



**NAVWAR-Simulation**  
**für robuste GPS/GNSS**  
**Navigations-Systeme**  
**Intelligente Abwehr von Jamming**

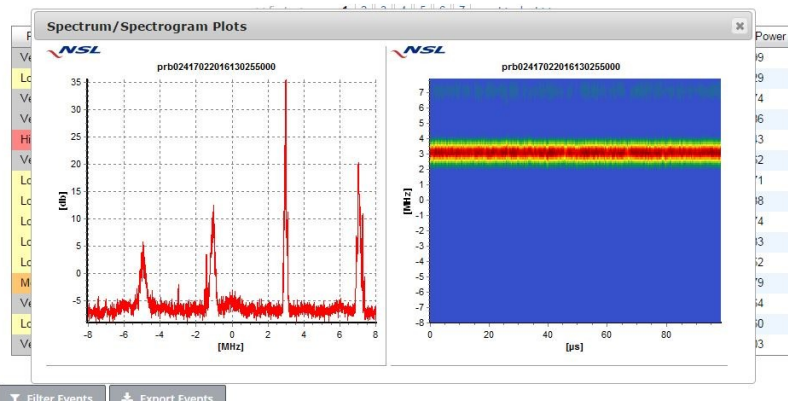
*Karen von Hünerbein*  
*Lange-Electronic GmbH*

# Gliederung

## Technische Lösungen gegen Jamming und Spoofing:



- Mit RF Simulation testen zum Härten  
→ Robusteres PNT (*Positionieren, Navigation, Timing*)
- Intelligentes Vorschaltgerät InVo  
*Herausfiltern der Störsignale*



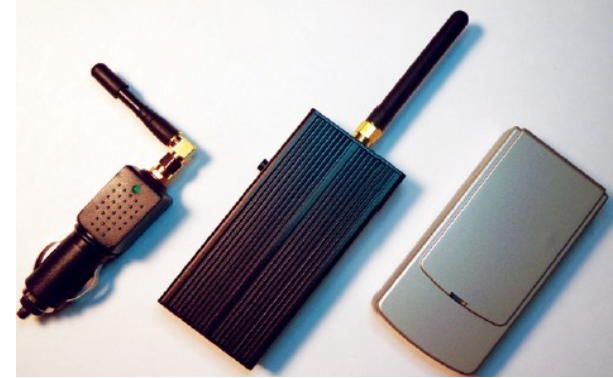
# Jamming - Störsignale

## Versehentliche Interferenz:

Jeder Sender in demselben Frequenzband L1, L2, L5

Defekte Elektronische Geräte,  
die Rauschen senden

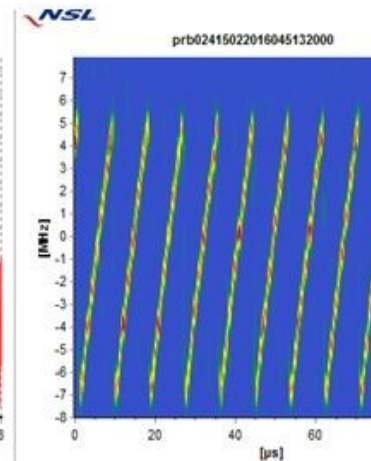
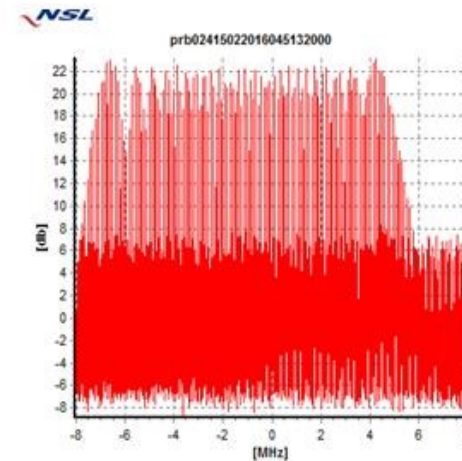
Mehrere Sender gemeinsam können  
stören durch Intermodulationseffekte



## Absichtliches Jamming:

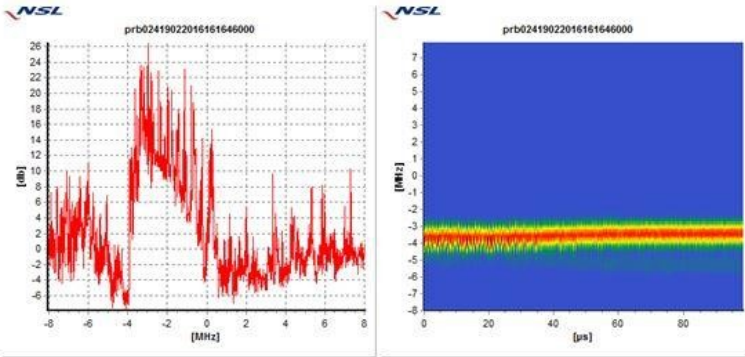
Senden starker L Band Signale  
zum Verhindern von GPS Empfang  
Beispiel: Personal Privacy  
Devices LKW Fahrer

