TACOT Project

Trusted multi **A**pplication re**C**eiver f**O**r **T**rucks

Bordeaux, 4 June 2014

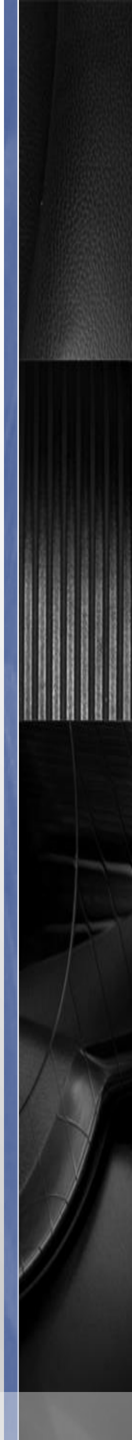
Agenda

TACOT Context & Solution

Technical developments

Test & Validation results

Conclusions



GNSS ease our lives…

GNSS is part of the every day's life of hundreds of millions of people:

- multitude of applications
- successful use since many years
- social / environmental dimension
- enable promising future services

Particularly true in the road transport domain:

- enables applications such as car navigation or fleet management
- ground to develop advanced applications in the ITS domain

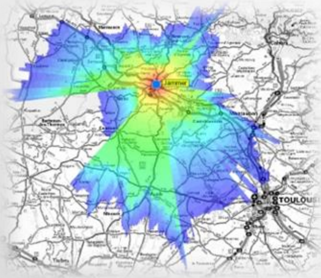
GNSS unique assets:

- accurate position, velocity and time (PVT) data
- worldwide
- high availability
- free of charge

… but also have limitations

The main GNSS weaknesses are:

- not available in “in-doors” environments (tunnels…) or partially available in masked environments (urban areas, mountains…)
- subject to threats (jamming, meaconing or spoofing)



Practically these issues lead to either:

- a lack of availability of the GNSS service
- a GNSS-like misleading information
- performance degradation

These issues hinder or slow down GNSS applications which require:

- high availability of the PVT services, even in constringent environments
- a good level of trust in PVT information

TACOT provides

PVT trustfulness
Trusted PVT with a Level of Confidence (LOC)

GNSS attacks detection
Jamming, spoofing, meaconing

Increased PVT availability
Dead reckoning

TACOT consortium 1/2

- **Coordinator**:
- The whole European Tachograph Industry:
- Expert in Trusted GNSS:
- Expert in Sensor fusion:
- Expert in Fleet management: (It)
- Experts in Security

TACOT consortium 2/2

- Users representative and institutions:

  Confederation of Organisations in Road Transport Enforcement

- Legal / regulatory aspects:

- Business & exploitation plans, dissemination:

- *Also consulted*
  - *European Automobile Manufacturers' Association:*
  - *International Road Transport Union:*
  - *European Traffic Police Network:*

