



GNSS Monitoring for Critical Applications (GMCA) - Overview

John Wilde
Vice President Commercial

A  Company



Project Overview

- Objective is to provide monitoring capability to allow for Galileo to be relied upon to the same extent as GPS for all user communities
- Additionally underpins stability and reliability offered by GNSS by detecting and modelling sources of interference to allow for the alerting and potential mitigation

Project Overview

- Activity is being conducted by a consortium under the supervision of the European Global Navigation Satellite Systems (GNSS) Agency (GSA)
- GNSS Monitoring for Critical Applications (GMCA) is a GSA project under the Horizon 2020 Programme (H2020)
- H2020 is an initiative to provide funding for satellite applications

The GSA

- Predecessor was the GALILEO Joint Undertaking (GJU) created in 2002 by the European Community and the European Space Agency to manage the development phase of the GALILEO Programme
- GSA officially took over all tasks previously assigned to the GJU on 1 January 2007 which are continued by the GSA as the “European GNSS Agency” within the scope of the EU Regulation No. 912/2010

GMCA Consortium



GMCA Consortium Roles

- DW International – Project Management. Prototype development - Addition of Galileo capability to the existing GNSS Performance Monitoring System (GPMS), with enhancements for interference, spoofing and jamming detection capability
- Integricom - Provides the GNSS processing engine
- Qascom - Adaption of GPMS to handle spoofing and interference threats
- Chronos Technology - To extend the capability of the existing GPS only jamming and interference detection sensors to include the Galileo GNSS
- Spirent Communications - Development of test platform and associated test cases for the prototype system

GMCA Project Goals

- Project Goals for GMCA:
 - Upgrade to include the capability to monitor and record GNSS/Galileo signal
 - Demonstrate the integration of Interference and Jamming Detection capability
 - Demonstrate the integration of Spoofing Detection capability
 - Exploitation of the results to expand within the aviation market and beyond

GMCA Project Goals

- Upgrade to include the capability to monitor and record GNSS/Galileo signal:
 - As the fleet adopts multi-constellation sensors, ANSPs, CAAs and Airports aiming to meet ICAO Annex 10 guidance will wish to include new constellations beyond GPS e.g. Galileo
 - EUROCONTROL CS7 aims to operate a monitoring system that includes Galileo
 - The project should serve as proof of concept for future updates to GPMS to include GLONASS and Beidou

GPMS Overview

- Allows users to comply with ICAO Guidance – Annex 10
 - Requires Monitoring and Recording of GNSS Data
- Localised GNSS Receivers
- Wide Area RAIM Prediction
- GNSS NOTAMs for State ANSP and Airspace users



GPMS Requirement



- ICAO guidance for recording of GNSS availability data and operational status
- ICAO Annex 10:
 - State approving GNSS operations should ensure relevant GNSS data are recorded. Data are for use in accident / incident investigations
 - ATC shall be provided without delay with operational status of radio navigation aids essential for approach, landing and take-off at aerodromes

GPMS Requirement



- GPMS continually monitors actual GNSS accuracy and integrity, determining real-time availability of GNSS and alerts during periods of unavailability
- All data recorded for playback and analysis

