

**“PROGRESS: Protection and Resilience Of Ground based infRastructures for European Space Systems”**

This article was published in 20<sup>th</sup> European Critical Information Infrastructure Protection Newsletter (ECN) Vol. 9, Issue 1, p. 13 - as part of Network of Excellence FP7 Project [CIPRNET](#). The full newsletter can be downloaded from [here](#).

# PROGRESS: Protection and Resilience Of Ground based infRAstructures for European Space Systems

The FP7 PROGRESS project focuses on the security and resilience of ground based assets of Global Navigation Satellite Systems (GNSS)

The PROGRESS project is a new research project co-funded by the European Union under the EU 7th framework programme. The project is related to the security call topic SEC-2013.2.2-5: "Security of ground based infrastructure and assets operating space systems". The PROGRESS project started on May 1st 2014 and is due to be completed by the end of April 2017.

## Abstract

PROGRESS will focus on improving the security and resilience of Global Navigation Satellite Systems (GNSS) and its results will also be applicable to earth observation infrastructure and assets.

At the start of the project a generic GNSS system will be designed and its associated augmentation system will be assessed with regards to vulnerability from intentional malicious threats. In focus are threats, which are generally considered to have a low risk of occurrence but potentially very large impacts.

PROGRESS will concentrate on those threats that have the potential to increase in the coming years. The resulting prioritization of threats and scenarios will be used as input to develop a prototype Security Management Solution (SMS). PROGRESS SMS will be a centralized solution able to automatically detect malicious actions with a built-in reconfiguration capability to ensure the overall system Quality of Service.

The PROGRESS SMS will be composed of an Integrated Ground Station Security Monitoring System (IGSSMS) and a Security Control Centre (SCC). The IGSSMS will be an innovative monitoring solution for the detection of specific malicious types of attacks. The Security Control Centre will analyse the impact of the reported disturbances to the system performance and Quality of Service

(QoS) and will propose mitigation strategies, including automatic system reconfiguration.

The SMS will be developed with full consideration of present methods and measures for the security and resilience of complex interconnected space control ground station networks by present operators.

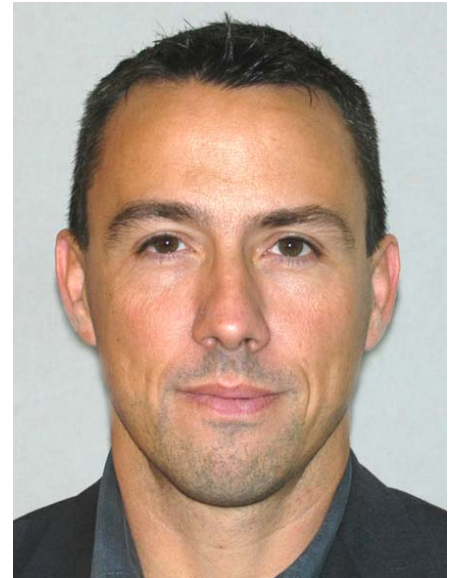
The high quality of the developed solutions will be assured by a consortium consisting of a number of experienced partners joining:

- The operator of the Galileo Control Centre in Oberpfaffenhofen,
- The EU leader for satellite systems,
- A manufacturer and world distributor of security solutions,
- Leading applied research institutes,
- Specialized SMEs,
- And a research institution specialized both in security and social aspects.

## Context

The main ideas leading to the PROGRESS project is related to the critical importance of GNSS to global society as Global Navigation Satellite Systems (GNSS) based services are used in an ever increasing number of applications, including a large number of critical applications for positioning, navigation and timing (PNT) services.

GNSS time references that are used for example to precisely synchronise critical networked infrastructures, such as: power distribution; fixed and wireless networks, including broadband access networks to the Internet; transportation networks - sea, air, rail and road e.g. for automatic tolls; and financial services e.g. for banking and the stock markets. A number of reports point towards the conclusion that GNSS should be classified as a critical infrastructure itself with the appropriate level of protection.



**Nicolas Ribière-Tharaud**

Nicolas Ribière-Tharaud is the PROGRESS project coordinator. He is involved in the field of critical infrastructure vulnerability and protection. He is also an expert in the field of electromagnetic effects and their consequences.

e-mail:  
[nicolas.ribiere-tharaud@cea.fr](mailto:nicolas.ribiere-tharaud@cea.fr)

CEA,DAM,GRAMAT,  
F-46500 Gramat, France

Based on the experience and needs of ground station operators and architects, the following main threats have been identified in [1]:

- Data corruption
- Ground facility physical attack
- Spoofing (Masquerade)
- Jamming
- Replay
- Software/HW threats
- Unauthorized access
- Natural disasters

The consortium plan to focus on threat assessment, detection, protection and mitigation strategies, which can be grouped into three categories: cyber-attacks, RF Interference attacks and physical attacks.

These threats have been focused on because:

- a. New technologies are available on the market or technical evolutions in general which are currently evaluated at research level, but require further assessment with specific focus from the security point of view.
- b. In the past, threats, which were previously analysed as having a low probability of occurrence, were potentially not taken into account in the system design to a large extent, regardless of the impact they could potentially have on the system or on the service provided to end-users. This

is particularly true in the case of terrorism.

- c. Europe needs to have the methods and tools to protect its GNSS critical infrastructure and the services expected by its citizens from the threats focused on.