- *Test & Validation*

Agenda

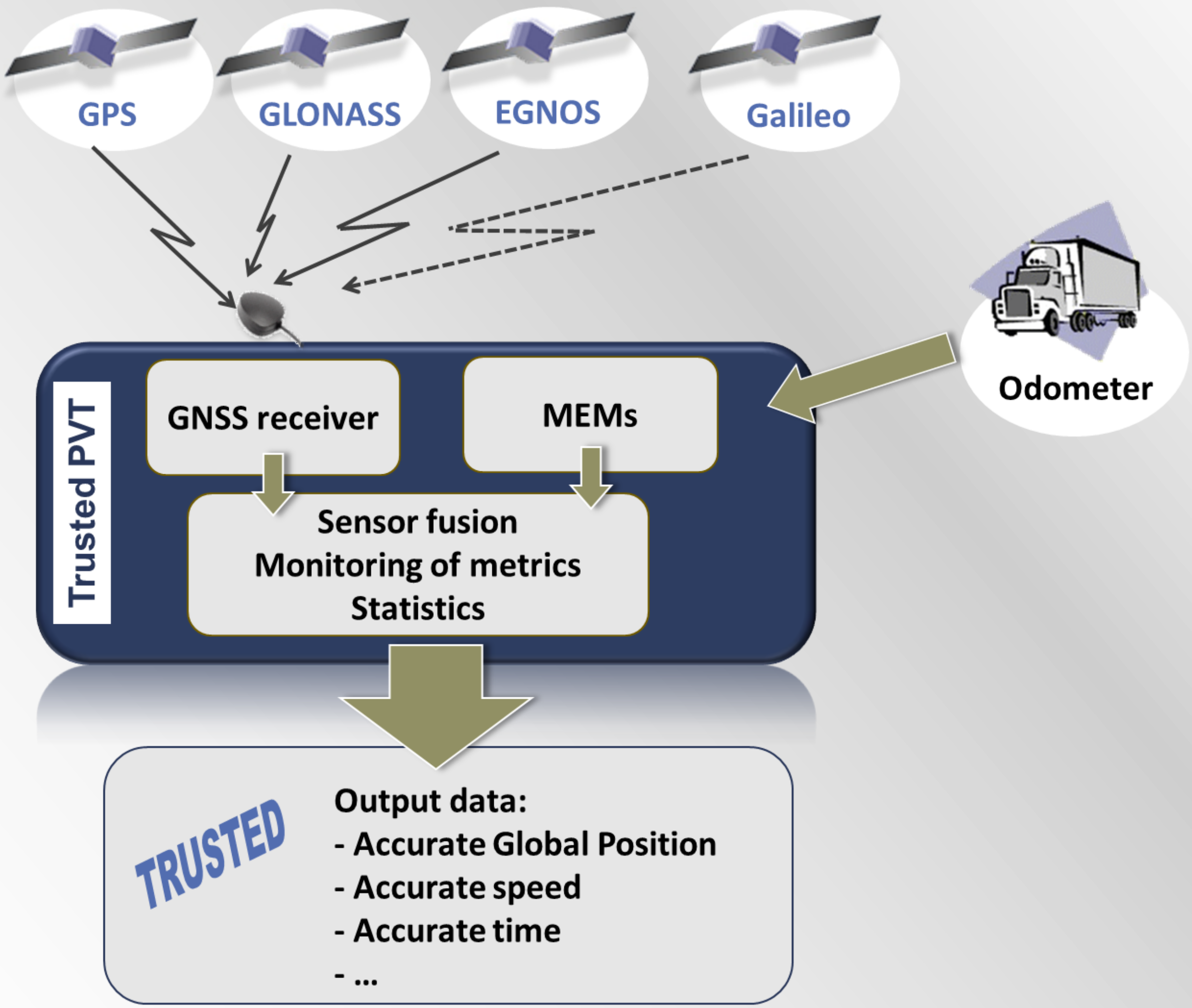
TACOT Context & Solution

Technical developments

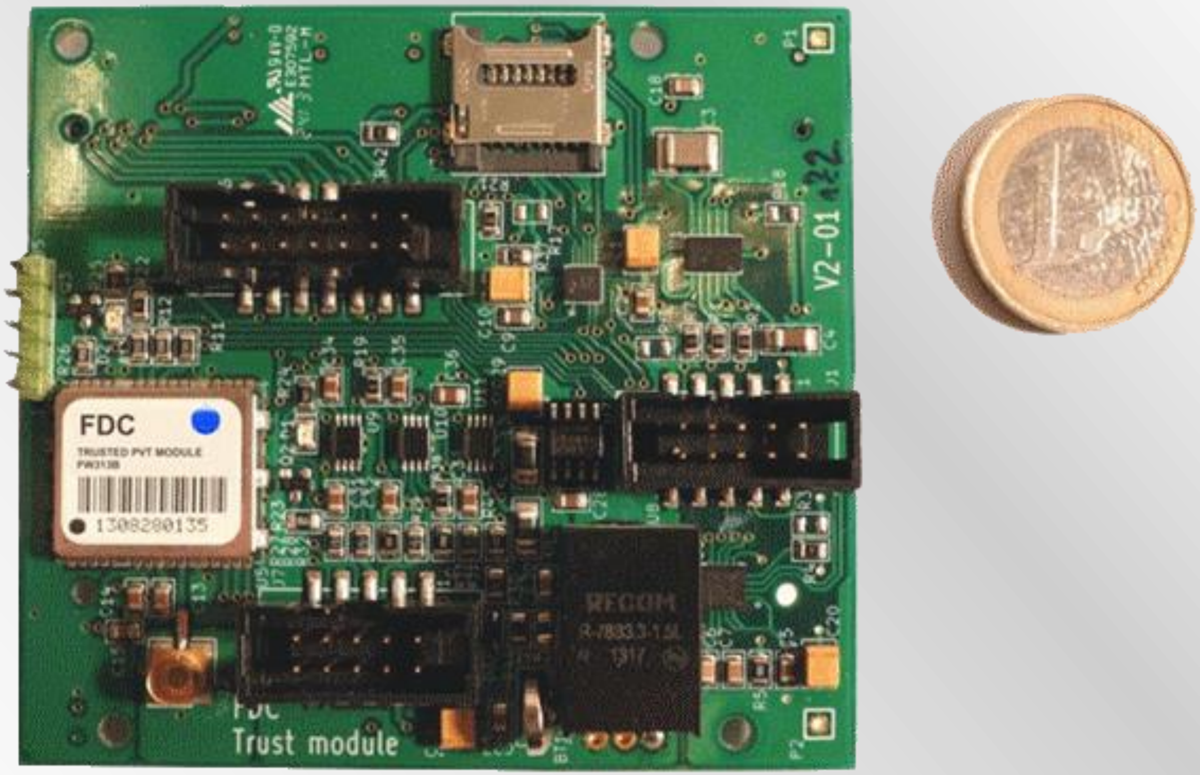
Test & Validation results

Conclusions

Trusted PVT module overview

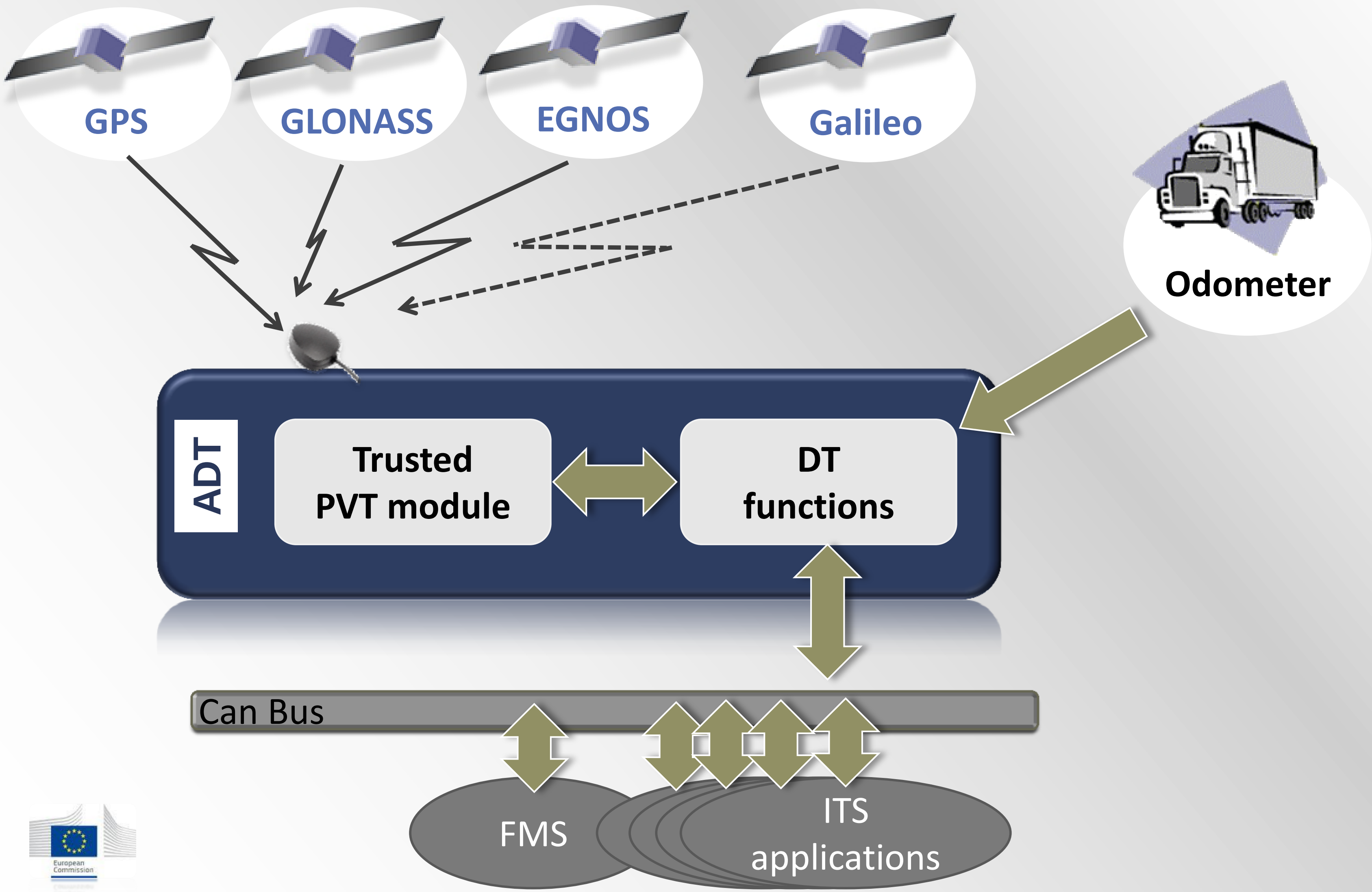


Trusted PVT module hardware



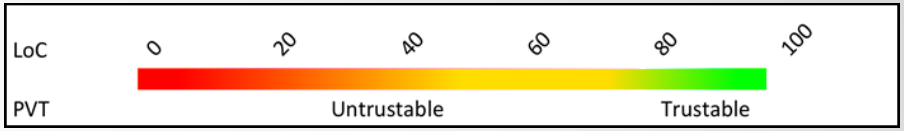
- Board designed and developed by FDC
- Implementing TESEO II and MEMS sensors from ST Microelectronics.

Augmented Digital Tachograph overview



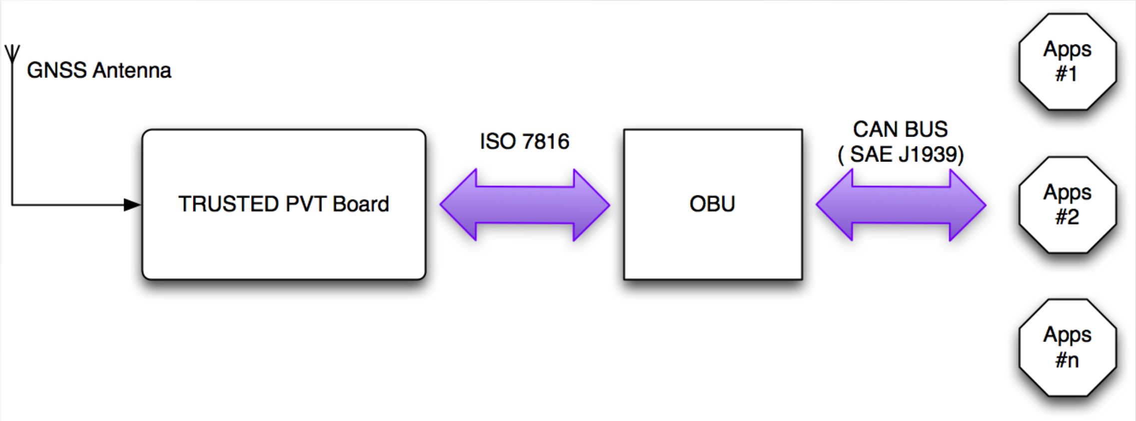
Overview of the trusted PVT interfaces

- Input data
  - GNSS, motion sensors, RTC time
  - Odometer data sent through the DT
- Output on request of the Digital tachograph
  - **Position, Velocity, Time**, Heading and associated accuracies (standard deviation, CEP95, CEP99)
  - **Status** of input data for each sensor (OK, Implausible, Corrupt, No info)
  - **Level of confidence** with the interpretation rule hereunder



Overview of the trusted PVT interfaces

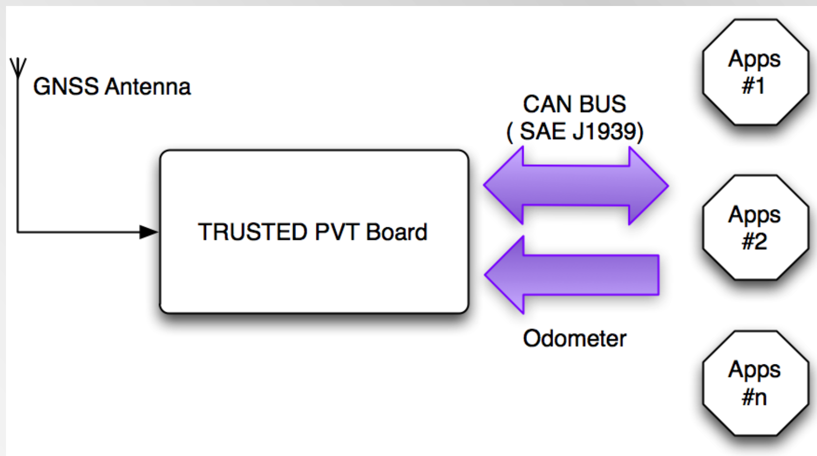
- Trusted PVT module is designed to be implemented in two different ways
- Connected to an OBU (TACOT case)



  - Secure communication through ISO 7816-3 protocol
  - PVTC information are sent (or not) by OBU to third-party applications
  - Use of proprietary J1939 messages to send digitally signed PVTC info.

