Dedicated to innovation in aerospace

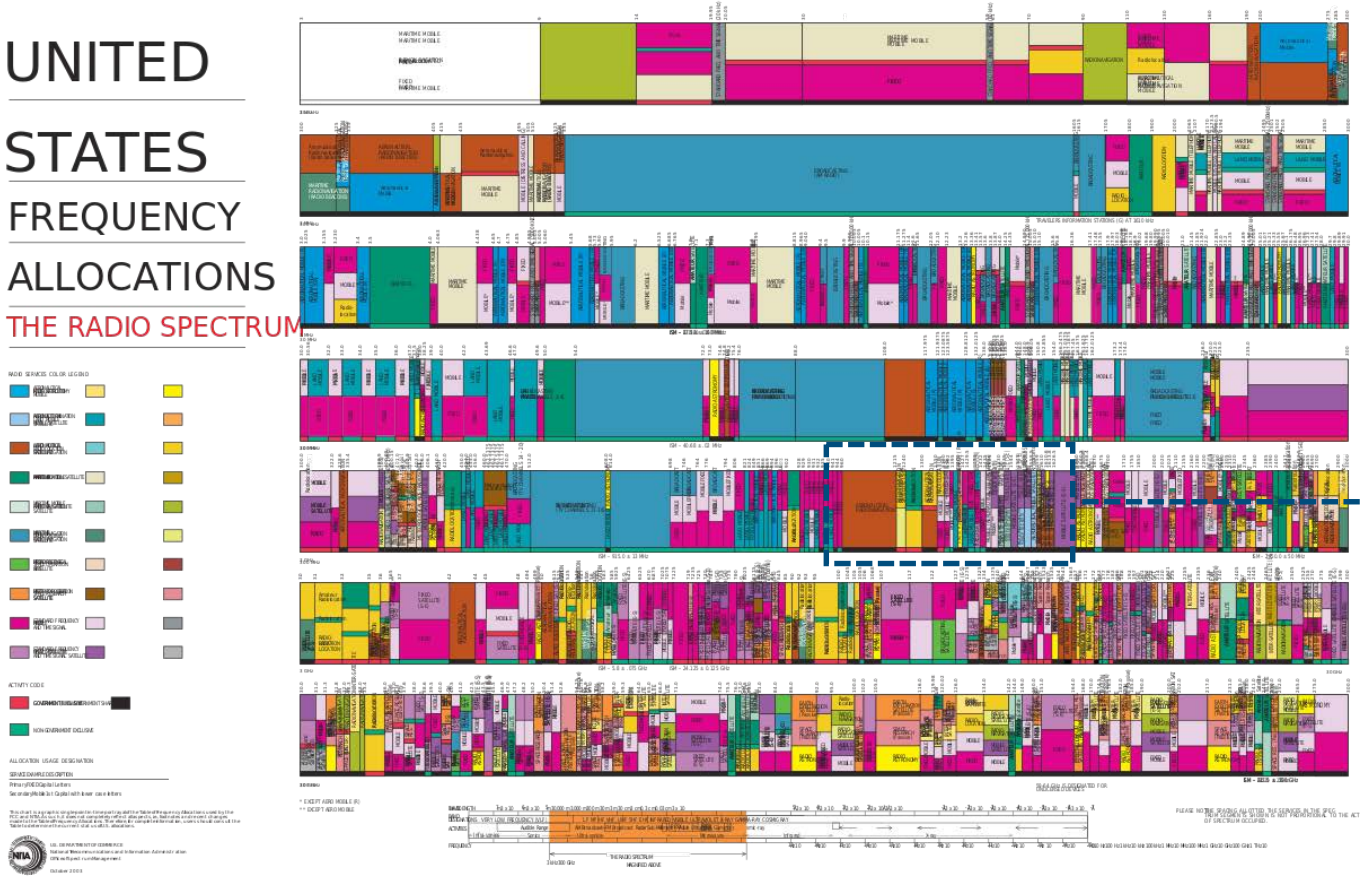
Introduction GNSS RF interference

Jan-Joris van Es (NLR)

