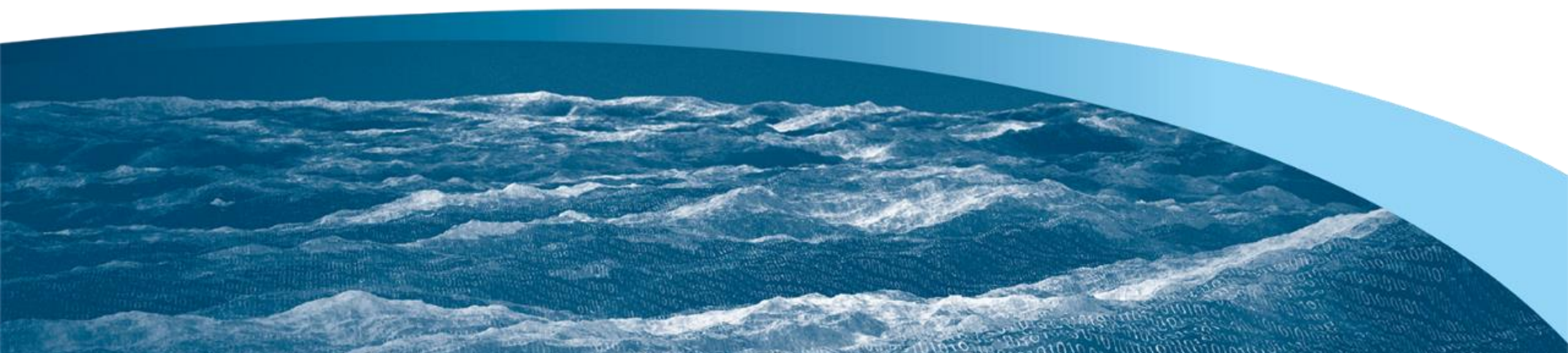


OHB Digital Solutions GmbH
Philipp Berglez, CTO
Graz, 2020-06-16



**Warum wir robuste GNSS-Signale
benötigen?**

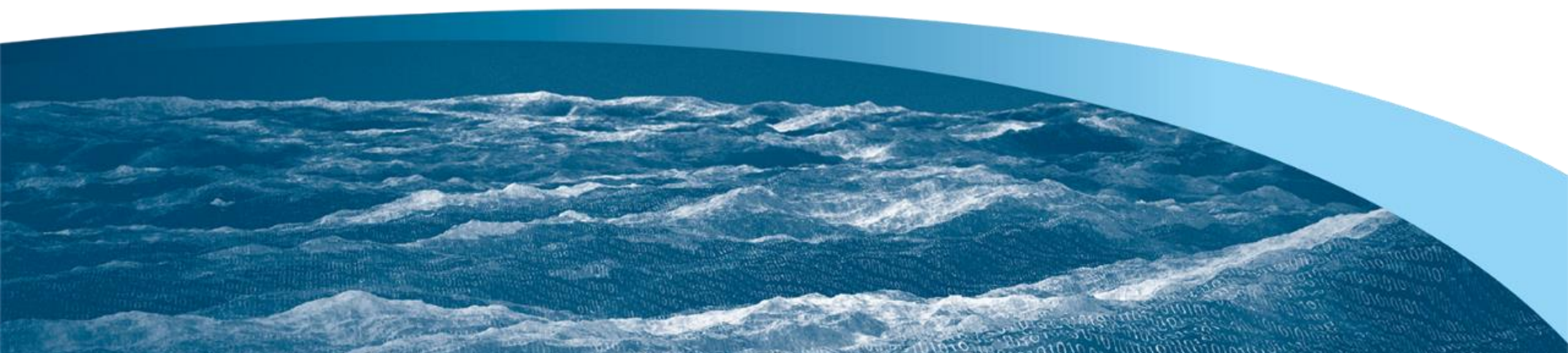
OHB Digital Solutions

- OHB Digital Solutions wurde 1999 als TeleConsult Austria GmbH gegründet
- Präzise und robuste Positionierung, Navigation und Location-based Services
- Seit Dezember 2018 Mitglied der OHB-Unternehmensgruppe