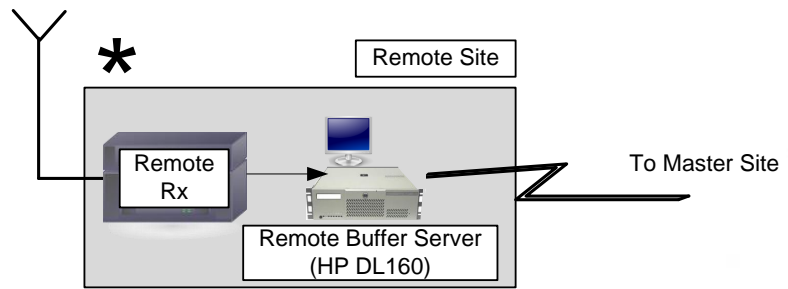
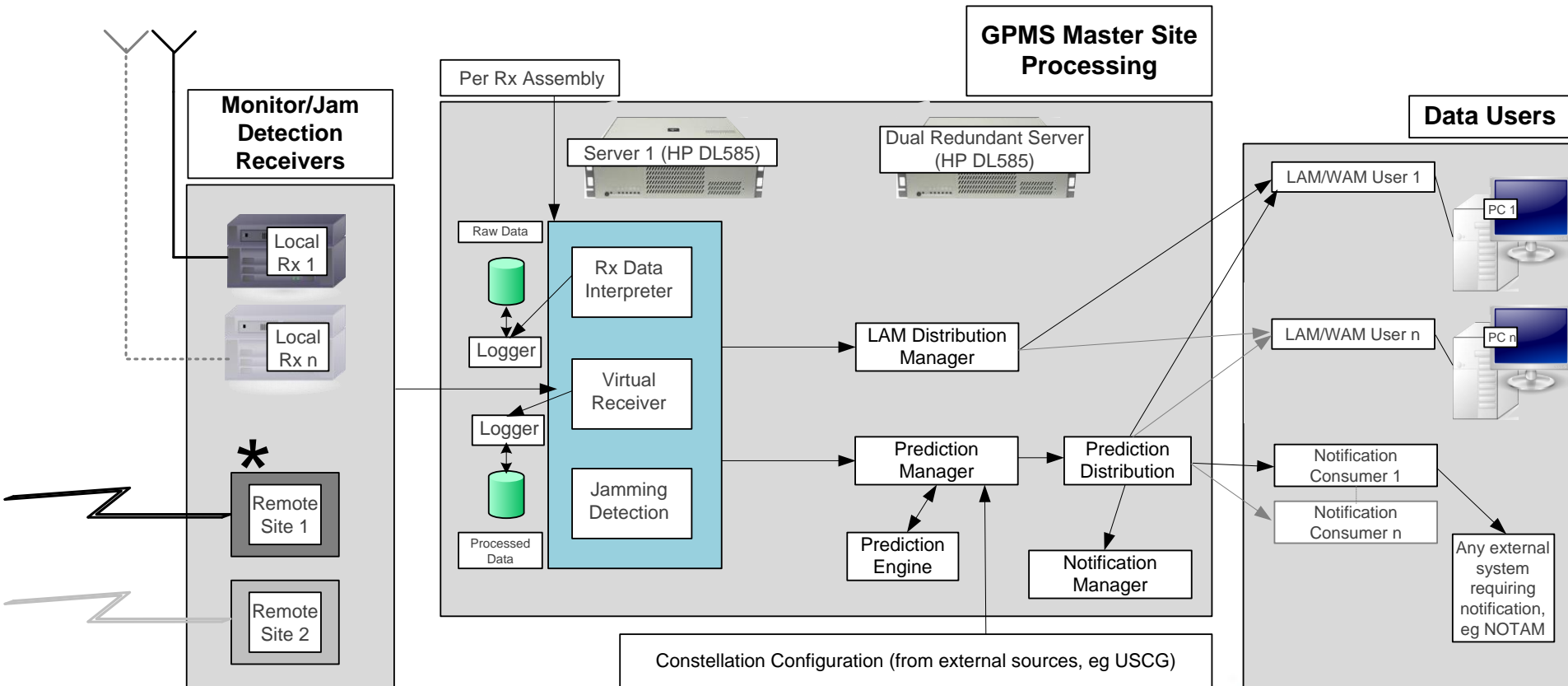
GPMS Award



- GPMS won at Galileo Masters in Nov 2013



GPMS Architecture



GPMS Deployments

- South Korea



- Hong Kong



Hong Kong GPMS



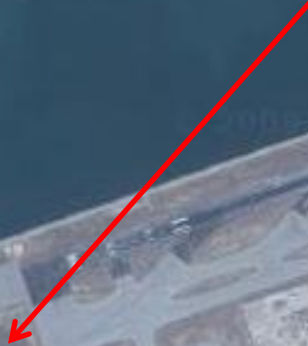
More...