Das führte zu Ausfällen eines Bodenkorrektur-  
Systems am Newark Flughafen vor ca. 12 Jahren  
Jammer auf dem nahegelegenen Highway



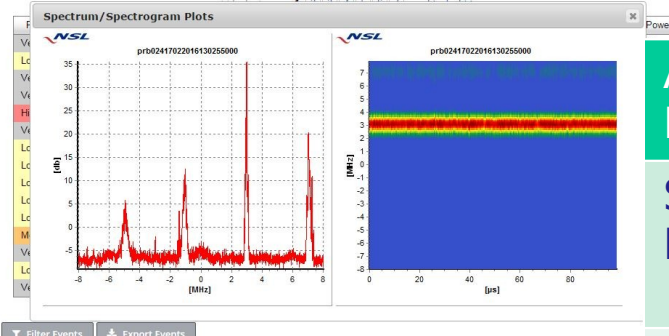
# Beispiele für Jamming 2016 an A2

## Event 2: CDMA interference, rating 8.2307



### DETECTOR Monitoring Centre

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



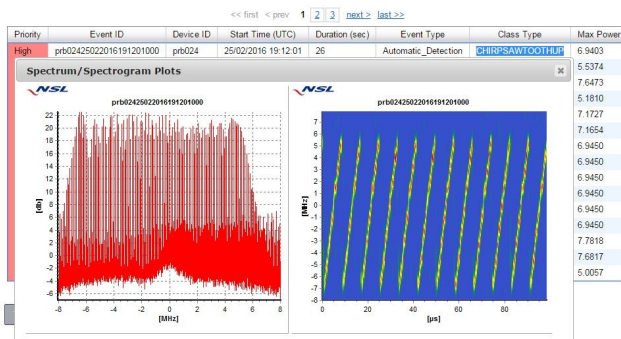
Anzahl Ereignisse	238
Schwächere Interferenz	177
mittelstarke	27
Sehr starke	34