- Unser Arbeitsfelder sind
 - Präzise, robuste und zuverlässige Positionierung und Navigation
 - Entwicklung von Navigations-, Telekommunikations- und Informationstechnologien
- Die Fachgebiete sind
 - GNSS Signalverarbeitung, Algorithmen Entwicklung und Simulation
 - GNSS Interferenzdetektion, -klassifikation, -lokalisierung und Gegenmaßnahmen
 - Hybride Positionierung (GNSS, INS, Wi-Fi, 5G)
 - Kooperative Prozessierungsmethoden
 - Standortbezogene Dienste

OHB Digital Solutions GmbH
Philipp Berglez, CTO
Graz, 2020-06-16



**Warum wir robuste GNSS-Signale
benötigen?**

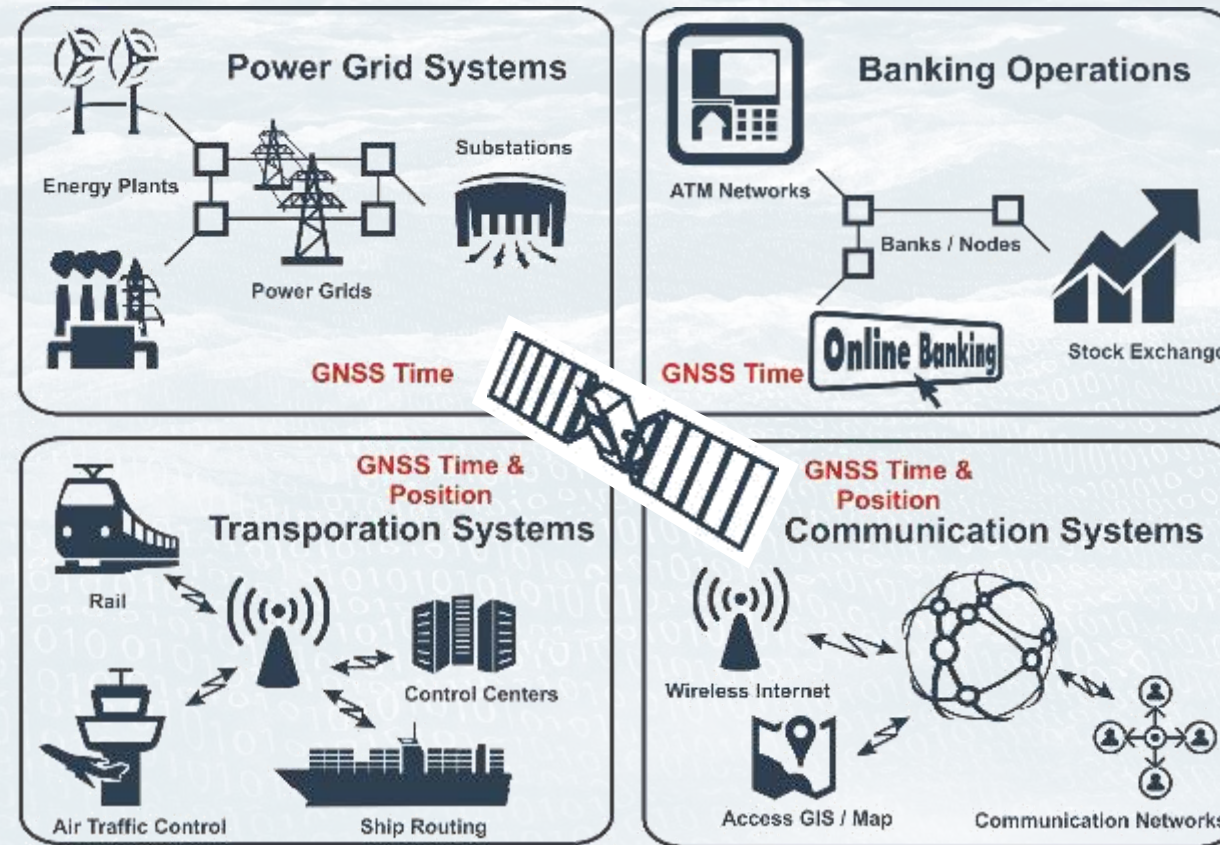
Wir alle sind Navigatoren