Overview of the trusted PVT interfaces

- Directly connected to the CANBUS



  - PVTC information are sent to third-party applications
  - Use of proprietary J1939 messages to send digitally signed PVTC info
  - Trusted PVT module reads odometer data on the CANBUS
  - The module implements built-in security features

Augmented Digital Tachograph hardware

- Integration of the trusted PVT module in the Digital Tachograph (DT)
- Communication interface with trusted PVT module (protocol ISO 7816)
- Broadcast of signed and unsigned trusted PVT data on the CAN bus
- Implementation of sample Use Cases utilizing trusted PVT data

Agenda

TACOT Context & Solution

Technical developments

Test & Validation results

Conclusions

Trusted PVT module tests methodology

Tests with the PVT module started one year ago (may 2013).
Three main parallel testing phases were performed for the validation:

Integration of the PVT module in DT environment (Phase A)

- Integration of the Trusted PVT function in a Digital Tachograph
- Provision of Trusted PVT information to any ITS application via a CAN bus

Behavior of the PVT function under nominal conditions (Phase B)

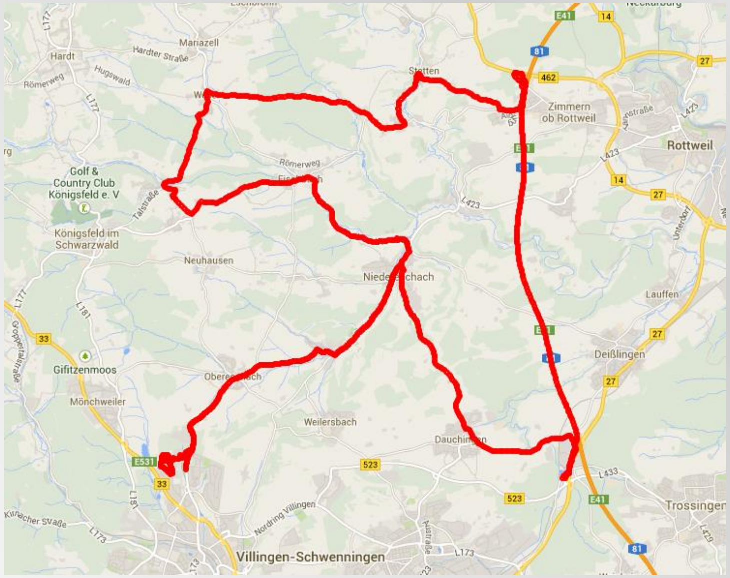
- Tuning of the Level of Confidence associated to the PVT
- Operational use cases

Performances of the PVT function under various attack scenarios (Phase C)

- Behavior of the LOC under GNSS attacks : spoofing, jamming, meaconing, replay
- Other attacks on sensors (odometer, barometer, etc.)

Phase A : Driving sessions in Villingen (Germany)

- Truck equipped by Continental (ADT, CAN recorder, etc.)
- ACTIA Italia ‘s OBU for the FMS
- Trusted PVT module provided by FDC
- 60 km trajectory in various environments (forest, varying altitude) dynamics (road, highway, urban) and GNSS reception condition (asymmetric, forest, open-sky, etc.)



Phase A : communication from PVT module to FMS system

- Actia Italia's OBU for the FMS and Continental ADT

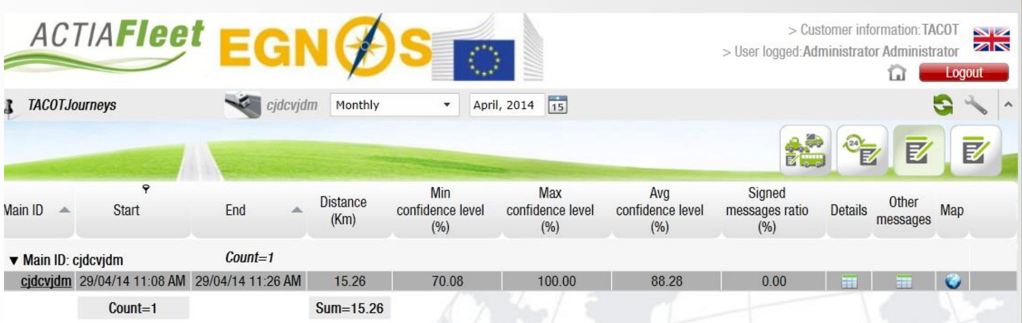
Trusted PVT module tests & results

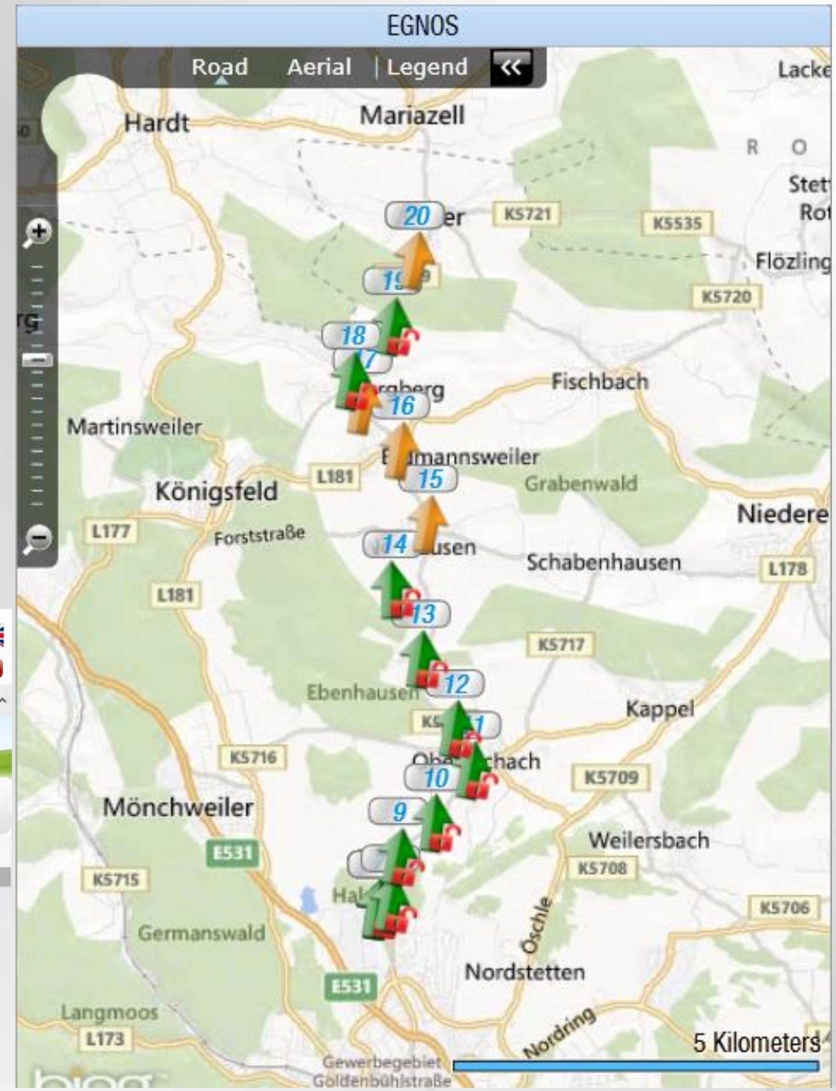
Phase A : Use cases

- **Trusted PVT function as Independent Motion Sensor**
  - ✓ The ADT uses the PVT function block as a secondary, independent motion sensor (IMS) in order to detect vehicle motion conflict events
- **Automatic re-adjustment of the internal DT clock**
  - ✓ The internal clock of the DT is re-adjusted automatically using the secure and precise time delivered by the trusted PVT module.
  - ✓ DT has always precise time
- **Recording of Location data**
  - ✓ The ADT records location data periodically (e.g. every 3h) and at the occurrence of certain events (e.g. start and stop of journey)
- **Transmission of trusted PVT data on CAN bus**
  - ✓ The ADT transmits trusted PVT data containing accuracy and confidence indicators to OBEs connected to the vehicle CAN bus

Phase A : communication from PVT module to FMS system

- First step done on test bench with real time communication to ACTIA's telematic servers
- Second step done installing both ADT and Telematic gateway unit in vehicle
- Here is an example of a trip of 15 kilometers



