"PROGRESS project: Improving the resilience of satellite ground station infrastructures: High power microwaves threat detection system and protection strategies"

This paper was published in *2016 International Symposium on Electromagnetic Compatibility - EMC EUROPE*, IEEE Catalog Number CFP1606F-ART, 978-1-5090-1416-3, Online ISSN 2325-0364

Link to the article abstract in IEEE Xplore: http://ieeexplore.ieee.org/document/7739208/

DOI: 10.1109/EMCEurope.2016.7739208

PROGRESS Project: Improving the Resilience of GNSS Ground-Based Infrastructures

HPM Threat Detection System and Protection Strategies

S. Schopferer[1], C. Michalski[1], M. Schimmerohn[1], N. Ribière-Tharaud[2], J.-C. Joly[2], A. Rouquand[2], S. Crabbe[3]
[1] Fraunhofer Ernst-Mach-Institut (EMI), 79104 Freiburg, Germany, sebastian.schopferer@emi.fraunhofer.de
[2] CEA, DAM, F-46500 Gramat, France
[3] Crabbe Consulting Ltd, 99084 Erfurt, Germany

***Abstract*—The FP7 project PROGRESS aims at improving the security and resilience of European space systems such as GNSS. It focuses on the detection and mitigation of attacks on ground-based infrastructures from highly educated attackers whose numbers may increase in the near future. This paper outlines the main project objectives and presents the work achieved in this framework considering the High Power Microwaves (HPM) threats. Development and characterization of a HPM detector are reported as well as the work carried out in terms of infrastructure protection.**

Keywords—High power microwaves (HPM), threat detection, protection, resilience, critical infrastructure, GNSS

I. INTRODUCTION

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 purposes. It is assumed that a malfunctioning of GNSS would cause instant problems in many sectors with high economic and societal impact [1]. PROGRESS[1] aims at improving the security and resilience of GNSS by enhancing the protection of ground-based infrastructures and assets [2]. At the start of the project a generic GNSS was defined and has been 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 concentrates on threats that have the potential to increase in the coming years:

- Physical attacks on ground facilities, including explosive attacks and High Power Microwaves (HPM) attacks,
- RF spoofing and jamming,
- Cyber-attacks.

The resulting prioritization of threats and scenarios has been used as input to develop a prototype Security Management Solution (SMS).

[1] Protection and Resilience Of Ground based infRastructures for European Space Systems

PROGRESS SMS (Fig. 1) is a centralized solution able to automatically detect malicious actions, analyze the impact and, where necessary, propose actions for system reconfiguration to ensure the overall GNSS Quality of Service. In addition, protective tools are developed to help build less vulnerable assets, in order to reduce the potential impact of attacks. While the overall project addresses a wider range of threats, this paper focuses on the detection and mitigation of HPM attacks.

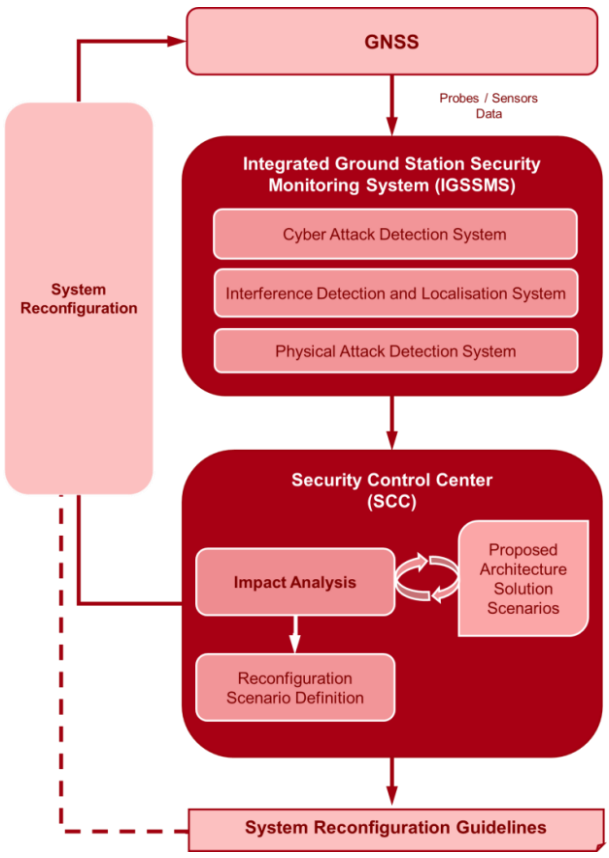

Fig. 1. PROGRESS Security Management Prototype.

II. PROGRESS SMS CONCEPT

The PROGRESS SMS is composed of an Integrated Ground Station Security Monitoring System (IGSSMS) and a Security Control Centre (SCC). The IGSSMS is an innovative monitoring solution for the detection of specific types of attacks. Together with traditional monitoring systems (CCTV, intrusion alarm…) it can provide a more complete picture of the security situation. The Security Control Centre role is to analyze the impact of the reported disturbances on the system performance and Quality of Service and to propose mitigation strategies, including semi-automatic system reconfiguration.