- Satellitenbasierte Positions- und Zeitbestimmung, Orientierung und Navigation sind tief in unserem täglichen Leben verwurzelt.
- Marktbericht 2019 der Europäischen GNSS-Agentur
 - 6,5 Milliarden GNSS-Empfänger auf dem Markt
 - 1,7 Milliarden Einheiten wurden 2019 ausgeliefert
 - 2029 9,5 Milliarden
 - ~ 1 GNSS-Empfänger pro Person
- 6-7% des Bruttoinlandsprodukts in westlichen Ländern hängen von Satellitennavigationsdaten ab
 - 800 Mrd. EUR in der EU

Ref.: GSA Market Report 2019

Ref.: European Space Agency 2014

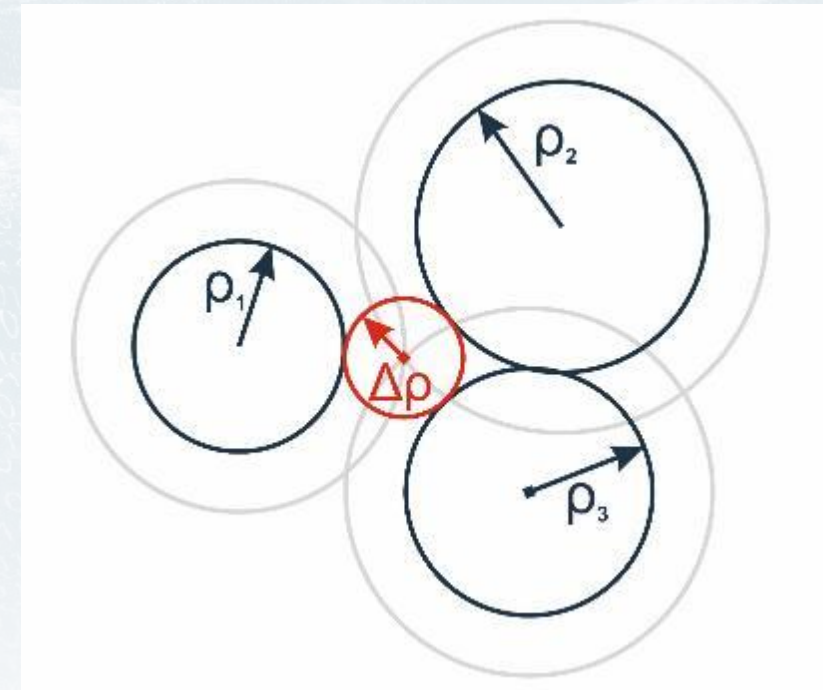
GNSS Anwendungen



Schon kleine Störungen können schwerwiegende Fehler verursachen!