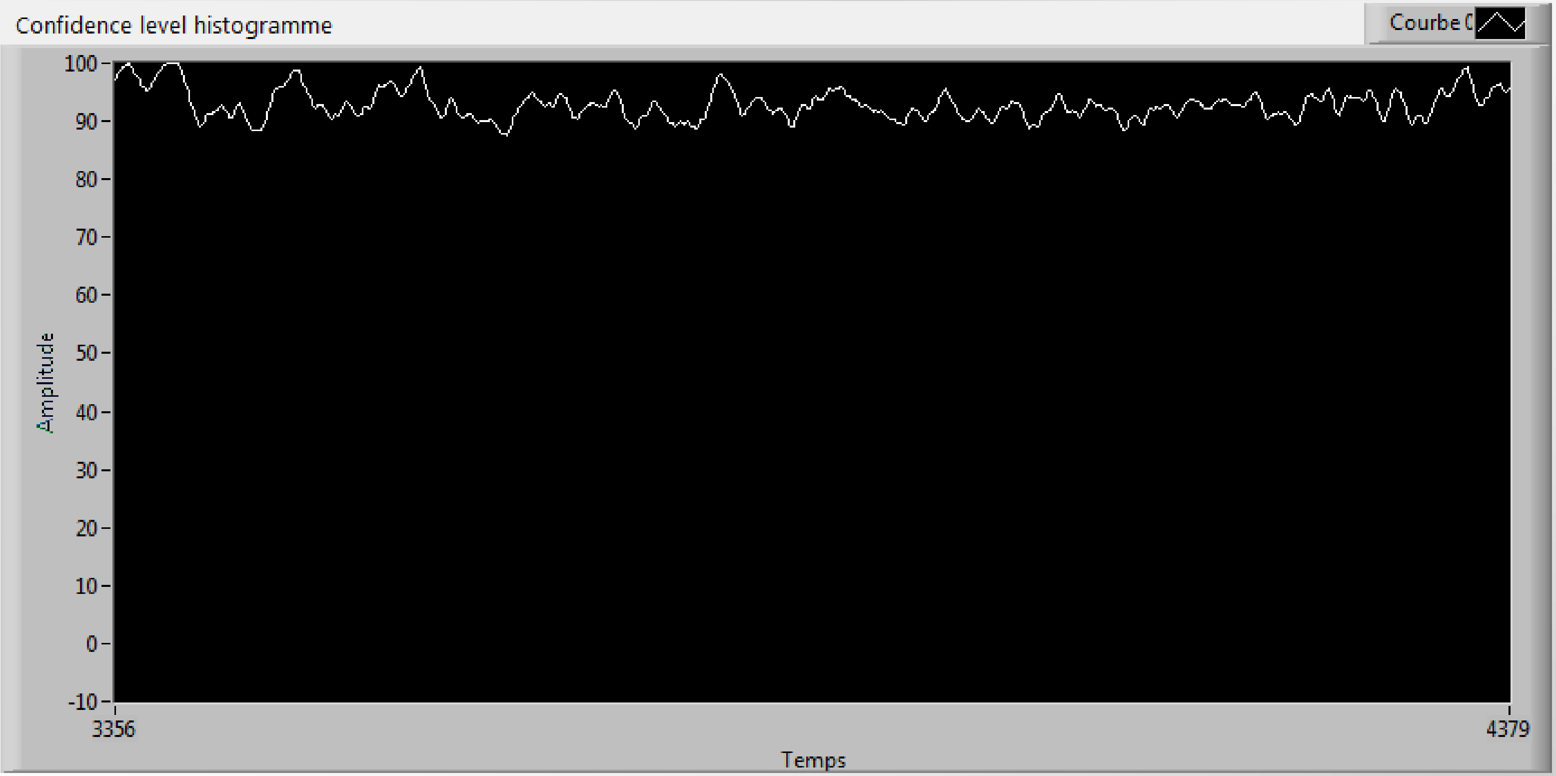


Phase B : Validation of the PVT function in nominal conditions

- **Development based on several internal data campaigns (FDC, Probayes)**
- **Static and dynamic tests to analyze and refine the PVT function**
  - ✓ Behavior of the PVT function in nominal conditions and degraded environment
  - ✓ Dead reckoning
- **Main validation tests based on two data campaigns (with Continental)**
  - ✓ July 2013
  - ✓ February 2014

Phase B : Typical behavior of LOC

- Static position and good GNSS reception



Phase C: Performances of the PVT function under various attacks

- **Main objective is to challenge the PVT module against GNSS attacks**
  - ✓ Meaconing, Jamming, Spoofing
- **Assess the behavior of the LOC under an attack on other sensors**
  - ✓ Odometer, barometer
- **Validation was performed during a test session at the JRC in ISPRA (29-30 April 2014)**
  - ✓ Tests conducted with the JRC team at the EMSL (European Microwave Signature laboratory)
  - ✓ Attack scenarios are detected

Attacks on the GNSS signal

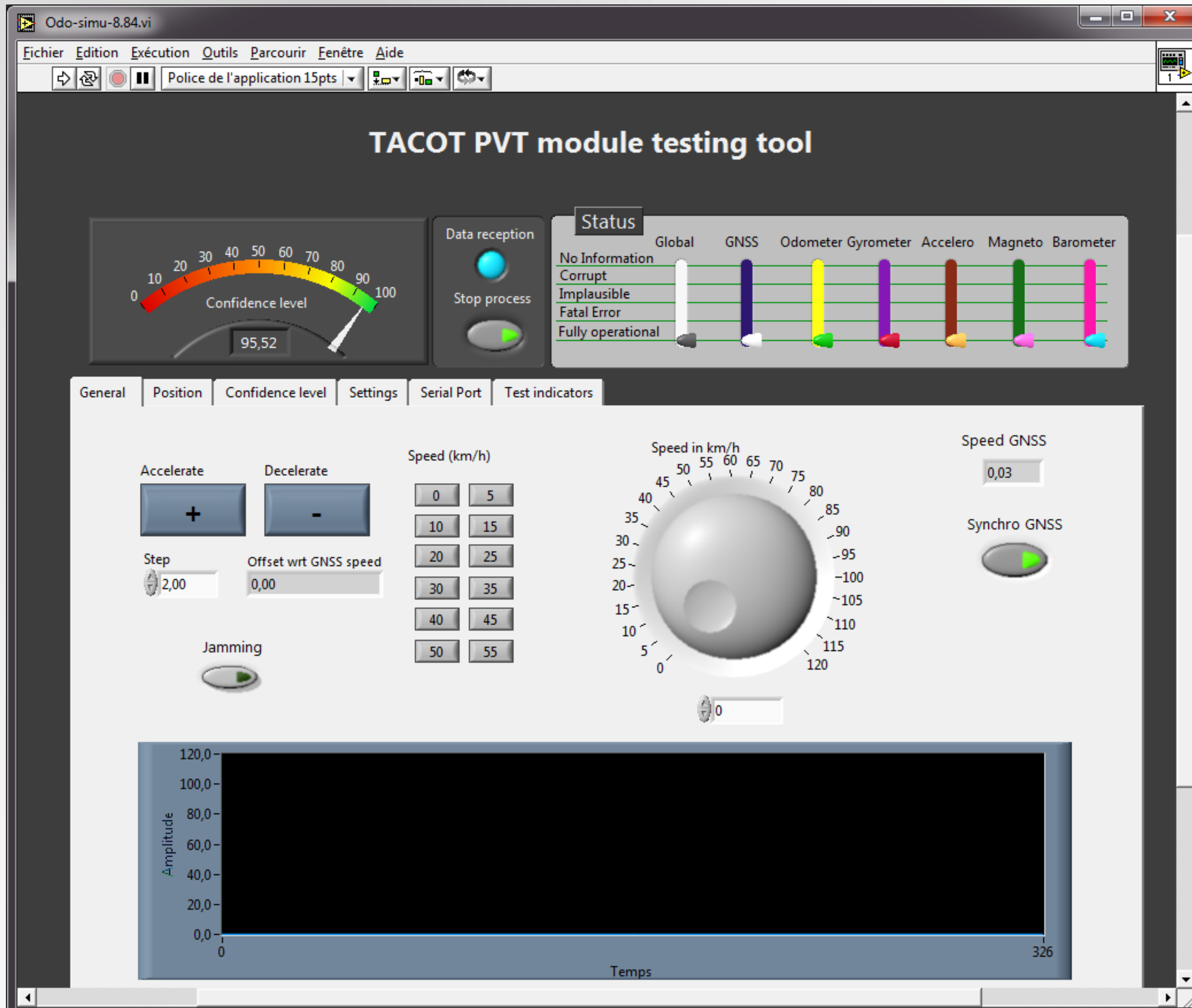
- **Replay scenario**
  - ✓ GNSS signal was grabbed and replayed
- **Inconsistencies in the GNSS signal characteristics**
  - ✓ Detection of simulated GNSS signal
- **Inconsistencies in GNSS navigation data**
  - ✓ Use a tampered GNSS navigation message
- **Jamming**
  - ✓ Jammer GPS/GLONASS provided by FDC

Attacks on the sensors

- **Attack on the remote sensors : odometer**
  - ✓ GNSS and odometer velocity differs
- **Attack on the local sensor**
  - ✓ Locally tamper barometer, accelerometer and gyrometer