January 2018

Contents

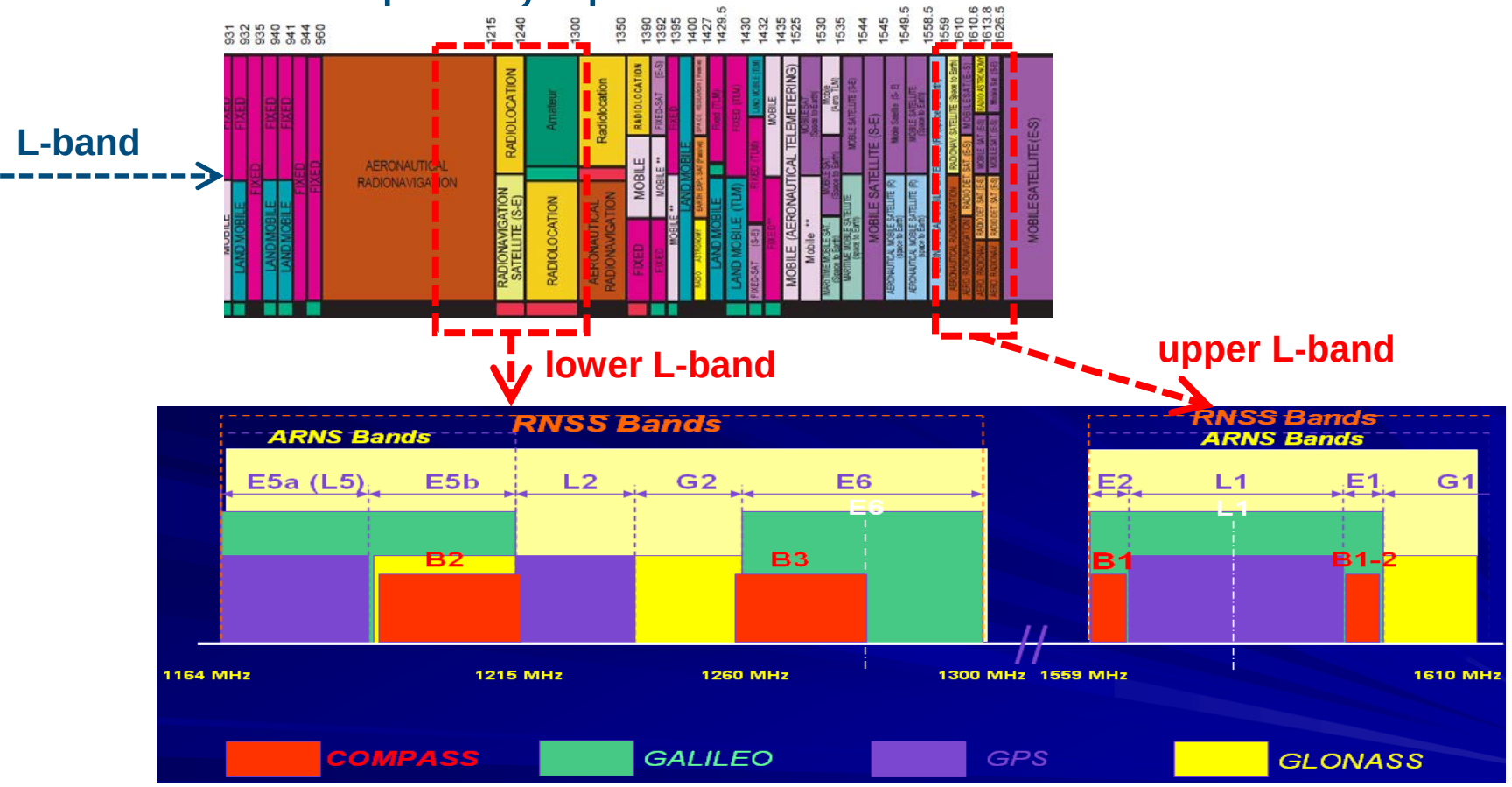
RF frequency spectrum



L-band

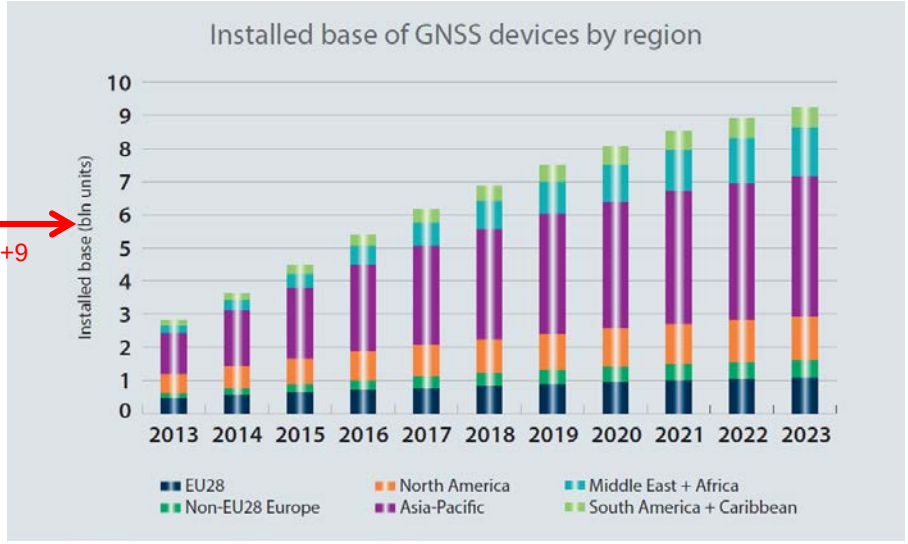
https://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf

