Benefits

- GNSS risk assessment methodology which includes risks with low probability but high impact
- Detection, identification, localisation and impact analysis of advanced and emerging RF interference, physical and cyber attacks
- Protective and mitigating solutions, including reconfiguration recommendations for RF interference, physical and cyber attacks
- Advanced security of information and data transmission
- Enabling of increased GNSS architecture intelligence reducing need for future additional redundancy

Partners

Contact

Nicolas Ribière-Tharaud

Atomic Energy and Alternative Energies Commission (Commissariat à l'Energie Atomique et aux Energies Alternatives)

Tel: +33 5 65 10 54 32

nicolas.ribiere-tharaud@cea.fr

Stephen Crabbe

Crabbe Consulting Ltd

Tel: +49 361 644 8842

stephen.crabbe@crabbe-consulting.com

www.progress-satellite.eu

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no 607679.

The project started in 2014 and will be completed in 2017.

Project flyer v3.0 (2017)

PROGRESS

Protection & Resilience of Ground Based infrastructures for European Space Systems

www.progress-satellite.eu

Motivation

Global Navigation Satellite Systems' (GNSS) Positioning, Navigation and Timing (PNT) products are used in almost all important sectors and this trend will continue.

These products' performances are characterised by accuracy, availability, continuity and integrity parameters as well as the confidentiality of data in motion and at rest.

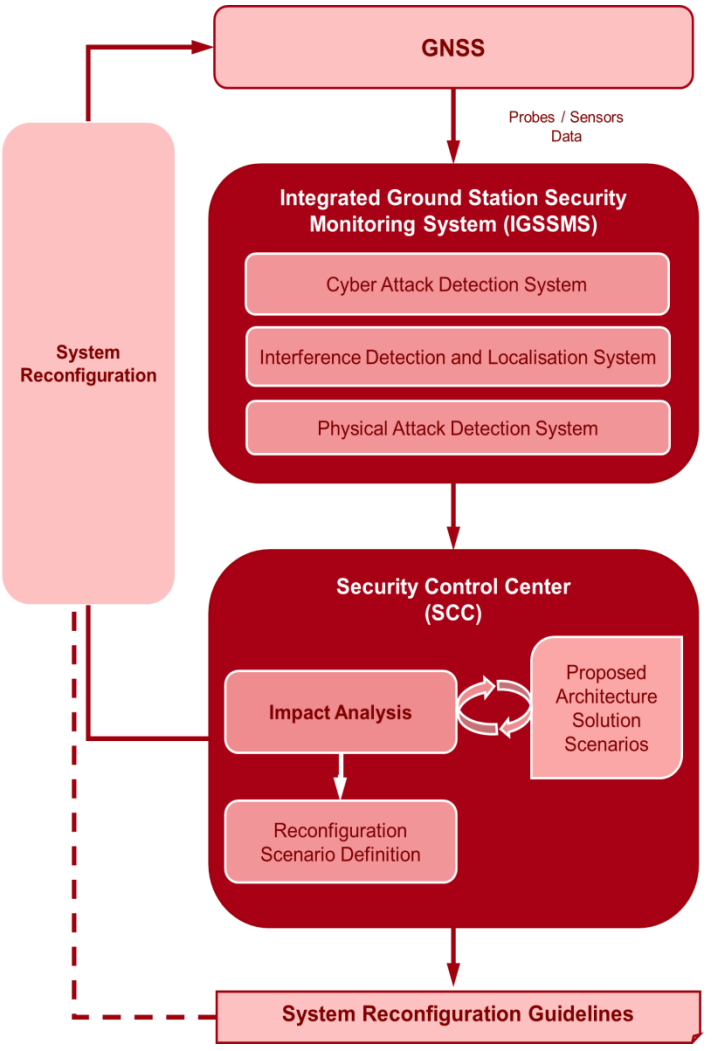
PROGRESS focuses on the detection and mitigation of intrusions to GNSS from highly educated attackers whose numbers may increase in the near future. The ultimate goal is to enable expanded intelligence in GNSS architectures so as to ensure uninterrupted performance of services. The potential impact of attacks will be reduced through protective solutions, attacks will be detected and analysed for impact and where necessary affected elements of the GNSS will be reconfigured.

Development objectives

- Holistic risk assessment tool
- Integrated Ground Station Security Monitoring System (IGSSMS) for Radio Frequency (RF) interference, physical and cyber attacks
- Threat protection and mitigation solutions
- "Security Control Centre (SCC)" for threat impact analysis and mitigation procedure propositions, incl. system reconfiguration
- IGSSMS and SCC prototype integration in Security Management Solution (SMS)
- Strengthened Telemetry, Tracking and Command (TT&C) links
- Testing and evaluation of the prototype
- Increased knowledge on GNSS societal impact

PROGRESS

Security Management Prototype



Key tools

- **Risk assessment methodology**

A holistic methodology enabling assessment of threat scenarios on GNSS, including the potential impact on society.

- **Security Management Solution (SMS)**

Centralized solution which is able to automatically detect attacks, analyse their impact and propose mitigation actions, including reconfiguration to ensure overall GNSS quality of service. The SMS will consist of:

- **Integrated Ground Station Security Monitoring System (IGSSMS)** with integrated detectors for Cyber-attacks (e.g. Distributed Denial of Service (DDoS) attacks); RF interference (e.g. jamming and spoofing); and physical attacks (e.g. explosive and high power microwaves).
- **Security Control Center (SCC)** to analyse the impact of events reported by IGSSMS and to trigger protection and/or mitigation procedures, including recommendations for system reconfiguration.

Our mission:

"Improved security for citizens, and enhanced competitiveness for the European space industry"