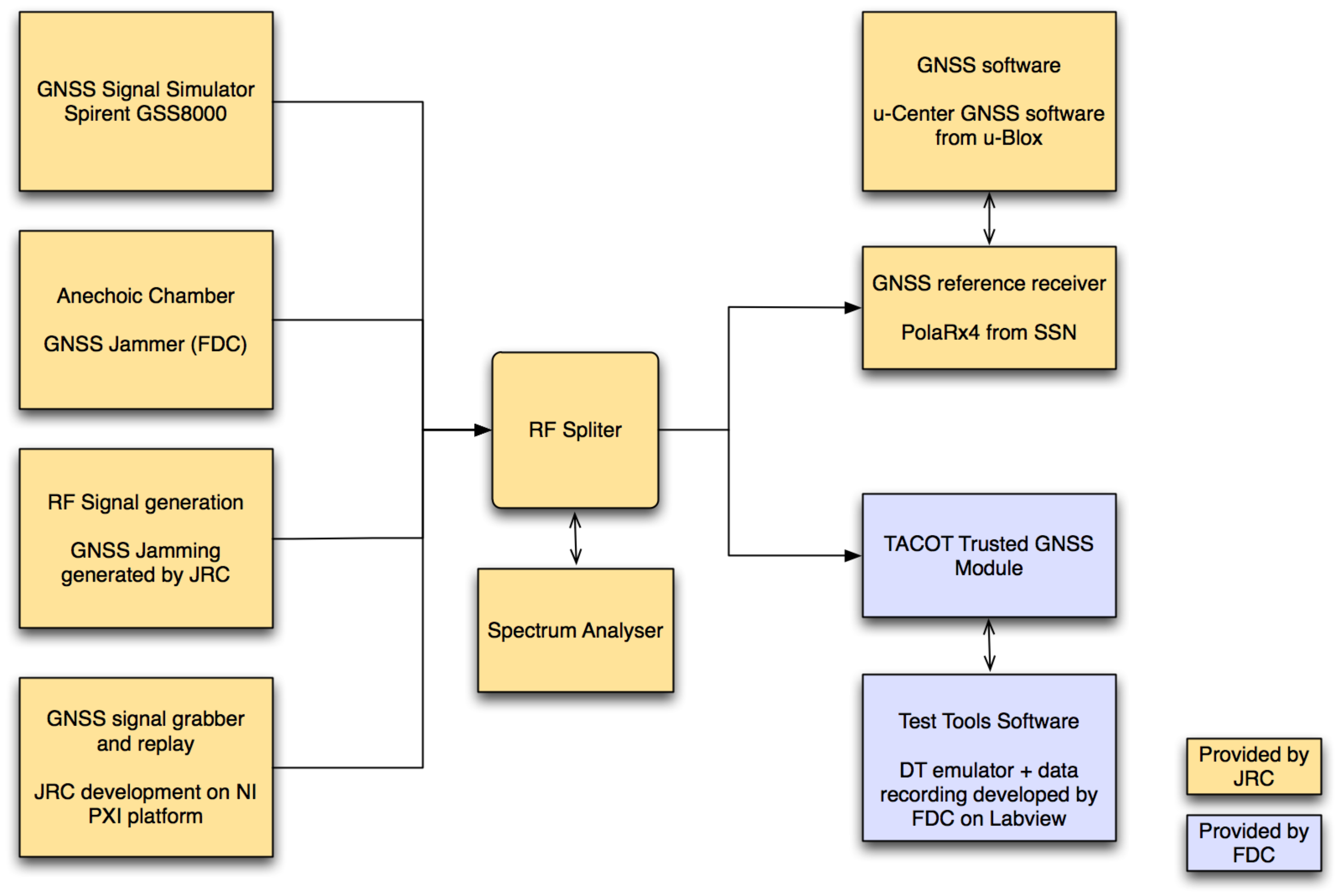
Trusted PVT testing tool

- ✓ Simulates the ISO7816 on a serial port
- ✓ Sends odometer data and retrieve the main output of PVT function
- ✓ Display the LOC and status of all components
- ✓ Odometer data is synchronized on the GNSS velocity or not (possibility to send fake velocity)



Equipment used during JRC test campaign (29-30 April 2014)

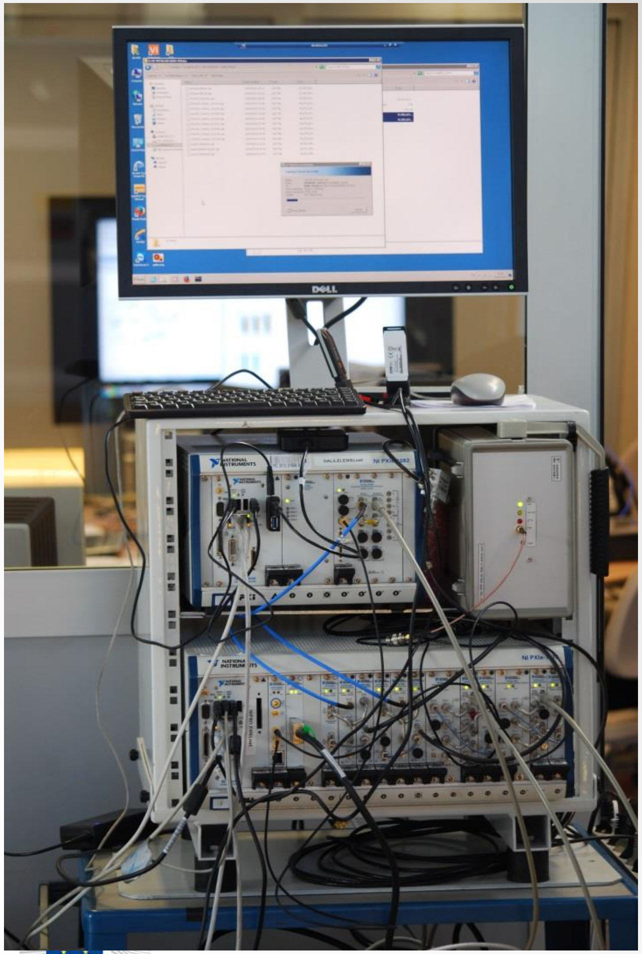
Tests conducted at EMSL (European Microwave Signature Laboratory)

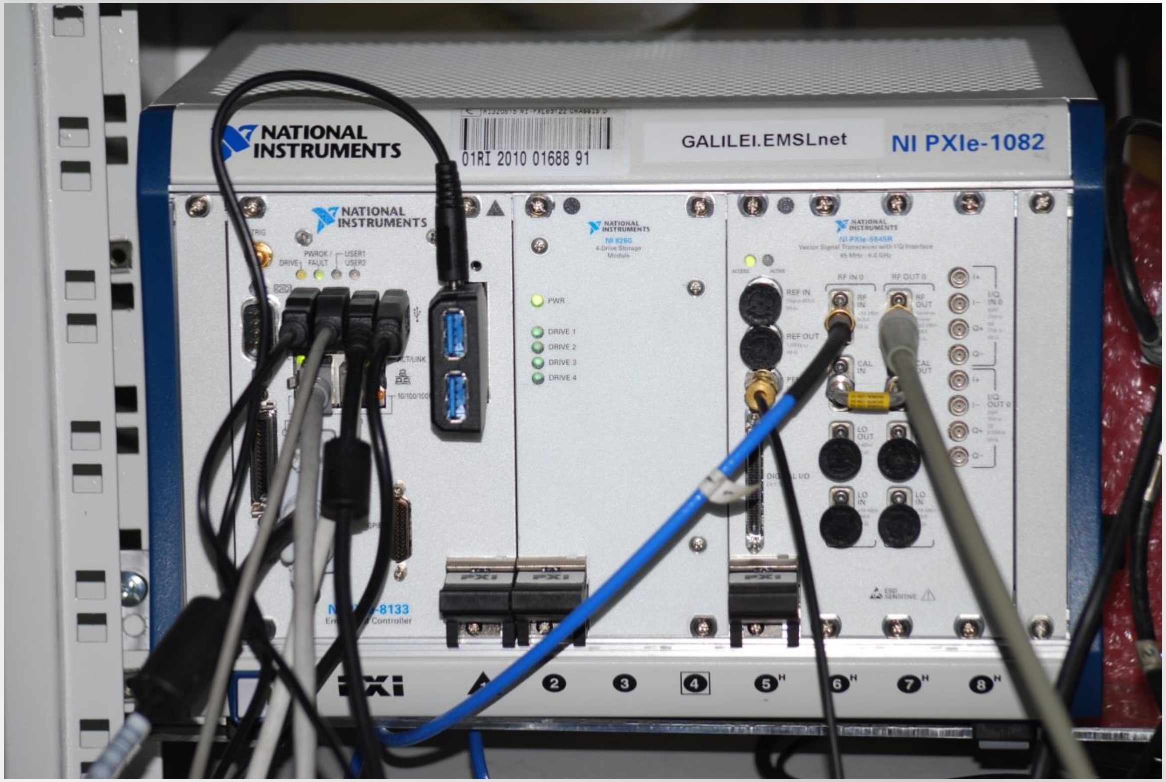


Preparation of the JRC test campaign

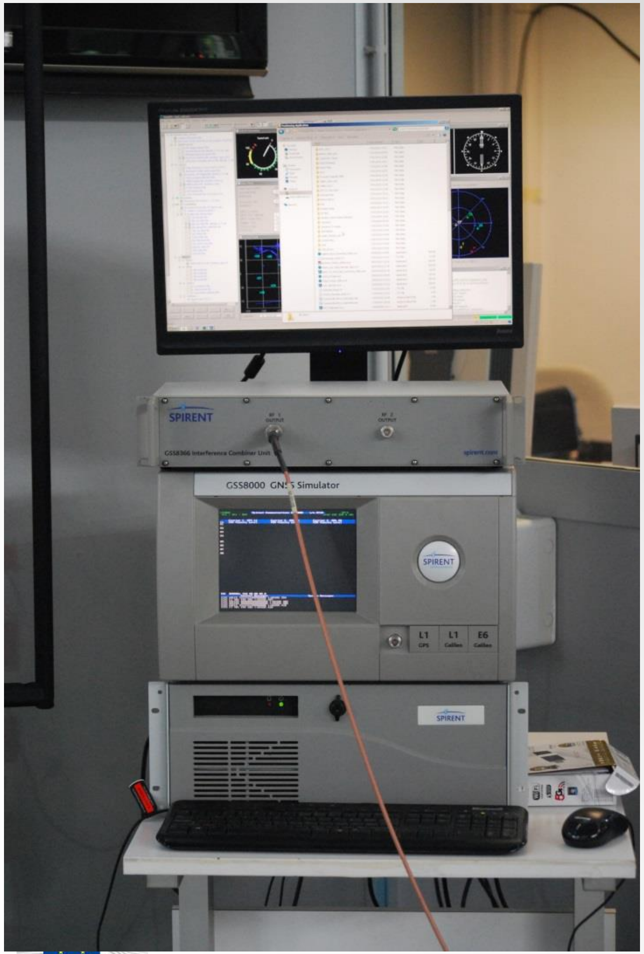
- ✓ Live datasets were recorded with a dual band data grabber connected to a geodetic antenna outside the EMSL (see picture)
- ✓ A reference NMEA file was fed in the Spirent SimGEN with the same location, time and reference almanacs
- ✓ Part of the static tests scenarios were setup by modifying the reference NMEA file and providing it to the Spirent GSS8000
- ✓ Replay scenarios were performed with NI PXIe-1082I