GNSS frequency spectrum



Growing dependence on GNSS

- **government agencies**: directing emergency services
- **farming**: automated, GNSS-based planting, watering
- **logistics and transportation**: fleet management, Just-In-Time management
- **container ports**: automated cranes
- **maritime industry**: ship navigation, basis for Automatic Identification System (AIS)
- **mobile networks**: precise timing for successful signal hand over
- **commercial aviation**: GNSS-assisted landing, 4D trajectory management
- **banks and financial institutions**: precision timestamping of transactions
- **building and construction**: surveying, guiding construction machinery
- ....



10^{+9}

Source: GSA GNSS Market Report 2015 Issue 4_0, March 2015

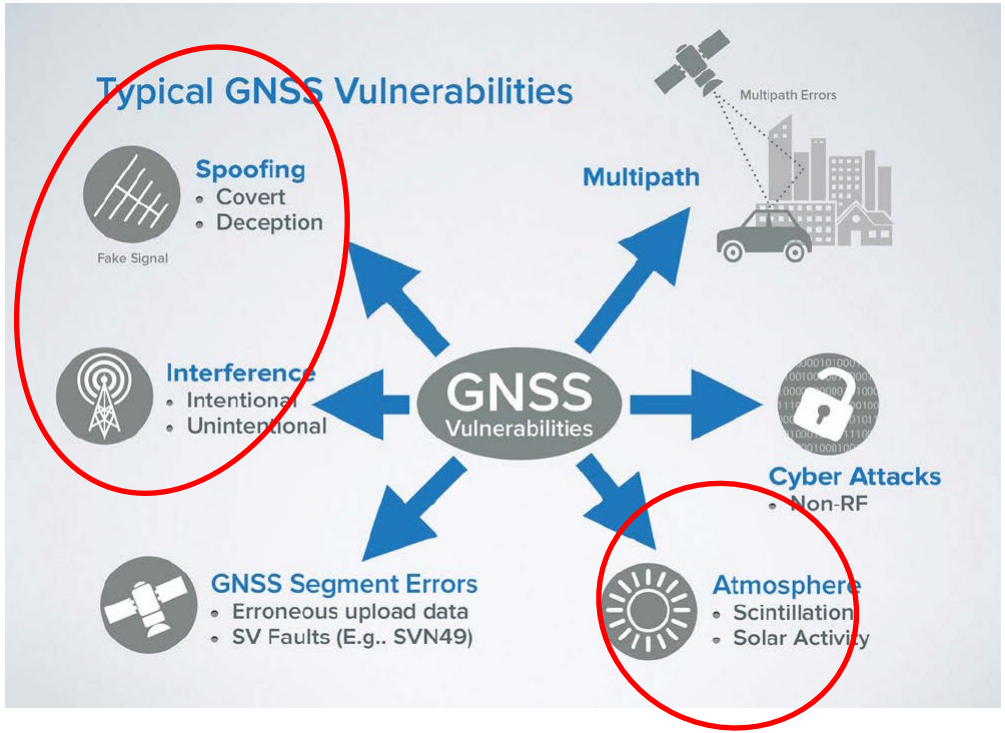
Fundaments of GPS Threats, Spirent, white paper

Electromagnetic interference - definition

Electromagnetic interference (EMI) , also called **radio-frequency interference (RFI),** is the effect of **unwanted energy** due to one or a combination of emissions, radiations, or inductions upon reception **in a radio-communication system**, manifested by any **performance degradation**, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy.

(ITU Radio Regulations, Section IV. Radio Stations and Systems – Article 1.166)

GNSS vulnerabilities



RF interference classification

- natural
- man-made
  - un-intentional
  - intentional
    - jamming
    - spoofing

Fundaments of GPS Threats, Spirent, white paper

GNSS vs interferer signal strength

The **GNSS signals are very weak** (-132 dBW/m^2) by the time that user equipment receives and processes them, they are especially vulnerable to RFI. Signals that overlap GNSS frequencies are likely to come from transmitters much closer than the satellites and, consequently, can easily overpower GNSS signals and render them unusable.