Map

Satellite

Te...

Receiver Site



Server Site

Saudi Arabia GPMS Deployment



GPMS Training

- Approx 10 days training required for:
 - Theory
 - Operation
 - Maintenance
 - Administration



Scintillation Data Collection System (SDCS)



- The Hong Kong CAD Scintillation Data Collection System (SDCS) collects scintillation data throughout the approaching solar max, adding the SDCS to the existing GPMS located at Hong Kong International Airport



SDCS Overview

- 2 additional receivers, specifically designed for logging scintillation data, to be installed at Receiver Site located at LLZ building at HKG
- Signals received from existing antennas (part of GPMS) are split:
 - Existing data stream for GPMS unaffected
 - New data stream directed to a new server (located at existing GPMS Server Site) for scintillation data collection only

GMCA Overview

- Demonstrate Interference and Jamming Detection capability:
 - Upgrade existing sensors to incorporate the capability to track Galileo satellites and detect interference and jamming in the Galileo frequency band
 - Include Interference and Jamming Detection sensor information within GPMS

GMCA Overview

- Demonstrate Spoofing Detection capability
 - Design of a new external probe that is able to communicate with the DWI GPMS providing spoofing detection metrics including spoofed Galileo signals
 - Include Spoofing Detection sensor information within GPMS

GMCA Overview



S. Korea to set up GPS jamming surveillance system

By Lee Minji

SEOUL, April 10 (Yonhap) -- Amid growing plans to beef up its surveillance system against jamming signals that have targeted civilians

In addition to cyber attacks on South Korea's global positioning system (GPS) signals since the system widely used by planes, ships and



GNSS Vulnerability Scores at Wide-Ranging INC 2015

Delegates at this year's International Navigation Conference in Manchester took aim at a range of pressing topics, from autonomy to quantum technologies, indoor navigation, and legal issues, with a heavy dose of "navigation under threat."

Latest News

Peter Gutierrez

February 27, 2015

Share via: Slashdot Technorati
 Twitter Facebook

Almost half of the sessions at the International Navigation Conference (INC) 2015 held this week (February 24–26) in Manchester, England, were devoted to the theme of GNSS resilience and vulnerability, a topic that Dana Goward of the Resilient Navigation and Timing Foundation has been trying to drive home for years.

Reporting some movement towards establishing eLORAN as a potential back-up system in the United States — or, at least, a slowing of the dismantling of legacy LORAN systems — Goward can't have been impressed by



Ray Clore, U.S. State Department. Peter Gutierrez photo

GMCA Overview

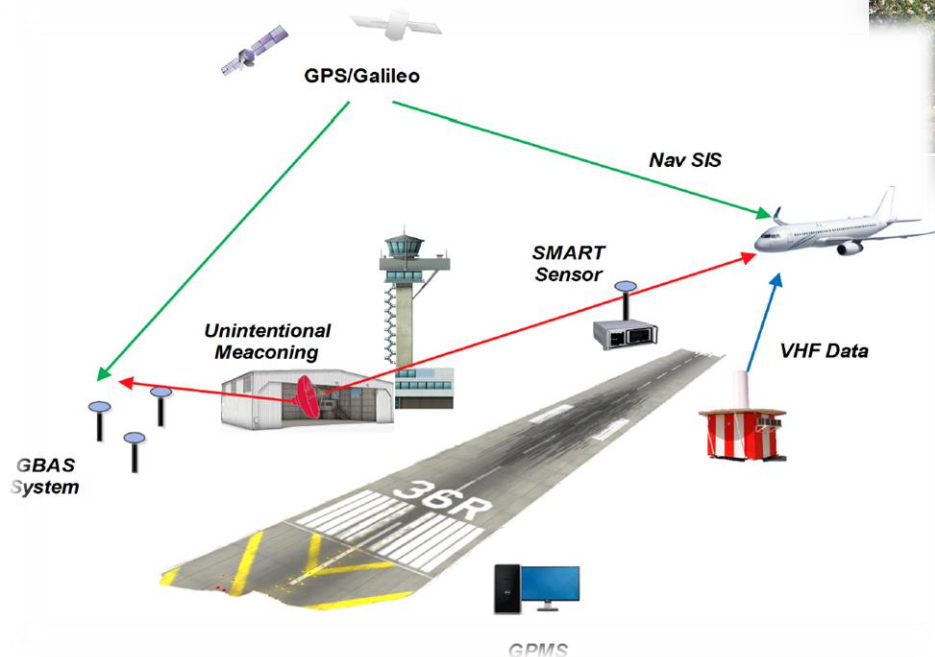
- Exploitation of the results to expand within the aviation market and beyond:
 - Deployment of the GPMS in operational environments where Galileo signal will be recorded and monitored in order to meet ICAO Annex 10
 - Deployment of GPMS to assist ANSPs, CAAs and airports in monitoring interference, jamming and spoofing
 - Expanding the operational scope of GPMS beyond Aviation, i.e. Maritime