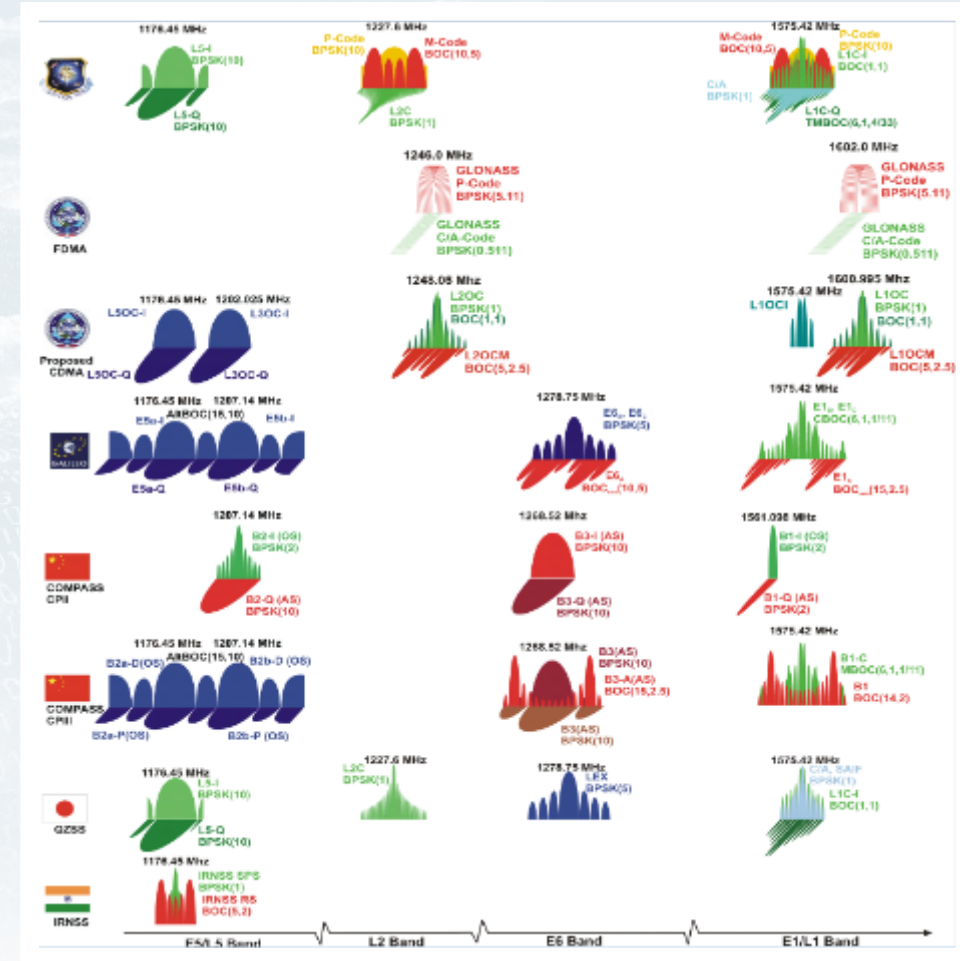
Prinzip der Positionsbestimmung

- Das Prinzip basiert auf Laufzeitmessungen (Entfernungen) zwischen den Satelliten und dem Empfänger
 - Bekannte Satellitenposition (wird vom Satellit übertragen)
 - Schnittpunkt von Kugelflächen
- Nicht synchronisierte Satelliten- und Empfängeruhren
 - Kein Schnitt möglich
 - Pseudoentfernungsmessungen
- Zusätzliche Messung (mindestens 4 Satelliten) erforderlich
 - Koordinaten (X, Y, Z) + Uhrenfehler
→ Position + Zeit