	GNSS satellite	typical jammer
RF power	+20 dBW (100 W)	-20 dBW (0.01 W)
distance	20.000 km	0.1 km
Received RF power	-160 dBW ⟷	-95 dBW

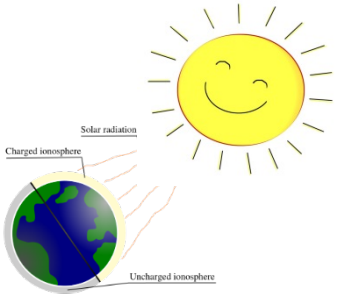
The received interference signal is much stronger than GNSS signal!

RF interference in GNSS bands

Galileo, GLONASS
EGNOS, Compass, ...

GPS

non-GNSS satellites



solar radio bursts
ionospheric scintillation

radar

DME

TV broadcast

Radio amateur

self-interference

GPS receiver

jammer

spoofer

An introduction to interference in the GNSS-bands, J Samson, ENC2014

Sources of interference to GNSS

Source	Frequency (MHz)	Effects on GNSS
other GNSSs	L1, E5, ...	in-band interference
Radio Navigation on Earth	1215-1240	in-band; GPS L2
Exploration Satellites & Radar		Galileo E5b (1215 MHz)
Aeronautical Radio Navigation Services; DME, TACAN, Link 16	960-1164 1164-1215	in band; GPS L5 & Galileo E5A at 1176 MHz
Harmonics of VHF Comm for ATC (Air Traffic Control)	118-137.5 MHz	12th and 13th harmonics at GPS L1
UHF TV	782-788 MHz	2nd and 3rd harmonics in GPS L1
amateur radio	220-225 MHz	7th harmonic in GPS L1
jamming	all GNSS bands	receiver tracking loop loses lock from high power signal
spoofing	all GNSS bands	deception by false signals
WB – impulse radar	L band >25% bandwidth	in-band interference from high power pulses
personal privacy devices	swept frequency car jammers, GPS L1 and Galileo E5	effective at a range of 1 km to 8 km depending on power of jammer

GPS/GNSS antennas, RAO et al., Artech House, Boston, 2013

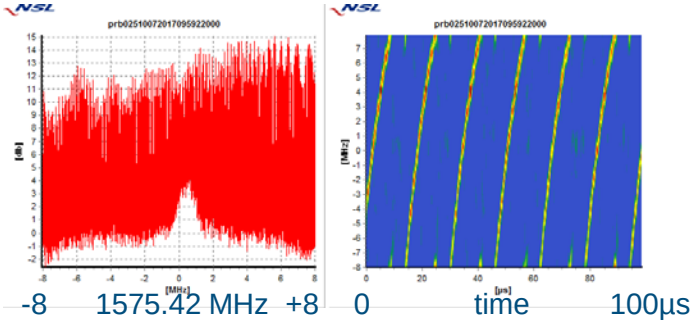
Types of RF Interference and Typical Sources