Spoofing & Interference Threat Monitoring

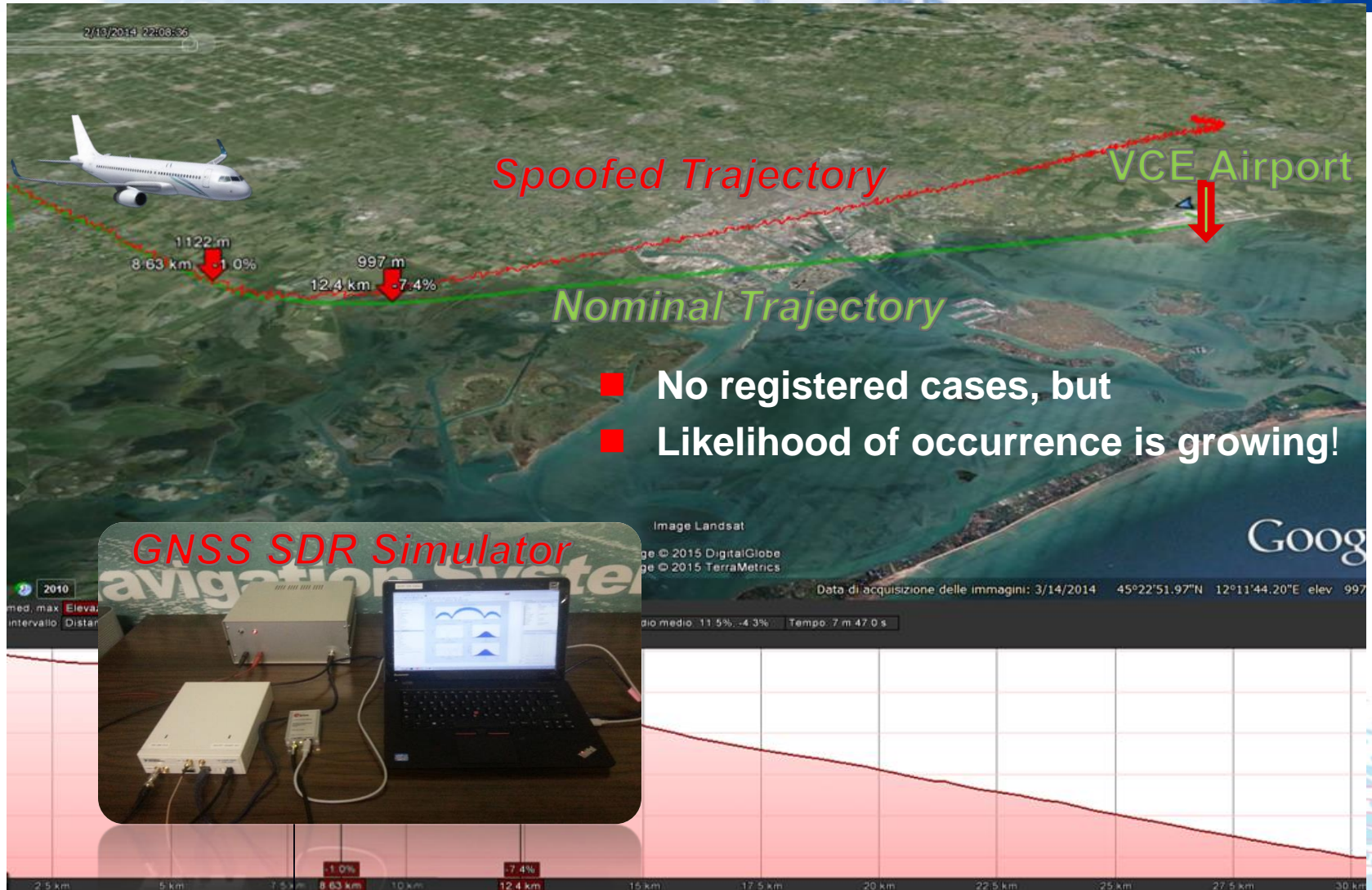
- Qascom offers Engineering technologies for Spoofing and Interference Monitoring in the Airport context:
 - State of Art Spoofing Detection
 - Monitoring of GPS L1, Galileo E1 and EGNOS
 - Spoofing Events reported to GPMS System
 - IQ samples Logging Available in case of Accident
 - Interference Monitoring based on Power Spectral Density
 - Time to Alarm below 6 seconds
- Demonstration to be performed in 2016