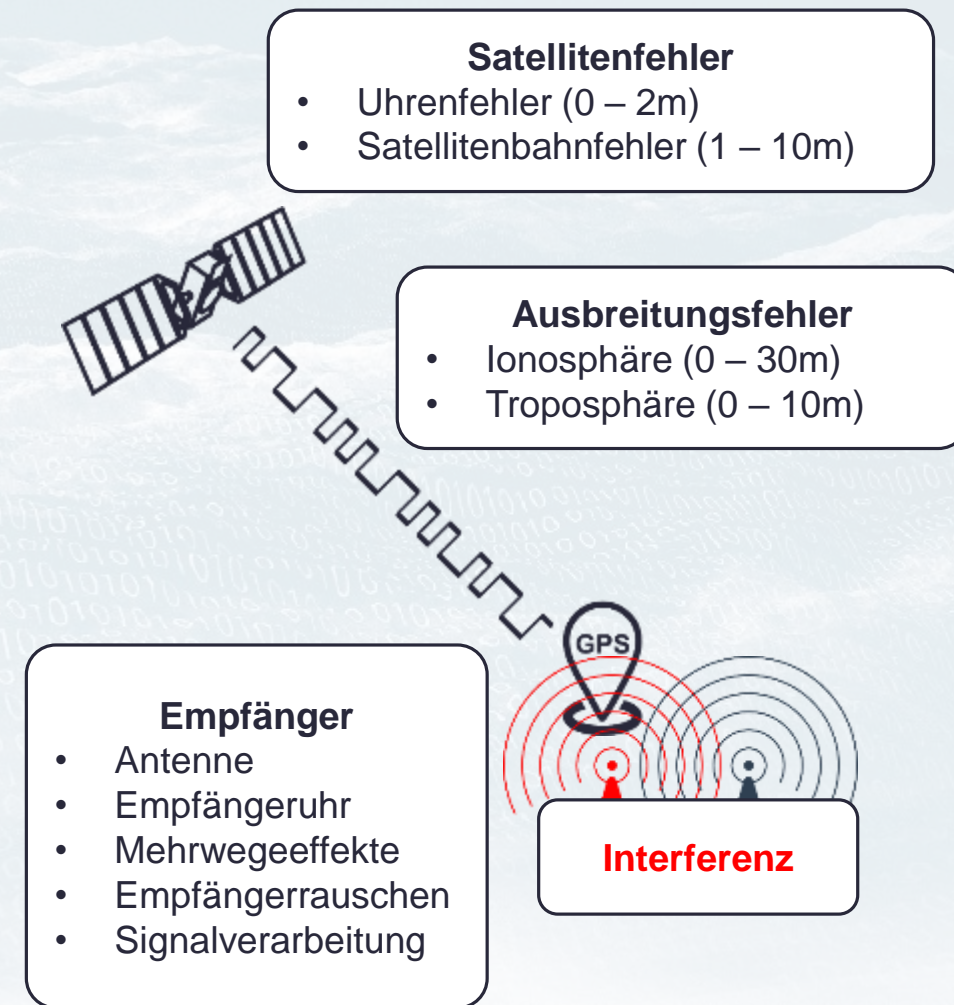
GNSS

- Globale Navigationssatellitensysteme
 - GPS
 - Galileo
 - GLONASS
 - BeiDou
- Augmentierungssysteme
 - SBAS (z.B. EGNOS, WAAS)
 - IRNSS
 - QZSS
 - Etc.
- Derzeit gibt es 4 globale Systeme und mehr als 40 Signale



GNSS Fehlerquellen

- GNSS sind hoch komplexe Systeme
→ zahlreiche mögliche Fehlerquellen
- Die empfangenen GNSS-Signale sind sehr schwach
 - Leistung entspricht einer 30-Watt-Glühbirne in einer Entfernung von 20.000 km
 - GNSS Signalbänder sind von weißem Rauschen dominiert
- GPS Signaldesign stammt aus den 70er/80er Jahren
 - Design der zivilen Signale bekannt
 - Beabsichtigte Interferenz war damals kein Thema



Komplexitätsgründe

- Mehrbenutzersystem
 - Einwegmessungen („nur hören“)
- Echtzeit-3D-Positionierung
 - Gleichzeitige Messungen zu mehreren Satelliten
 - Echtzeitbestimmung der Satellitenpositionen
- Hohe Genauigkeit der Positions-, Geschwindigkeits- und Zeitlösung
 - Verwendung hochfrequenter Signale (z.B. 1.5 GHz)
 - Trägerfrequenz im Mikrowellenbereich (Durchgang durch Atmosphäre)
 - Mehrfrequenzübertragung aufgrund des dispersiven Charakters der Ionosphäre
- Einschränkungen bei der Frequenzzuweisung und Robustheit der Signale
 - ITU-Vorschriften
 - Spread-Spectrum-Signale
 - Begrenzte Signalleistung
- Mischung aus militärischem und zivilem Gebrauch
 - Verwendung mehrere Signale

Sind GNSS Signale robust?



- GPS Messungen im Raum Seetaler Alpe
- 21. September 2016
- Verschlechterung der Positionierungsgenauigkeit
- Totaler Ausfall der Positionsbestimmung → Verlust der Robustheit