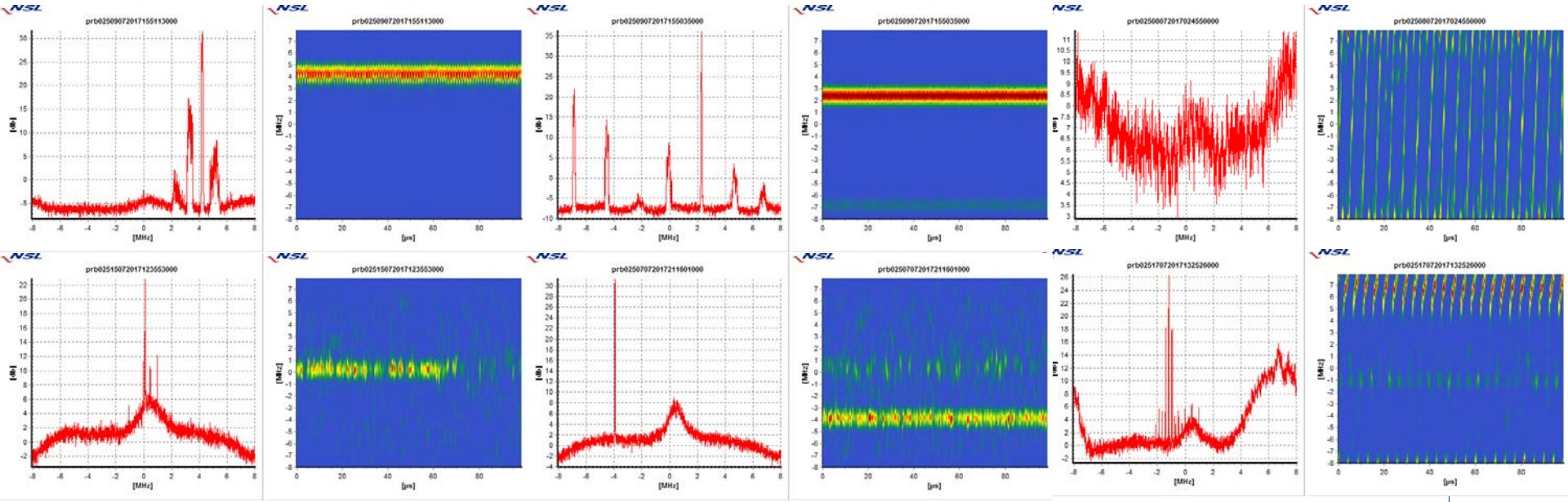
Type	Typical Sources
Wideband-Gaussian	• Intentional noise jammers
Wideband phase/frequency modulation	• Television transmitter's harmonics • Near-band microwave link transmitters overcoming front-end filter of GNSS receiver
Wideband-spread spectrum	• Intentional spread spectrum jammers • Near-field of speudolites
Wideband-pulse	• Radar transmitters
Narrowband phase/frequency modulation	• AM stations transmitter's harmonics • CB transmitter's harmonics
Narrowband-swept continuous wave	• Intentional CW jammers • FM stations transmitter's harmonics
Narrowband-continous wave	• Intentional CW jammers • Near-band unmodulated transmitter's carriers

Understanding GPS principles and applications, E. D. Kaplan, Artech House, Boston, 1996

Types of RF Interference in L1 band

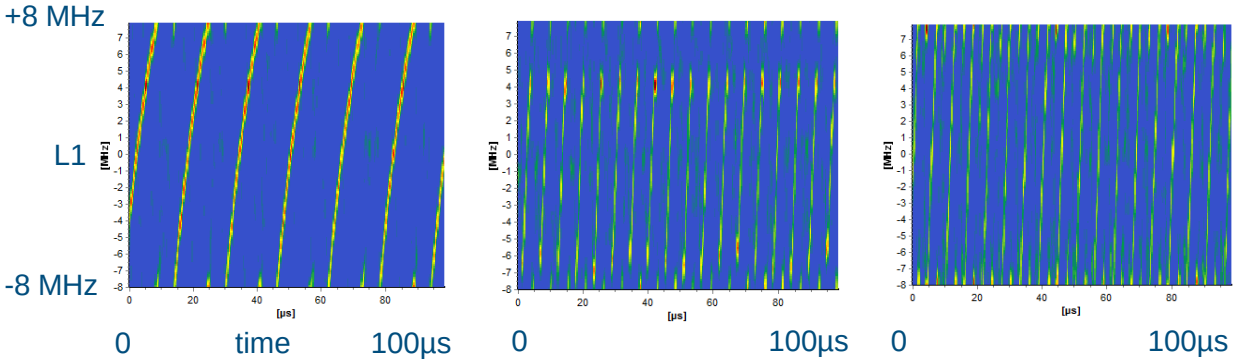
- Interference detected at NLR Amsterdam office (close to A10 ringroad)
- NSL Detector probe





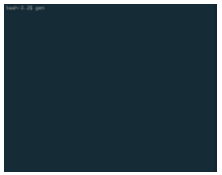
Personal Privacy Devices (PPD)

- Used by people to **avoid being tracked** or monitored by GNSS in their vehicles.
- **Low cost**, small, light-weight
- **Illegal**, but easy to obtain
- 100m to 8 km range, depending on power
- only L1/E1 or multi-band (incl. GSM)
- typical chirp (**swept CW**) signal



