### GALILEO – secure positioning

14th PSCE Biannual Conference

Daniel Zerbib 19/05/2016



#### **AGENDA - IDEAS**

# GALILEO IS NOT a telecommunication system

#### **AGENDA - IDEAS**

- Telecom and geo localization
- Threats on traditional GNSS (GPS)
- Improvement thanks to Galileo & PMR
- Benefits for PPDR organizations
- The PRS4PMR project



#### Telecom and geo localization

### PPDR organizations use:

- telecommunications
- geo localization.

Thanks to PMR telecom are operational and secured.

Thanks to legacy GNSS (GPS)

Geo localization are operational but not secured

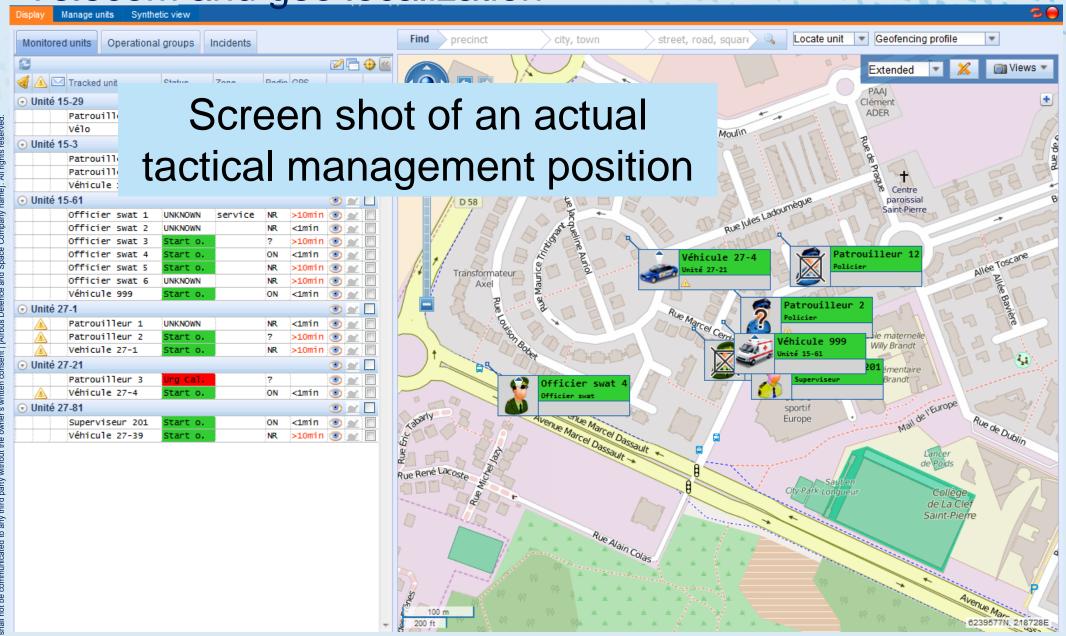


## geo localization for PPDR organizations

Use case

- Operational
- Tactical

Telecom and geo localization





#### Threats on traditional GNSS (GPS)

## Some defects and some new threats affects traditional GNSS (GPS)

- bad reception conditions
- intentional jamming "new" threat
- signal spoofing "new" threat



### Threats on traditional GNSS (GPS)

### Two samples of intentional jamming in France

Localization and <u>seizure</u> of a <u>GSM / GPS jammer</u> In Montélimar - France

Civil Aviation
Near Lyon-Bron airport
(France)
In <u>flight perturbation of</u>
the GNSS system on GPS
frequency 1575,42 MHz



#### Threats on traditional GNSS (GPS)

#### The jammer tool is

- Very simple to use
- Very cheap
- Difficult to detect





#### Improvement thanks to Galileo

=> Those threats may be mitigated thanks to Galileo technical solution

Galileo plans to propose 3 services levels
Open Channel - OC
Commercial service - CS
Public Regulated Service - PRS



#### Improvement thanks to Galileo

=> Those threats may be mitigated thanks to Galileo technical solution

Galileo proposes 3 different services Open Channel Service - OCS Commercial Service - CS Public Regulated Service - PRS

Both services will use Galileo and GPS satellites. Galileo uses 3 frequencies bands. PRS implements an authentication mechanism.



#### Improvement thanks to Galileo

The GSA (GNSS Security Agency) declares: (see <a href="http://www.gsa.europa.eu/security/prs">http://www.gsa.europa.eu/security/prs</a>

**PRS** is an encrypted navigation service more resistant to 'jamming', involuntary interference and 'spoofing'. Similar to other services, but some important differences:

- Ensures continuity of service to authorized users when access to other navigation services is denied.
- In cases of malicious interference, the PRS increases the likelihood of continuous availability of the Signal-in-Space.

#### Who is it for?

The PRS is primarily intended for use by EU Member State government agencies, including emergency services and police. Access to the PRS will be controlled through an encryption key system approved by Member States' governments.

PRS will be accessible to clearly identified categories of users authorized by the EU and participating States.

The PRS can provide support for a range of European public safety and emergency services as well as law enforcement, internal security and customs authorities:



#### PMR4PRS an implementation of Galileo PRS

A proof of concept has been specified, designed and developed, showing

- The feasibility (a global architecture has been designed)
- Synergy between PMR and PRS
- Definition of Use Cases relevant for current PMR users
- Complete Security Study of the proposed solution
- Cost Benefit Analysis (CBA) study
- Proposals for Draft Standards
- Performance Metrics Comparison between PRS alone and PRS+PMR
- The reliable PMR networks are able to ensure secure data transmission from/to the PRS receiver and a PRS Server, making if faster.
- The PMR users take benefit from the PRS geo localization advantages