Non Intentional Spoofing: Repeaters

- Hannover Airport Case, 2012
- a GPS repeater in a Hangar
- Power ~ 20 dB higher than limit
- Interference impact for hundreds of meters
- Operations (Taxiing and Take off) highly affected

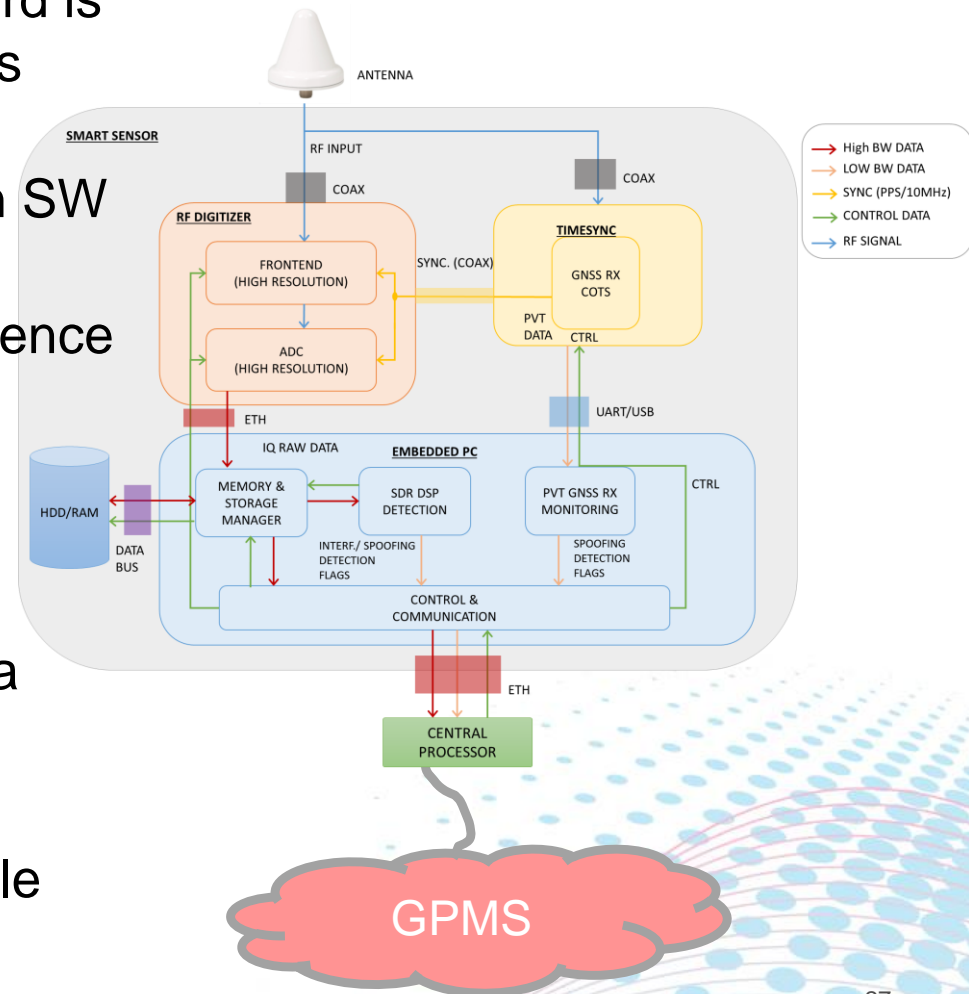