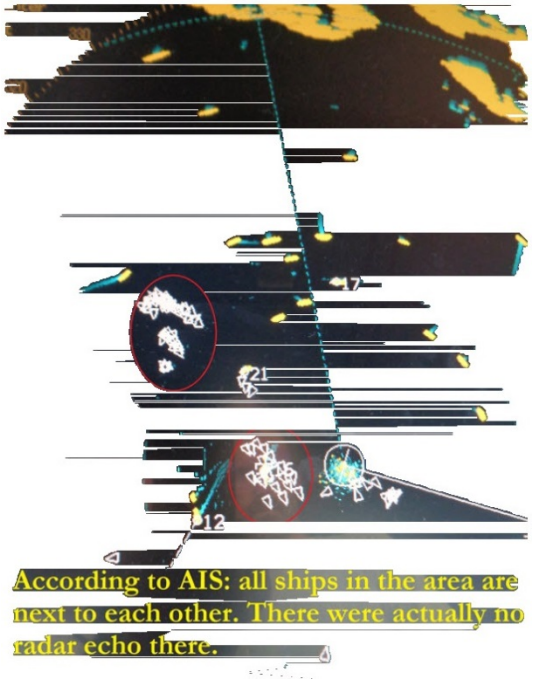
Spoofing

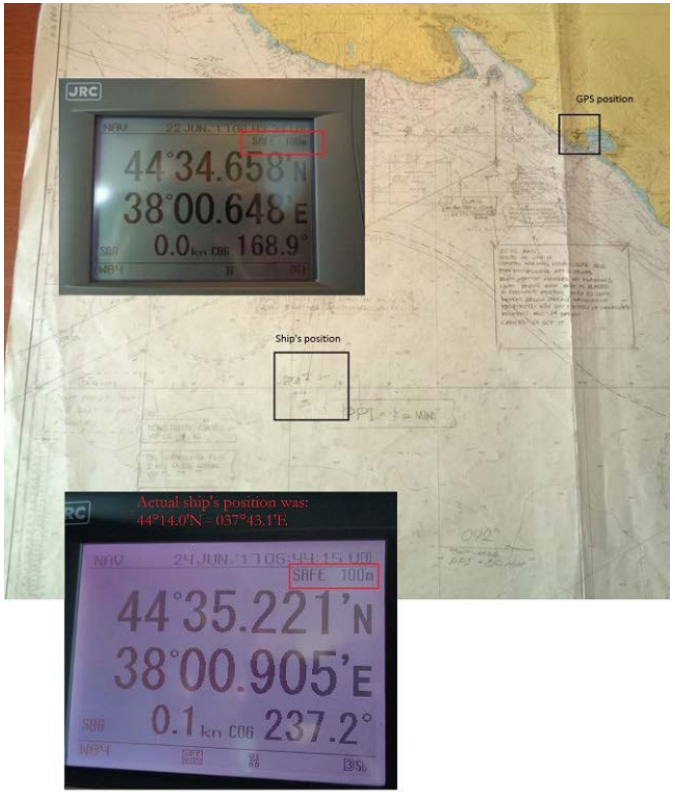
- **Misleading of GNSS receivers with artificial GNSS signals**
  - using GNSS signal generator
  - by recording and replaying GNSS signals (=meaconing)
- **Several GPS spoofing events reported**
  - capture of a Lockheed RQ-170 in Iran (Dec. 2011)
  - “proof-of-concept” attack on luxury yacht “White Rose” June 2013)
  - ~20 ships in the Black Sea report an incorrect position, placing them at a nearby airfield (June 2017)
- **More and more accessible**
  - cheap hardware and software available



Black Sea incident (1/2)