## Objectives

PROGRESS has 7 main objectives that are described below:

1. Development of risk assessment methodology and tools to assess threats on generic GNSS ground based infrastructure and assets operating space systems and their secure communication links to satellites and a prioritization of the threats for which detection, protection and mitigation solutions should be developed
2. Development of detection solutions for: Cyber-attacks (DoS attacks and spoofing); RF interference (Jamming and Spoofing) detection and localization; and physical attacks (explosive and high power microwaves). These detectors will be integrated in an Integrated Ground Station Security Monitoring System (IGSSMS).
3. Development of threat protection and mitigation solutions for the cyber, RF interferences and physical attacks: guidelines and proposed best practices; architecture solutions; and

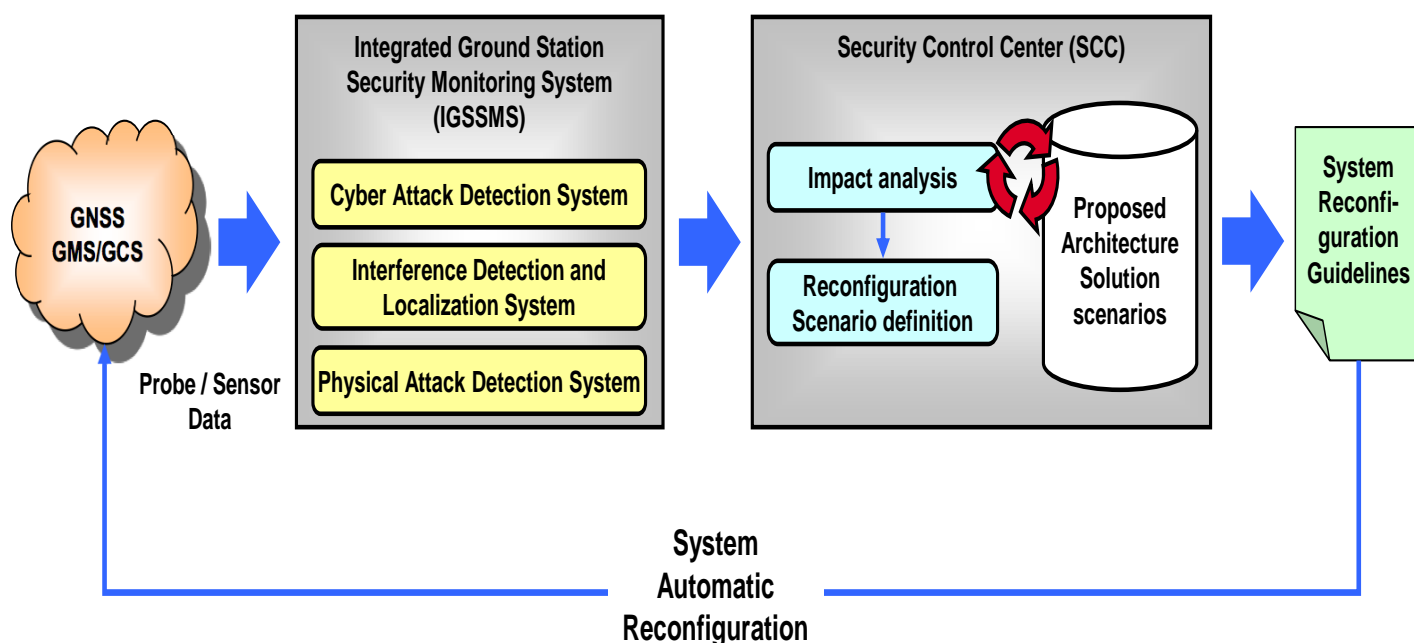
The PROGRESS project aims at delivering a **prototype Security Management Solution** (PROGRESS solution) composed of an Integrated Ground Station Security Monitoring System and a Security Control Centre. The prototype will be developed on the basis of a generic architecture but with full consideration of present methods and measures for the security and resilience of complex interconnected space control ground station networks

The project will lead to a limitation of the impact of accidents/attacks by providing knowledge for more resilient future GNSS systems and ground stations.

PROGRESS has received funding from EU FP7 under grant agreement Contract No. 607679

specific countermeasures and

PROGRESS main concept



procedures to be implemented once an attack(s) is identified.

4. Development of a Security Control Centre (SCC) to analyse the impact of detected threats and to propose mitigation procedures, including system reconfiguration.
5. Development and integration of a prototype to prove the PROGRESS innovative security concepts, including the IGSSMS and SCC. This aspect includes the development of tools to generate the attack scenario addressed in the project.
6. Testing and evaluation of the prototype Security Management Solution through the PROGRESS prototype testbeds.
7. Further development of strategies to exploit the results of the project in commercial products and services.

PROGRESS objectives include the development of a risk assessment methodology, attack detection and protection means, with respect to threats that have the potential to increase in the coming year. The innovative concepts are assessed through tests carried on the PROGRESS solution prototype.

## The Partners

CEA (France), THALES ALENIA SPACE (France, Italy, Spain), Fraunhofer EMI (Germany), DLR-GfR (Germany), CRABBE CONSULTING LTD (Germany), SECURITON (Germany), DECISIO (The Netherlands), University of Ljubljana (Slovenia), QASCOM (Italy).

If you would like to know more about PROGRESS please visit regularly our website at [www.progress-satellite.eu](http://www.progress-satellite.eu)

## References

[1] CCSDS 350.1-G-1, Security Threats against Space Missions, Informational Report, Issue 1, October 2006

*"The information appearing in this document has been prepared in good faith and represents the opinions of the authors. The authors are solely responsible for this publication and it does not represent the opinion of the European Commission. Neither the authors nor the European Commission are responsible or any use that might be made of data including opinions appearing herein.*