Definition von Interferenz

- Unbeabsichtigte Störungen
 - Verursacht durch die Natur, andere Systeme / Signale, Mehrwegeeffekte usw.
 - Bekannt und Gegenmaßnahmen verfügbar
- Beabsichtigte Störungen / Attacken
 - Jamming
 - Aussenden von Störsignalen (Rauschen) und Verdrängung des Nutzsignals
 - Verschlechterte Genauigkeit oder keine Positionsbestimmung, Navigation und Zeitbestimmung (PNT)
 - Spoofing
 - Manipulation, Täuschung, Fälschung von GNSS-Positions-, Geschwindigkeits- und Zeitinformationen
 - Übertragung gefälschter GNSS-ähnlicher Signale mit der Absicht, eine falsche Position / Zeit im Opferempfänger zu erzeugen, ohne den Betrieb zu stören



Ref: www.navigadget.com, www.infostream.biz

GNSS Verwundbarkeit – einige Beispiele

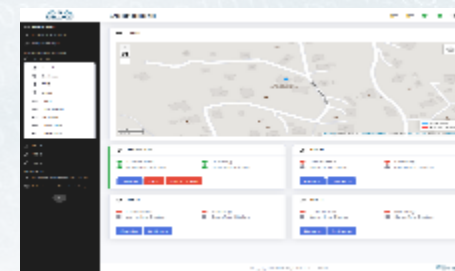
- Störung des GBAS am Newark Airport durch Jammer
- GNSS Störattacke von Nordkorea gegen Südkorea → eLoran
- 117 Zwischenfälle am Flughafen Kaohsiung in Taiwan
- Drohne wurde in USA durch Spoofingattacke (University of Texas) zum Landen gezwungen
- 65m Yacht wurde im Rahmen eines Feldversuchs vom Kurs abgebracht
- Untersuchung der Auswirkung von Störungen des Zeitsignals bei Finanzinstituten
- Ausfall von Notfallpagern, Verkehrsmangementsystemen und Bankomaten in San Diego 2007, verursacht durch US Marine
- Berichte über Spoofing am Schwarzen Meer und in Moskau in 2017

Not just an urban legend

- GNSS Interferenzmonitoring im Raum Graz (2014 - 2018)

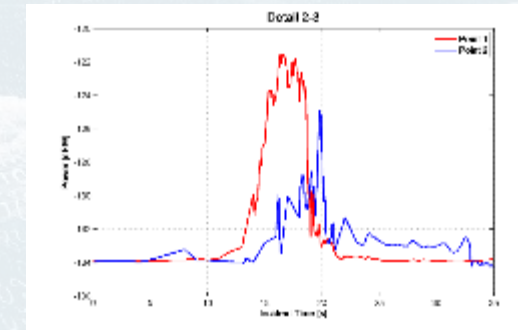
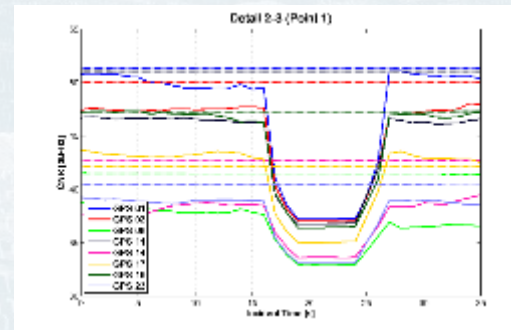
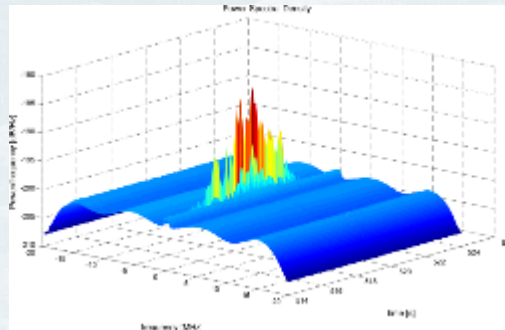


- GNSS Interference Detection and Analysis System (GIDAS) von OHB DS



GNSS Interferenzmonitoring

- Verfügbarkeit von GNSS-Störsendern und damit die Bedrohung nimmt stetig zu
 - Im Jahr 2014 wurde durchschnittlich ein Vorfall pro Stunde festgestellt
 - Im Jahr 2018 wurden durchschnittlich vier Vorfälle pro Stunde festgestellt