Intentional Spoofing, Landing Case (Simulated)



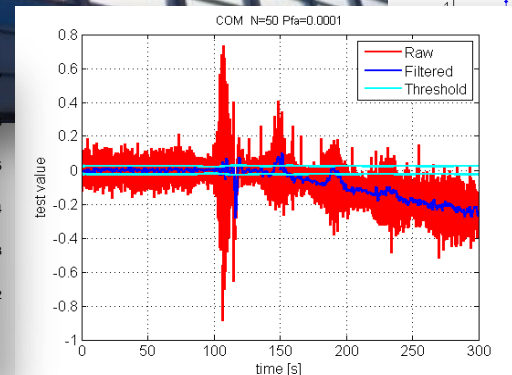
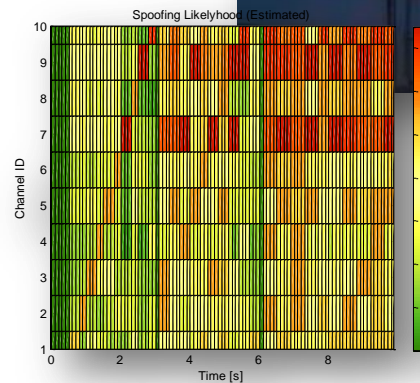
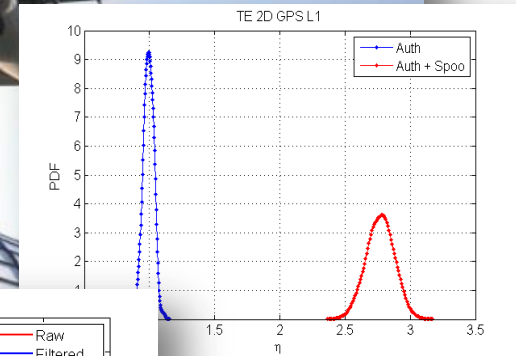
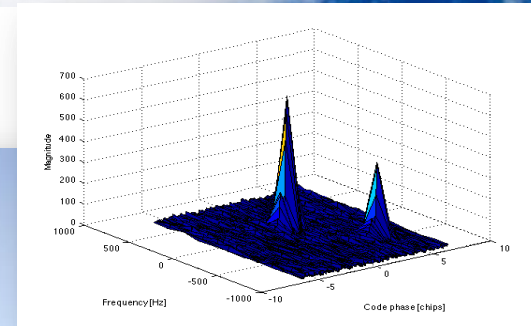
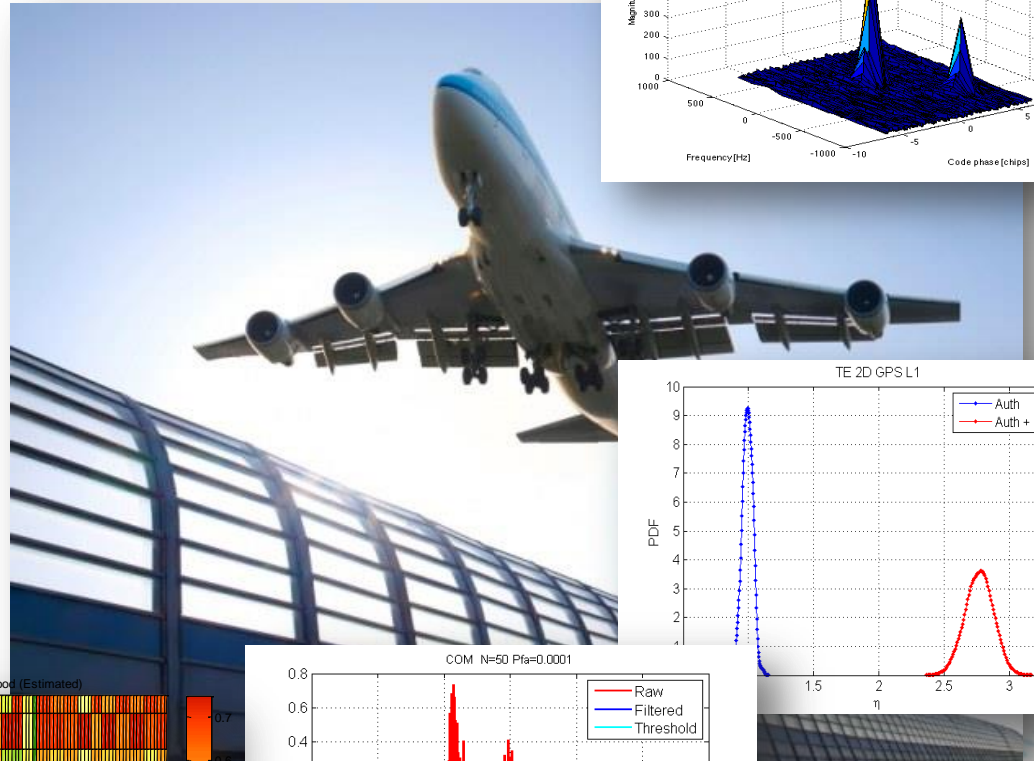
SMART Sensor Architecture