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



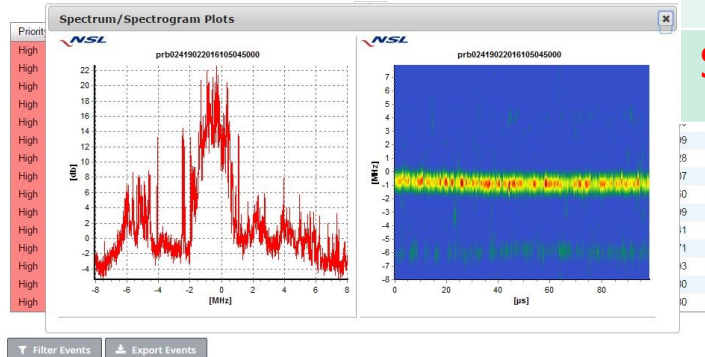
### DETECTOR Monitoring Centre

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



### 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

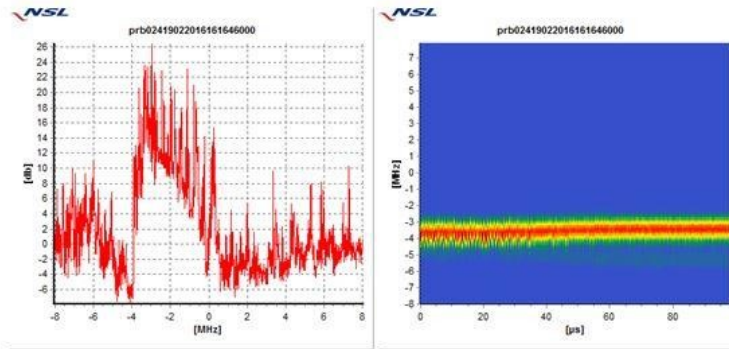
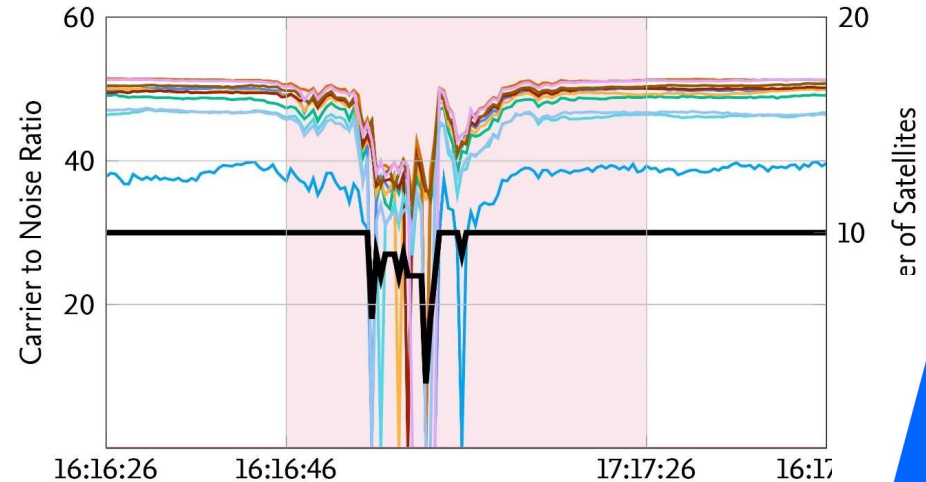


Figure 8: CDMA interference event (Feb. 19 2016, 16:16:46 UTC)

## Empfangene Satellitensignale



# Technische Lösungen



# Test mit GPS Satellitensignalsimulator

Realistische Emulation von

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



 Introducing PNT X

# Testfunktionen



- GNSS Signale: Multi GNSS und Multi Frequenz
- Jamming Signale:  
viele verschiedene Signaltypen
- Spoofing Signale
  - Mehrere Spoofsender
  - Navigationsdatenattacke
  - Meaconing Attacke
  - Timing Error Attacke



# Test und Validierung



- o Identifizieren der Probleme vorab
  - Voll Kontrollierbar und voll wiederholbar
- o mithilfe eines **GPS Satellitensignal Simulators, der realistische RF Signale emuliert**
- o Testen der Empfänger mit 2-3 GNSS-Signalen und Störsignalen:
  - *Hochdynamische Flugobjekte – high speed*
  - *Starke Jammer bis 140 dB Signalstärkebereich*
  - *Abschattung und Mehrwegeeffekte für alle Signale*
  - *Spin Model ultraschnell 2 kHz Update rate*



## Spirent F&E Simulator Architektur

- Erzeugen präziser Wellenfronten
  - Mit hoher Phasenstabilität und geringem Rauschen*
- Ununterbrochener dynamischer Bereich von 140 dB
  - *Repliziert sehr starkes Jamming mit hoher Realitätstreue*
  - *On top: breitbandiges 90 MHz AWGN (weißes Rauschen)*
  - *Matched spectrum*
  - *Benutzerdefinierte Wellenformen passend zur Flugzeugbewegung*
- Fernsteuerkommandos ermöglichen Modifikation von Jammer Parametern on-the-fly in Echtzeit

# NavWAR: Hardware in the Loop mit extrem hoher Dynamik

**Ziel:** Evaluieren des PGK (precision guidance kit) auf rotierender Artillerie mit Hardware-in-the-loop (HIL) in einer GPS-gestörten Umgebung.

Hohe Dynamik **mit 2 kHz** Update Rate  
für Raketen, Raummissionen und Drohnen

HIL Latenzzeit **2 ms**  
bei allen Szenarien und Konfigurationen.

Spin Modell mit bis zu 100 kHz  
für die Winkeldynamik entlang der  
Rotationsachse



# NavWAR: Modernes GPS User Equipment (MGUE)



## Verschlüsselte Signale

Vom **GPS-Directorate-abgesegener MNSA M-Code**, AES M-Code, auf Server liegender SDS M-Code.  
sowie **Galileo PRS** und **CS**

M-Code RMP (Regional Military Protection)  
Militärische Anwender können hier mit dem narrow-beam M-Code Signal testen