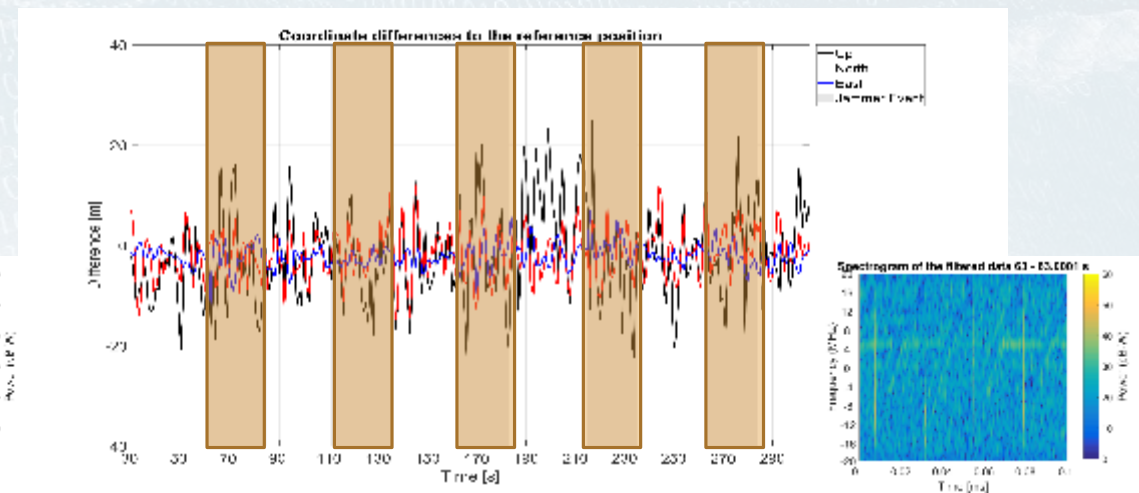
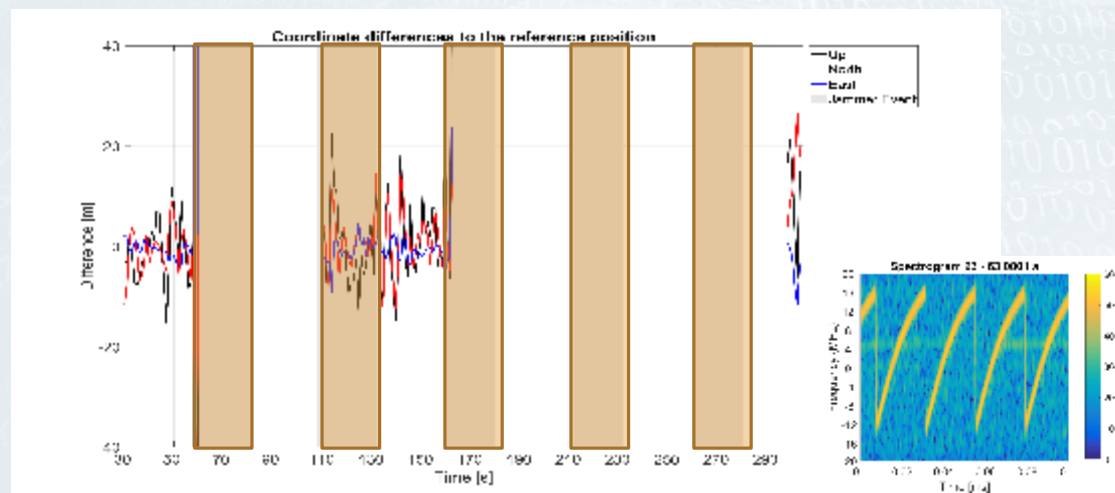
- Motivation für den Einsatz von Störsendern sind Datenschutz, kriminelle Aktivitäten, Schutz kritischer Infrastrukturen usw.
- Die meisten Vorfälle werden durch in Fahrzeugen installierte Störsender verursacht, die zu einer Verschlechterung der GNSS-Genauigkeit oder zu einem vollständigen Verlust des Dienstes führen
- **Der Betrieb von Störsendern jeglicher Art ist in der gesamten EU illegal**