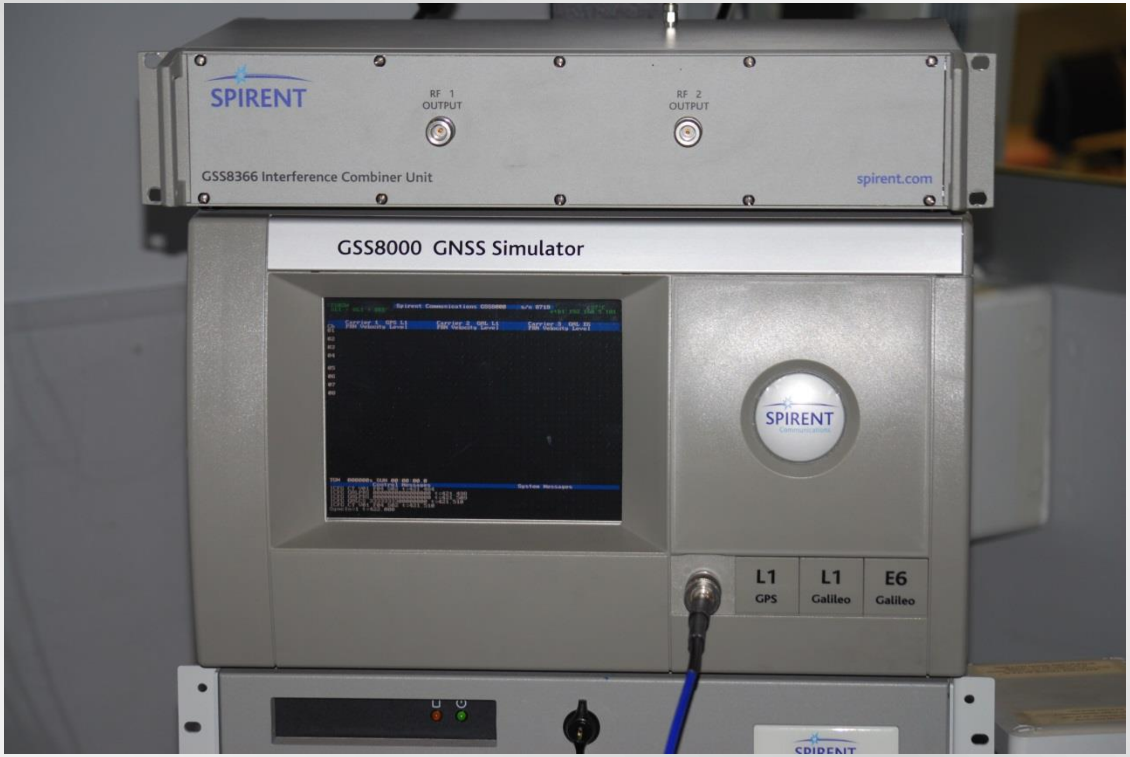
NI PXIe-1082: GNSS signal grabber and replay equipment