AIS and JRC GPS Display during incident

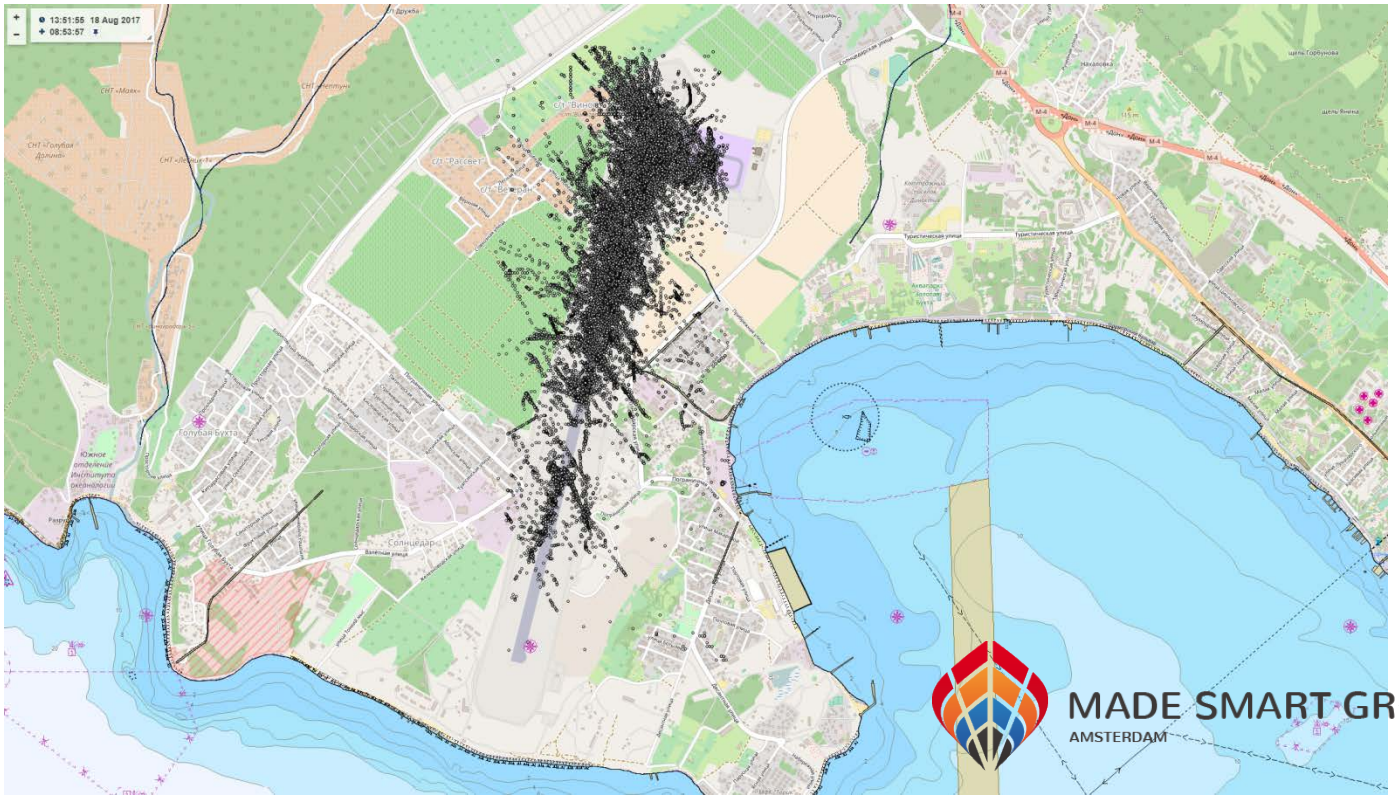




http://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea

Black Sea incident (2/2)

Overzicht alle scheepsposities van Juli - Augustus 2017



Interference mitigation (1/2)

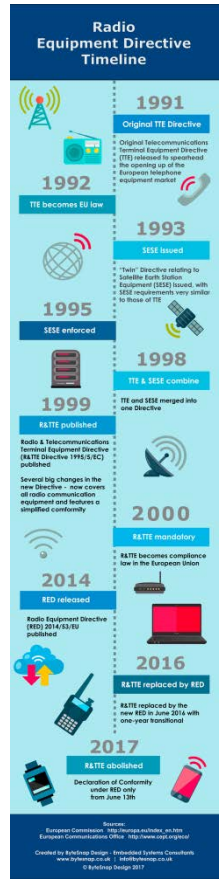
- **Interference reporting** (using sensor network)
  - input for authorities to take action
- **Multi-constellation**, **Multi-frequency**
  - for unintentional interference only
- Local **shielding** of antenna
  - for sensor stations only
- Integration with **other sensors** (e.g. wheel sensors, etc.)
  - for short outages only

Interference mitigation (2/2)

- **Phase Array** antenna
  - strong suppression of interference, but complex and large
- Make receiver more **robust**
  - mitigation in **time domain** (pulse blanking)
  - mitigation in **frequency domain** (e.g. notch-filter)
  - mitigation in **time-frequency domain** (signal processing)
- Use **backup system**

Radio Equipment Directive (RED) 2014/53/EU

- **Replaced** Radio & Telecommunication Terminal Equipment Directive (**RTTED**) 1999/5/EC
- RED to be applied from **13 June 2016** (+1 year transition period)
- Applies to equipment which intentionally **transmits or receives radio waves** for communications or radiodetermination, regardless of primary function
- Some requirements (article 3):
  - protection of health and **safety** of persons and domestic animals
  - provision for universal chargers to address wastage
  - adequate level of **electromagnetic compatibilty**
  - **efficient use** of the **radio spectrum** (ETSI EN 303-413)
  - incorporation of safeguards to **protect personal data and privacy**
  - ...