## Sicherheit im Design

entspricht den CAT I und CAT II STIGS:  
Security Technical Implementation Guide

# NavWAR: Alternative Ortung und Navigation

## Low Earth Orbit Satelliten

- hochpräzise LEO Orbits
- Benutzerdefinierte alternative Signale

## S Band

- alternative Signale im S-Funkband

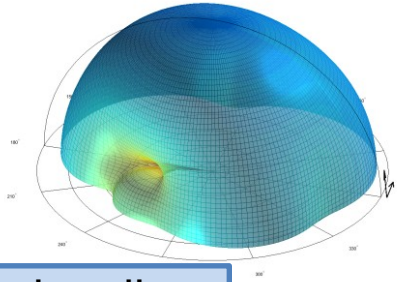
## Inertiale und andere Sensoren

- integrierte und eingebettete GPS/Inertialsysteme



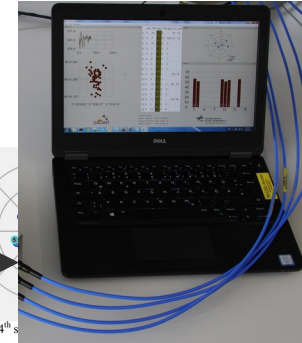
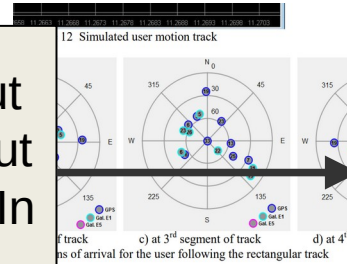


Vorhandenes  
Antennenkabel



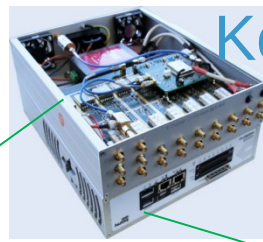
Konventionelle  
L1/L5 GNSS  
Empfänger

Ant-Out  
MMI-Out  
Power-In

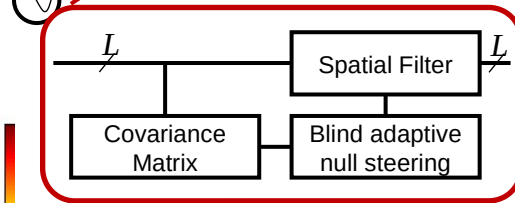
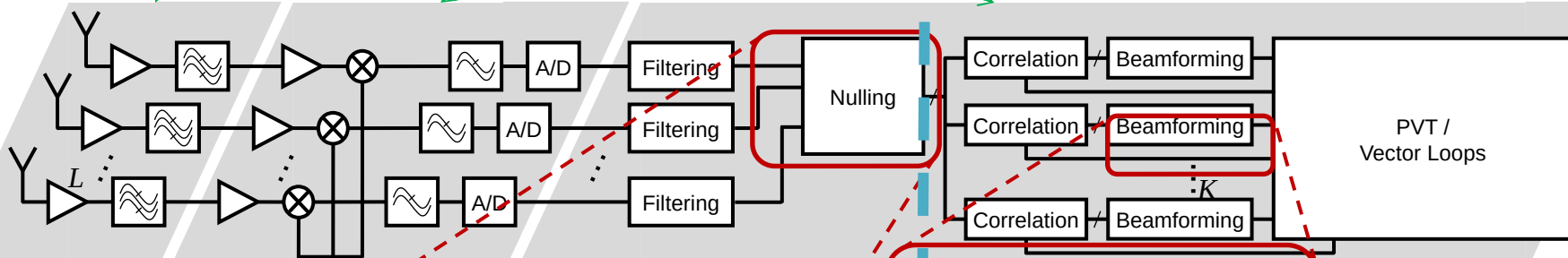


Darstellung von  
Zusatz-  
Informationen

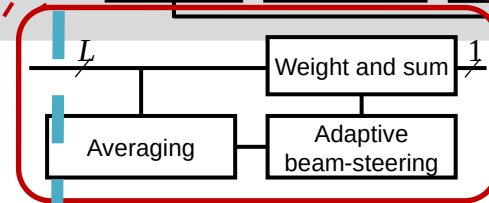
Power-Input



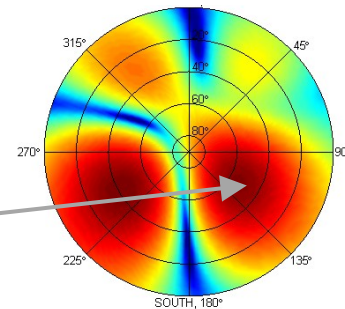
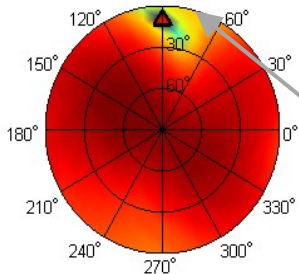
# Korrelatoren