SPIRENT GSS8000: GNSS signal simulator

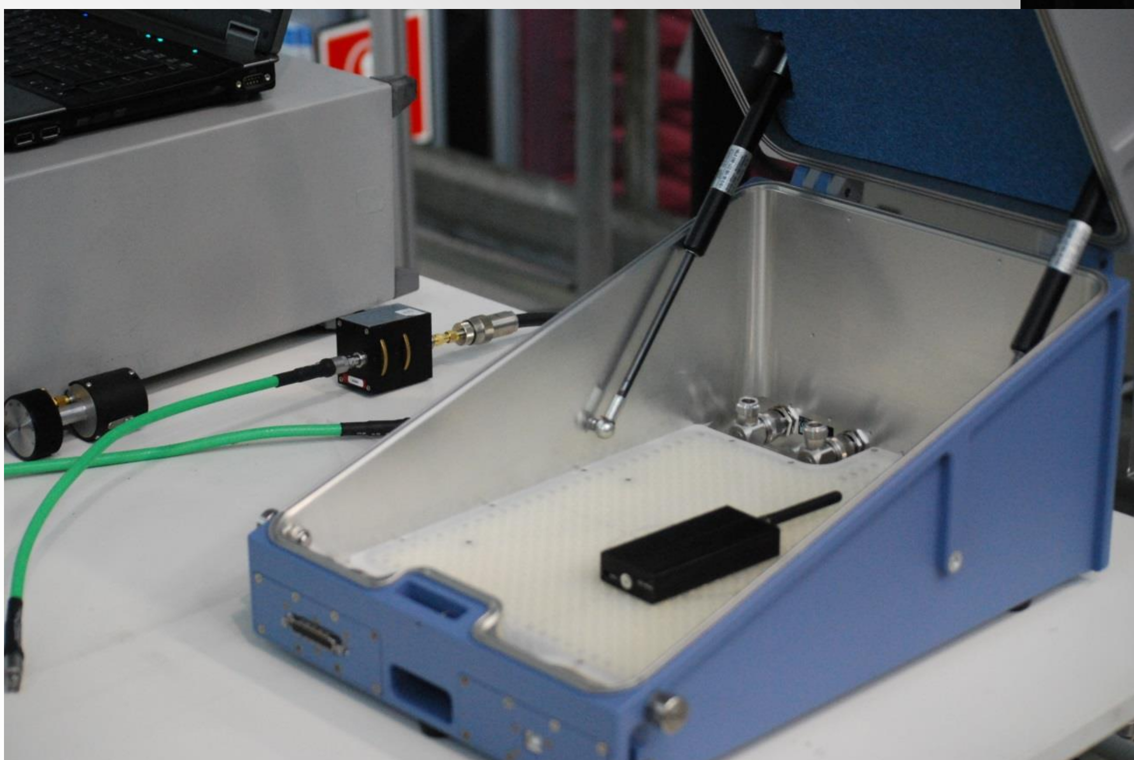


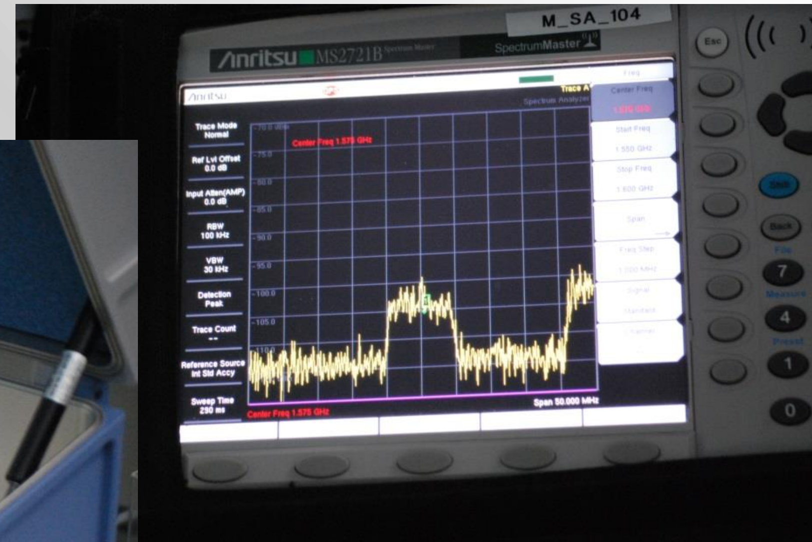


European Commission

SEVENTH FRAMEWORK PROGRAMME

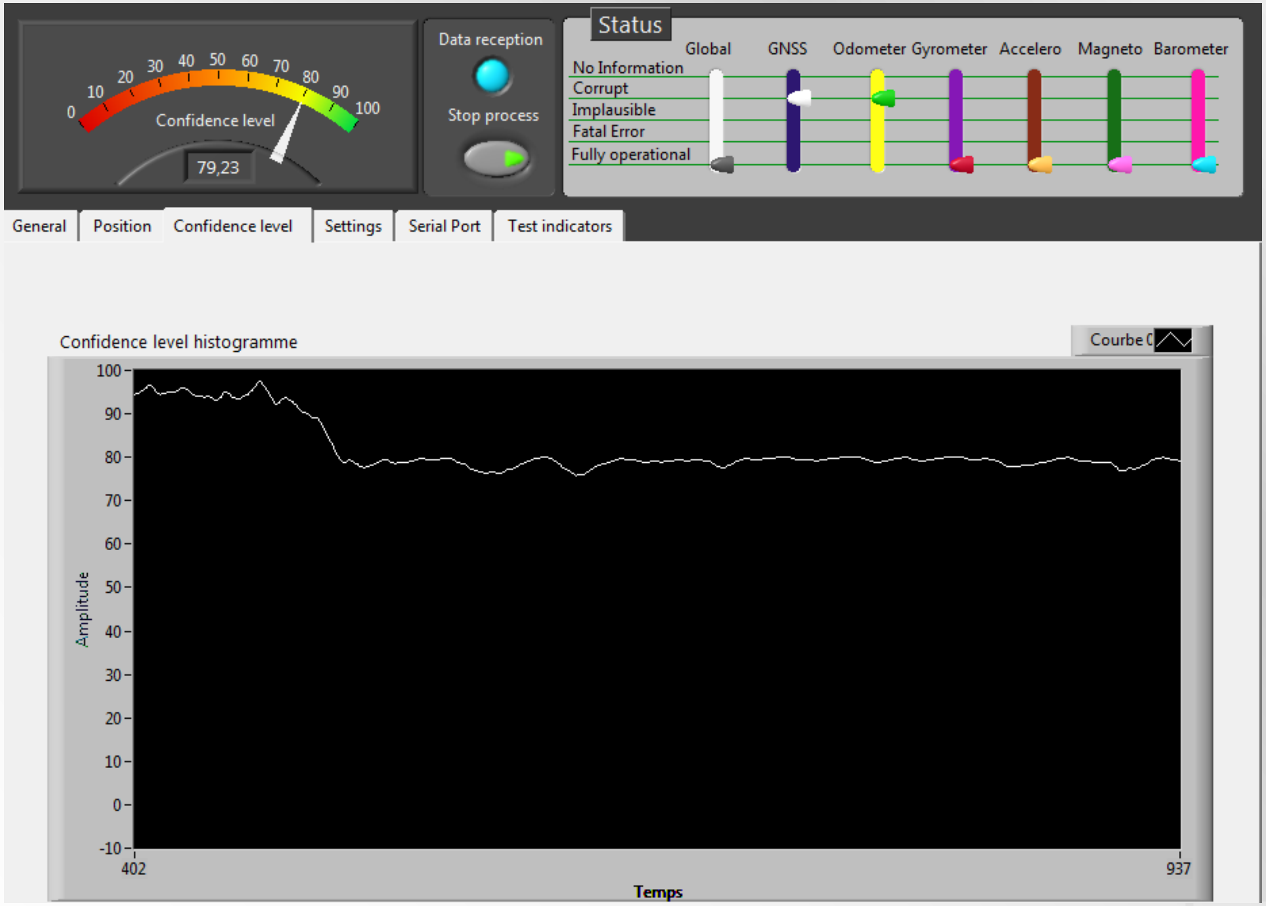
Anechoic chamber + Jammer and Spectrum analyzer





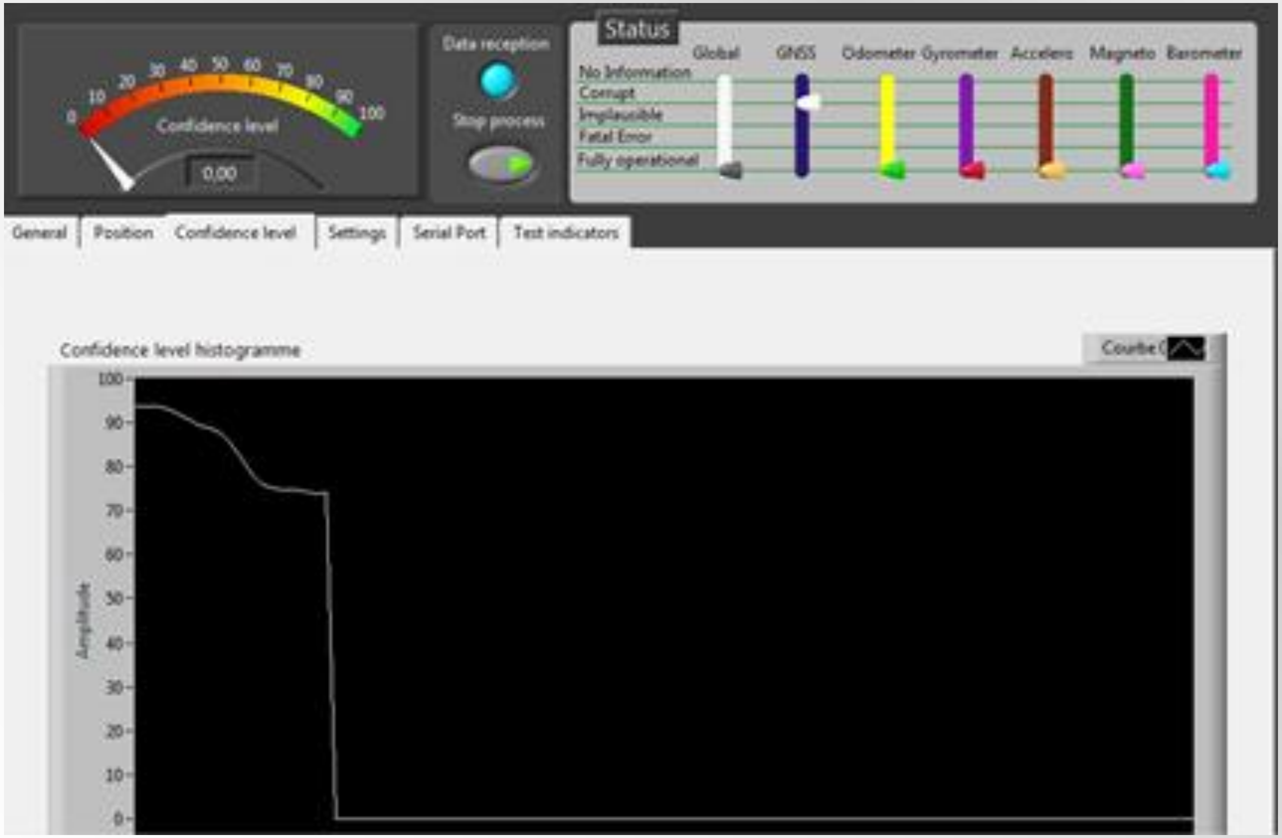
Attack on the odometer

- Example with a difference of 20 km/h between GNSS and Odometer speed
- LOC falls below 80 and status of Odometer and GNSS is set to Corrupt



Replay scenario

- After 5 minutes the reference data set was rewound back 1 minute
- LOC began to drop then falls brutally to 0 when the GNSS time is compared with an internal accurate source of time. Status of GNSS is set to Corrupt

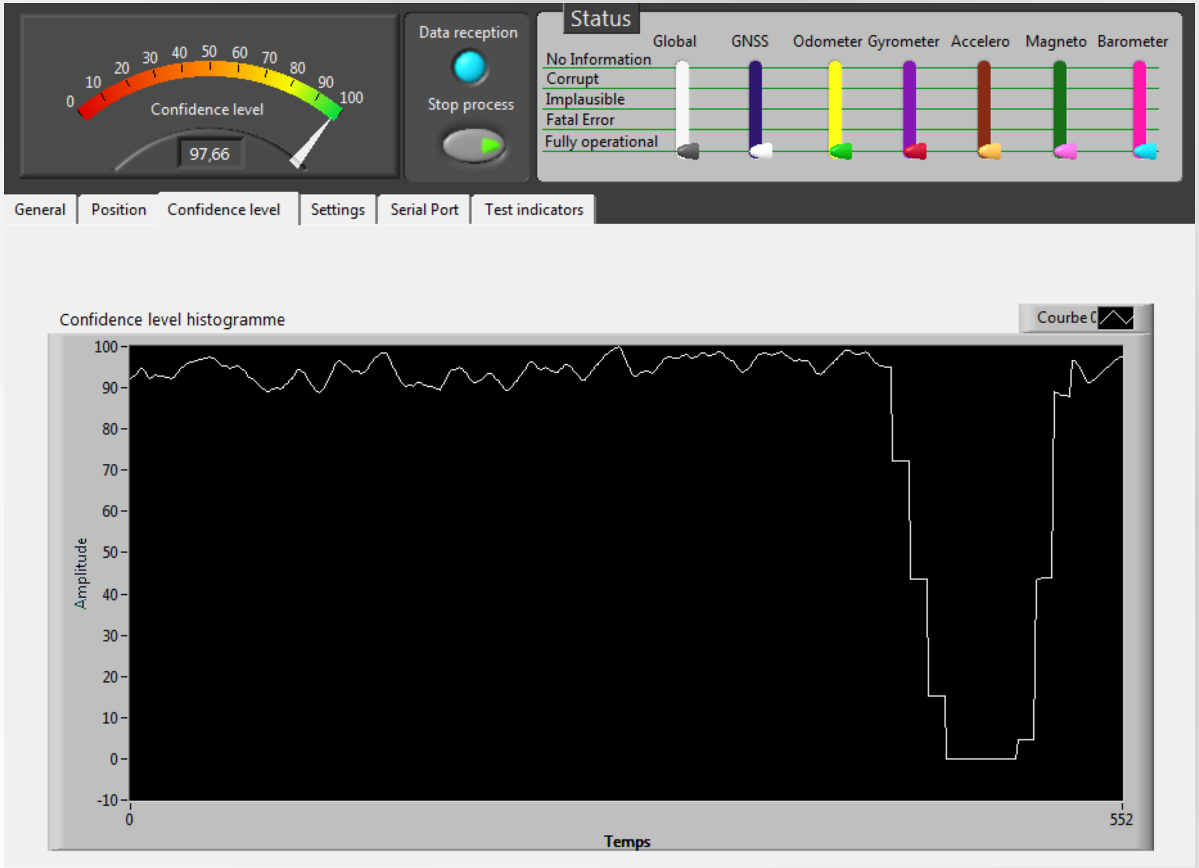


Tampered GNSS navigation message

- LOC drops progressively (in the figure below there are two steps)
- Not enough to have a change of the GNSS status (need to wait longer)