Umgang mit GNSS Störattacken

- Aufmerksamkeit und Bewusstsein
 - **Vertrauen Sie Ihrer GNSS-Position nicht immer!**
- Detektion und Klassifizierung sind Voraussetzung für Gegenmaßnahmen
- Gegenmaßnahmen
 - Signal- und Datenverarbeitung
 - Signaldesign
 - Verwendung robuster Signale / Dienste
 - Authentifizierung
 - Verwendung von Backupsystemen
 - Karten, Inertialsensorik, WLAN, Zellortung, etc.
- Ziel sollte ein umfassendes GNSS Risiko Management sein

Beispiel – Robustheit durch Signalverarbeitung

- Filterung der Störsignale im Frequenzbereich
 - 5 unterschiedliche Störattacken
 - Adaptiver Notch-Filter
- Wird die Signalleistung zu stark sind die Möglichkeiten derzeit limitiert
 - Robustes Signaldesign erforderlich



GNSS Robustheit

- Robustheit ist die Fähigkeit eines Systems, Veränderungen ohne Anpassung seiner anfänglich stabilen Struktur standzuhalten
- Nutzer erwarten
 - Genauigkeit, Verfügbarkeit, Zuverlässigkeit und Robustheit
- GNSS Robustheit gegenüber absichtlichen Störattacken
 - Jamming
 - Erhöhung der Signalleistung
 - Mehrfrequenz GNSS
 - Maßnahmen in der Signalverarbeitung und komplementäre Systeme
 - Spoofing
 - Maßnahmen in der Signalverarbeitung und komplementäre Systeme
 - Verschlüsselung
 - Authentifizierung

Was bietet Galileo?

- Galileo bietet neben dem Open Service zwei "spezielle" Dienste
 - Public Regulated Service (PRS)
 - High Accuracy Service (HAS) mit Signalauthentifizierung
- Public Regulated Service
 - PRS-Signale sind extrem robust gegen Jamming und Spoofing
 - Limitierter Zugang für staatliche Nutzergruppen
 - Österreichische Competent PRS Authority (CPA)
- Signalauthentifizierung
 - Wird ein Teil von Open Service sein
 - Fortgeschrittene Authentifizierung durch HAS-Signale

Zusammenfassung

- Satellitengestützte Positions- und Zeitbestimmung, Orientierung und Navigation sind tief in unserem täglichen Leben verankert
- Nutzer erwarten Genauigkeit, Verfügbarkeit, Zuverlässigkeit und Robustheit
- Absichtliche Störungen der GNSS Signale stellen eine große Gefahr für die Anwender dar
- GNSS Robustheit gegenüber absichtlichen Störattacken ist derzeit ein „Hot Topic“
- Detektion, Klassifikation und Lokalisierung ermöglichen den Einsatz von Gegenmaßnahmen
- Ziel sollte ein umfassendes GNSS Risiko Management sein

Be aware, know the risk, monitor your GNSS information and be prepared!



Ref.: <http://wednesdaywilsondowunder.blogspot.com>

We are the Navigation Experts

Dr. Philipp Berglez
CTO

OHB Digital Solutions GmbH

Rettenbacher Straße 22

8044 Graz, Austria

Mail: philipp.berglez@ohb-digital.at

Tel: +43-316-890971-14

GNSS im Vergleich

	GPS	Galileo	GLONASS	BeiDou
Betreiber	USA	Europa	Russland	China
Nominelle Anzahl Satelliten	24+3 MEO	30 MEO	24 MEO	27 MEO, 5 GEO, 3 IGSO
Bahnebenen	6	3	3	6
Flughöhe	20.200 km	19.100 km	23.616 km	21.550 km
Inklination	55°	64.8°	56°	55°
Umlaufzeit	11h 58m	14h 04min	11h 15min	12h 38min
Ground Track Repeat	~ 1 Tag	~ 10 Tage	~ 8 Tage	~ 9 Tage
Globale Genauigkeit ziviles Signal (95%)	5 – 10 m	4 – 8 m	~ 10 m	< 10 m

Ref.: Navipedia <http://gssc.esa.int/navipedia/index.php>