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



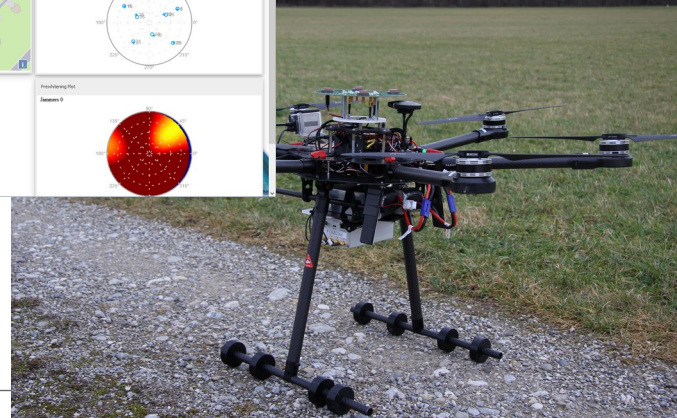
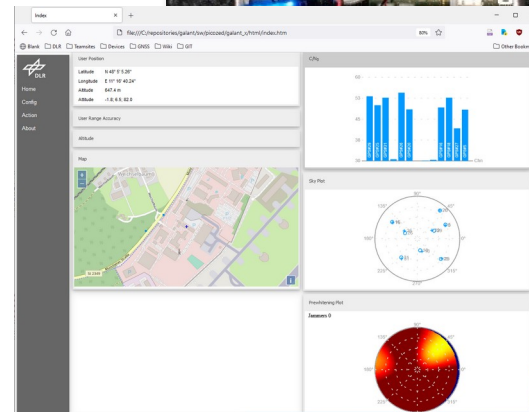
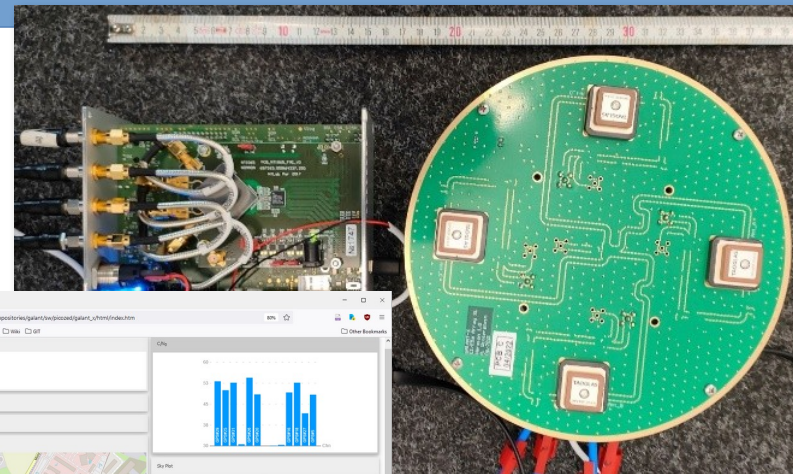
Maximale Verstärkung in Richtung des Satelliten (individuell für jedes Satellitensignal)



# Robuster Navigationsempfänger auf UAS (ROSANNA)



- 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



# Vorteile von Labortests

- Im Labor Schwächen finden bevor im Einsatz etwas schief geht
- Kein Materialverschleiß und Verlust
- Testen bis an die Grenzen und darüber hinaus, *Flug nahe Felswänden – Satellitenausfälle*
- Kontrollierte Bedingungen
- Volle Wiederholbarkeit
- Tests im Labor schneller durchführbar

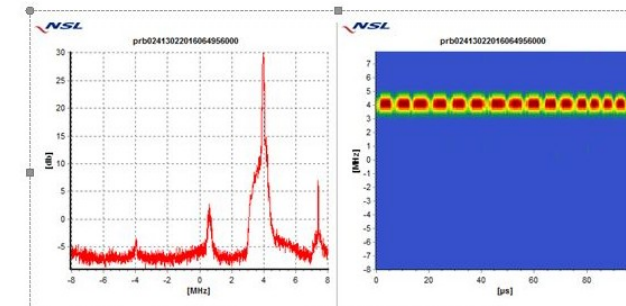


Figure 12: Narrow band interference event (Feb. 13 2016, 06:49:56 UTC)

# Zusammenfassung

- ❖ Jamming und Spoofing stellen eine zunehmende Bedrohung dar
- ❖ Dagegen gibt es technische Maßnahmen u.a.
- ❖ Testen der Empfänger mit GPS/GNSS Signalgenerator
  - ***PNT-X von Spirent***
- ❖ Eliminieren des Jamming Signals durch Null Forming
  - ***Intelligentes Vorschaltgerät von DLR***
- ❖ Ergebnis: Resilientere Empfänger,  
Schutz im Einsatz durch CRPA multi-Elemente Antennen

# Mein Dank geht an



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

