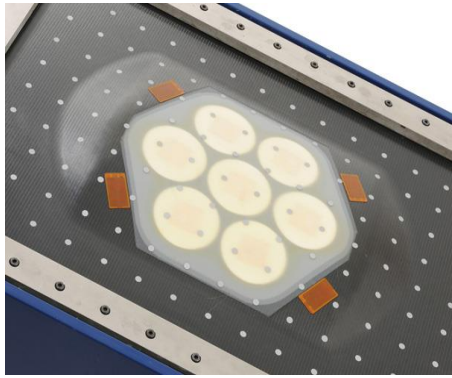
- Aufbau eines Meßnetzes mit kontinuierlichen Messungen
- Erarbeiten eines Katalogs von Maßnahmen für das Finden und Ausschalten von Störquellen


- Öffentliche Warnung an die Benutzer:
  z.B. ähnlich einer Wetterkarte
- Testen von Auswirkungen auf wichtige GNSS Systeme und Gegenmaßnahmen / technische Lösungen
- Bei kritischer Infrastruktur und Safety of Life Anwendungen: Aufrüsten durch geeignete technische Zusatzsysteme

Lange GmbH electronic

# Zusammenfassung

- Jamming kann Ortung und Navigation mit GPS /GNSS massiv beeinträchtigen oder gar ganz ausschalten



Fraunhofer Institut

- Jamming Ereignisse hatten in unseren Messungen deutliche Auswirkungen auf einen hochwertigen GNSS Empfänger:
  - Abfall des Carrier to Noise Ratio
  - Verlust von getrackten Satelliten

- Spoofing und Meaconing kann GPS / GNSS Empfänger gefährlich in die Irre führen

  Bis hin zum Absturz von Flugzeugen

Technische Universität Braunschweig

Institute of Flight Guidance IFF

Lange electronic GmbH

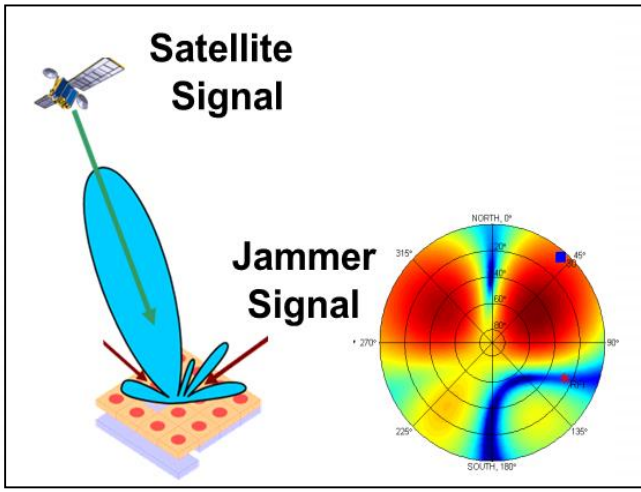
# Zusammenfassung - 2 -

- Es gibt eine Vielzahl an technischen Lösungen:
  Messgeräte, Filterung, Empfängeralgorithmen, Zusatzsysteme
- eine sehr gute ist CRPA *Controlled Reception Pattern Antenna* mithilfe von Antennenarrays: Nullforming und Digital Beam Forming (DLR)
- Eine weitere sehr gute sind Inertialsensoren, mit hoher Kurzzeitstabilität und Unabhängigkeit von äußeren Signalen
- Kontinuierliche, flächendeckende Messungen sind sinnvoll
- In sicherheitsrelevanten Anwendungen braucht man technische Lösungen zum Absichern des GPS/GNSS Empfangs
  - Blockieren oder Herausfiltern der Jammingsignale
  - Zusatz-Systeme: Zusatzsensoren oder Oszillatoren

Institute of Flight Guidance IFF

Lange GmbH electronic

# Dank an




- A. Hornbostel, M. Kuntz und A. Konovaltsev, DLR
- Felix Butsch, Deutsche Flugsicherung
- Mirko Stanisak, TU Braunschweig
- Alexander Rügamer, Fraunhofer iis
- Guy Buesnel, Spirent Communications
- Michael Jones, Roke, UK