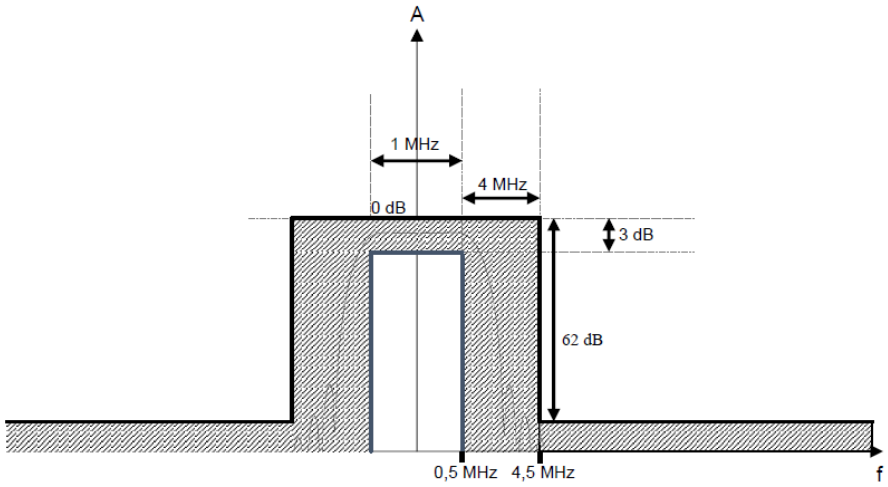


http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0053&from=EN

ETSI EN 303 413

What does the standard include?

- Adjacent Band Compatibility (ABC) testing
- Spurious emissions test



ETSI EN 303 413
figure B-1: Adjacent frequency signal

Conclusions

- We rely more and more on GNSS
- GNSS are weak making them vulnerable to interference
- Risk of interference is increasing
  - the RF spectrum is getting more crowded
  - cheap jammers are available
  - spoofing getting accessible
- Mitigation
  - several options for mitigation

Dedicated to innovation in aerospace

Bijzonder betrokken

Nederlands Lucht- en Ruimtevaartcentrum

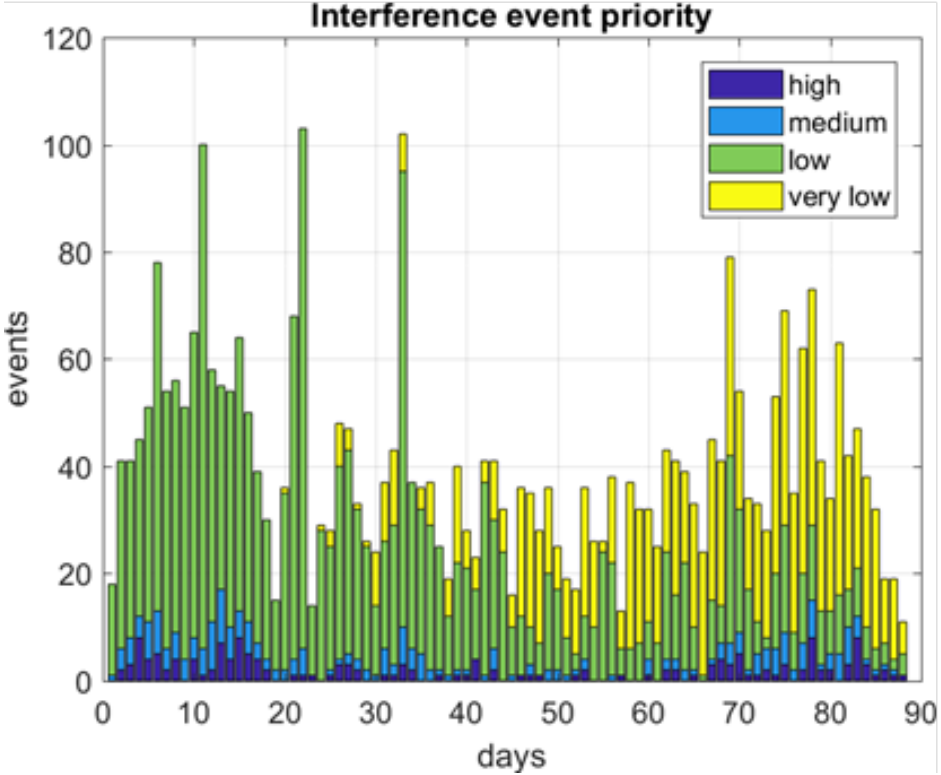
NLR Amsterdam
Anthony Fokkerweg 2
1059 CM Amsterdam

t) +31 88 511 31 13 f) +31 88 511 32 10
e) info@nlr.nl i) www.nlr.nl

NLR Marknesse
Voorsterweg 31
8316 PR Marknesse

t) +31 88 511 44 44 f) +31 88 511 42 10
e) info@nlr.nl i) www.nlr.nl

Number of interferers at NLR Amsterdam office



high priority:

high power, swept CW signal

low priority:

low power