- Multiband GNSS Antenna
- High End RF Digitizer: the board is capable of sampling RF signals with a high resolution ADC.
- Embedded PC: device that run SW to:
 - Perform SDR based interference and spoofing detection techniques
 - Monitor GNSS RX PVT for spoofing detection
 - Manage collection of IQ data batches
 - Communication with GPMS
 - Time Synchronization Module



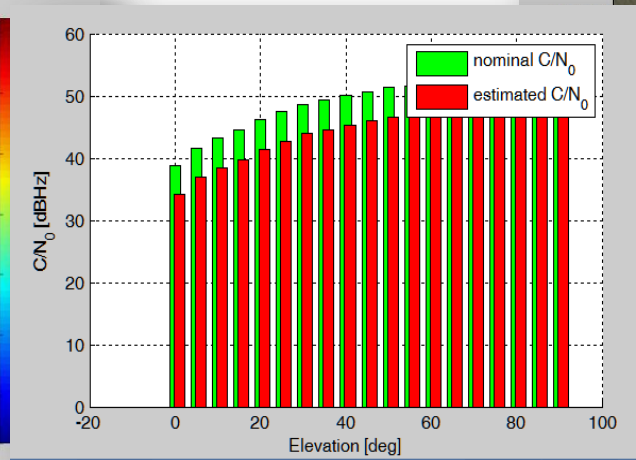
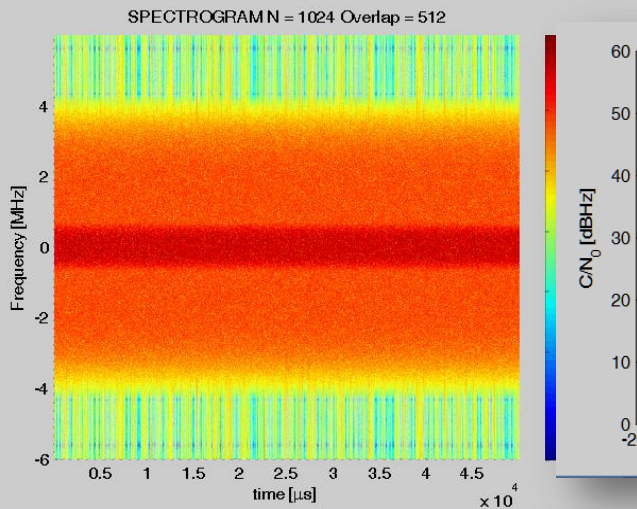
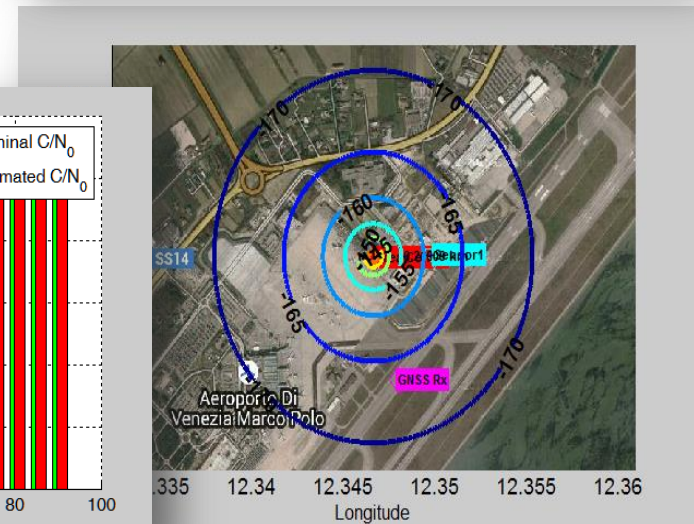
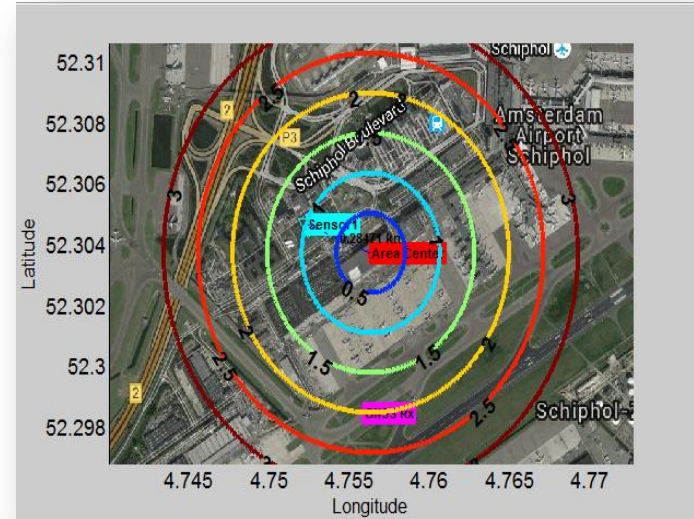
Spoofing Monitoring Technologies

- A set of techniques are being tuned for airport scenario
 - Baseband DSP
 - Multi Peak Detection
 - Correlators Energy Detection
 - Observable Monitoring
 - Doppler and CN0 Variance
 - RAIM for Antispoofing
 - PVT Monitoring



Spoofing and Interference Scenario Emulation

- Pre-Analysis before field Testing
- Tools for Spoofing and Interference Scenario Reproduction
 - Sensors Configuration
 - Spoofing Analysis
 - Interference Monitoring Area
 - GNSS Rx impact assessment
 - AGC monitoring, Spectrograms



Thank you for listening - Any questions?

john.wilde@dwint.com john.wilde@navtech.aero

www.dwint.com

www.navtech.aero