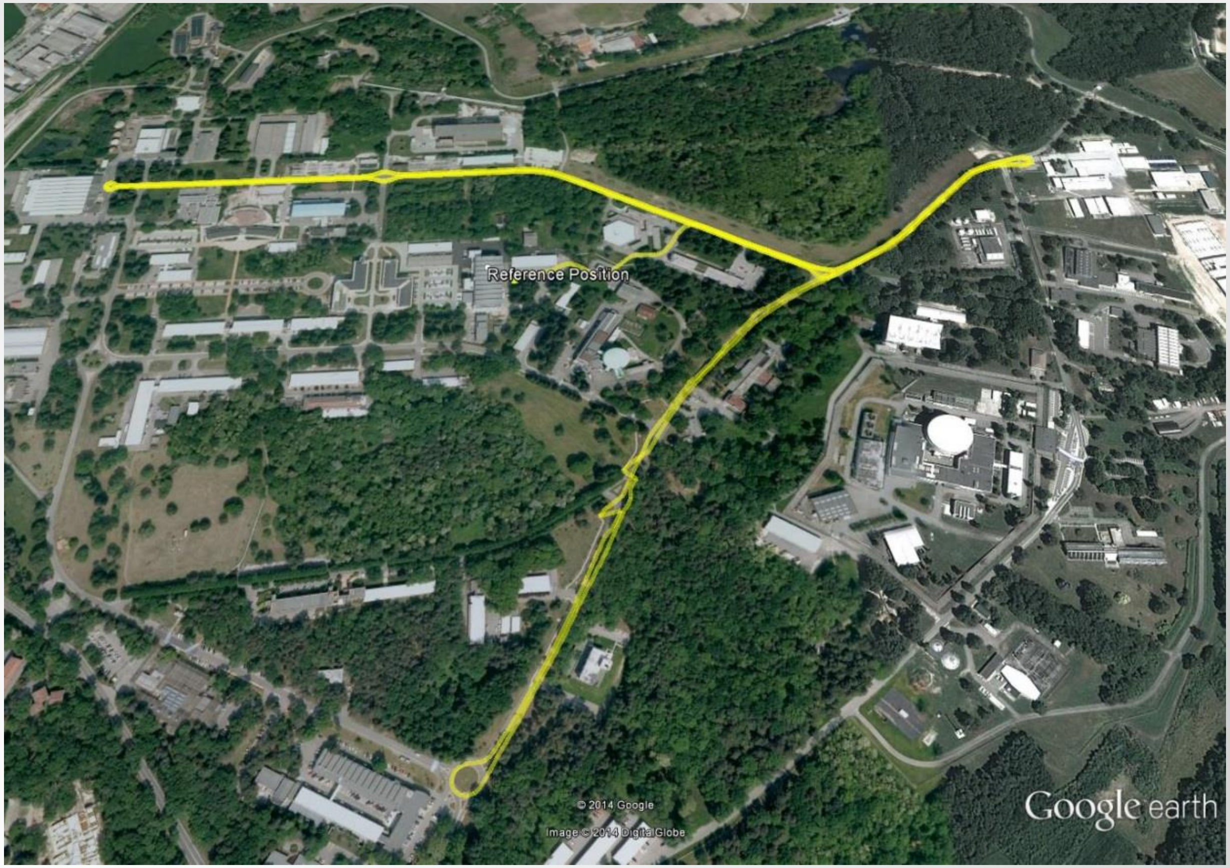
Jamming detection

- LOC drops as long as the jamming is detected then recovers to 100
- GNSS status is Implausible then Corrupt



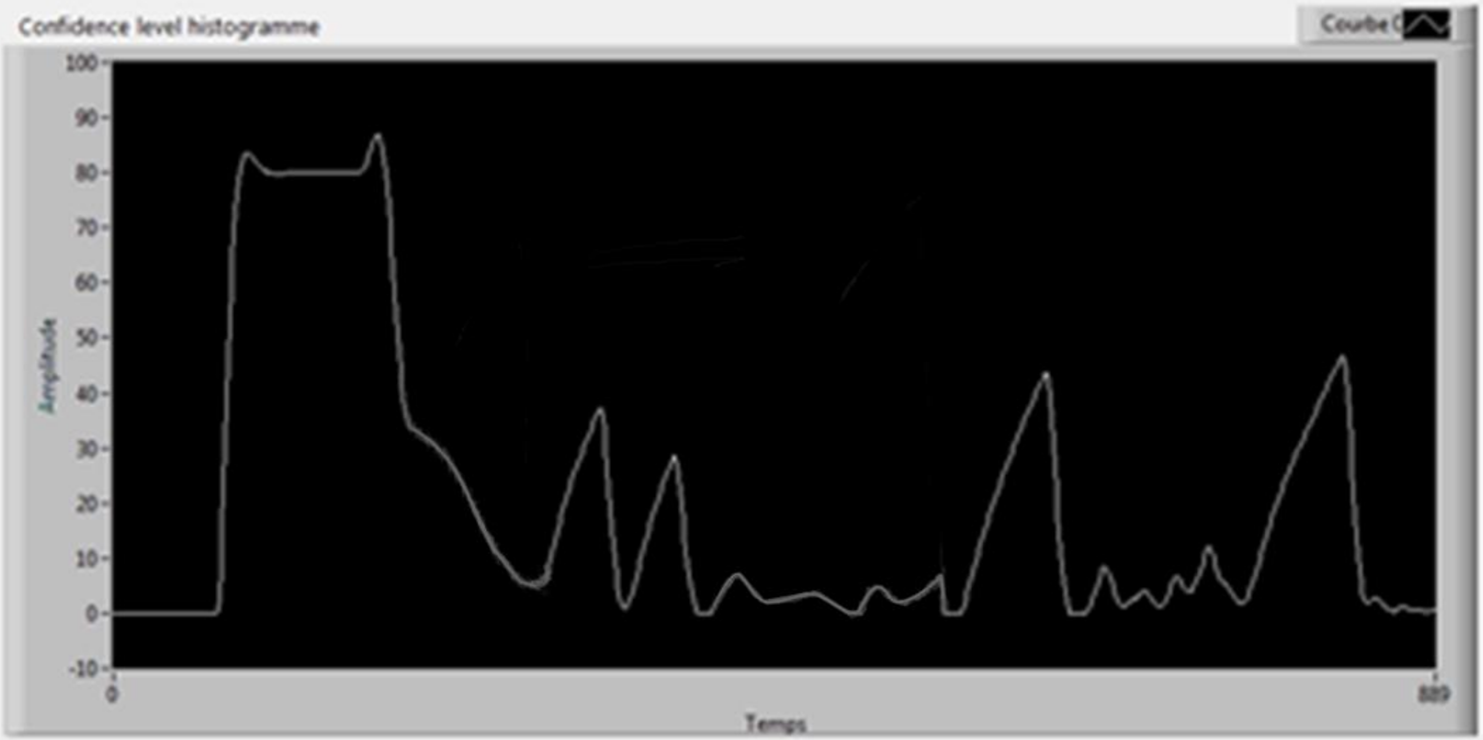
Dynamic tests setup : moving trajectory and static PVT module

- JRC carried out a data recording campaign using the dual frequency RF data grabber
- Reference trajectory has total length of 7.5 km and duration of about 16 minutes



Dynamic tests

- Inconsistencies between internal motion sensors and GNSS position
- LOC drops along the trajectory recorded on JRC site
- GNSS, magnetometer and accelerometer status are set to Corrupt



Agenda

TACOT Context & Solution

Technical developments

Test & Validation results

Conclusions

Conclusions

- TACOT is designed to detect attacks that can be implement ed with COTS equipment such as GNSS simulator or open source SDR platforms (BladeRF, HackRF).
- TACOT increases the attack cost.
- TACOT is designed to evolve according to the threat by implementing ad-hoc countermeasures.
- TACOT demonstrates that:
  - ✓ Its is technically feasible to provide an efficient solution to mitigate GNSS weaknesses impacts
  - ✓ Such a solution can be cost effective
  - ✓ Its solution provides an actual added value for ITS applications and can be tailored to various requirements

Conclusions

TACOT's outcomes:

- Is a first step security solution before the built-in defence mechanisms that will be included in Galileo (Galileo authentication)
- Is furthermore complementary to Galileo authentication service:
  - ✓ Provides a confidence level in a multi-constellation context
  - ✓ Do not limit its analysis to GNSS but can include all data sources (MEMs, barometer…)
  - ✓ Can detect meaconing and spoofing attacks

Way forward

FDC plans to manufacture an evaluation kit:

- ✓ This EK will contain hardware, software and documentation to evaluate Trusted PVT solution for ITS applications
- ✓ EK will be available Q4 2014
- ✓ If you are interested, send a mail to alexandre.allien@fdc.eu

Thank you for your attention

- Further information: pascal.campagne@fdc.eu