III. THREAT DETECTION

A. *HPM Threat*

Intense electromagnetic fields with the capability to damage or upset electronic systems are called high-power electromagnetic (HPEM) environments [3]. They are usually classified by spectral attributes into narrowband environments, referred to as high-power microwave (HPM), and wideband environments. A HPM pulse consists of some hundred cycles of a single frequency, with a pulse repetition rate up to several hundred Hertz. Portable HPM sources typically operate in the frequency range between 0.5 GHz and 8 GHz. With a powerful generator and a sufficiently large antenna gain far voltages[2] in the order of several Megavolts are possible.

Intentional electromagnetic interference (IEMI) denotes the malicious application of intense electromagnetic fields in order to incapacitate electronic systems. Several IEMI attacks with criminal background have been reported in the past [4]. Depending on the generated field strength at the position of the target system the following effects can occur: (1) interruption of communication due to disturbance of RF receivers, (2) transient or semi-permanent malfunction, which may require a system reset, (3) permanent damage due to destruction of semiconductor components. Without appropriate detection systems, linking these consequences to an IEMI attack may not be always obvious. Thus, detection of this threat appears as a first protection level in order to ensure appropriate reactions in case of such events. This is especially important for unmanned ground stations, where otherwise, for example, a loss of communication links could not be easily attributed to an attack. Several approaches for detecting HPM attacks are known from literature [5-7] and the PROGRESS solution is based on a similar approach.

B. *HPM Detector*

The IGSSMS includes a detection system dedicated to physical attacks (HPM and explosive attacks), the so-called Physical Attack Detection System (PADS). Suitable detection techniques developed within the PROGRESS framework have been integrated into an autonomous sensor node (Fig. 2). The electronics is enclosed in a rugged EM-shielded box, and the sensors are mounted on top of it (Fig. 3). The sensor node contains two signal-processing chains, one for detecting blast waves from explosions (which will not be discussed in this paper) and one for detecting HPEM fields. A shared controller provides the interface to the IGSSMS server for sending alert messages and for configuration. Multiple autonomous nodes can be distributed across the monitored site, connected to the server via fiber-optic links.

The developed HPM detector consists of electromagnetic sensors, an analog front-end and a digital signal processing part. Four cavity-backed spiral antennas are used as the electromagnetic sensors, oriented in orthogonal directions for the purpose of attack direction finding. The antennas are designed to cover the frequency range of [0.5 – 8 GHz] with a 10dB-beamwidth of about 140°. The analog front-end uses a logarithmic detector with large dynamic range (> 60 dB) and fast rise-time (< 20 ns) combined with attenuators and limiters. The detector generates the envelope signal of incident HPM pulses and drives it to an analog-to-digital converter. A subsequent FPGA-based processing module is used for real-time pulse feature extraction (amplitude, width, shape, repetition rate). Based on the combined pulse data from all four channels, the direction finding and intensity determination is performed.

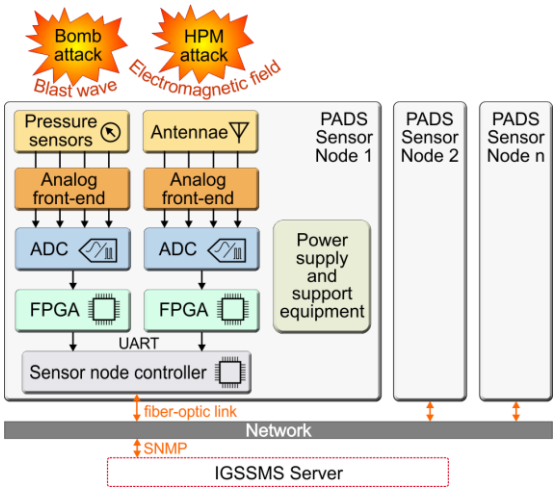

Fig. 2. PROGRESS Physical Attack Detection System sensor node.

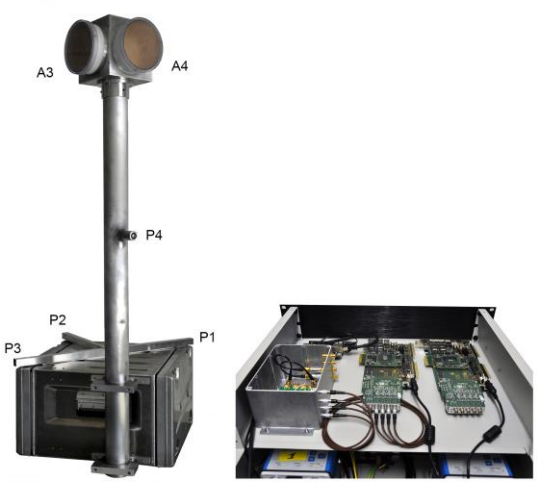

Fig. 3. Left: prototype of the PROGRESS PADS electronics box with mounted pressure sensors (P*n*) and antennas (A*n*). Right: view into the 19-inch drawers.

[2] "far voltage": range-normalized radiated E-field, $V_{far} = r \cdot E_f$

C. HPM Detector Characterization

In order to assess the HPM detector prototype developed by Fraunhofer EMI, tests have been carried out in the CEA Hypérion test facility in Gramat (France). The purpose of the measurement campaign was to test the HPM detection system under realistic conditions, i.e. in an intense electromagnetic environment. The following points were targeted to be verified / achieved:

- The system shall be able to detect IEMI threats produced by various types of HPM sources [8].
- The system shall be able to measure the intensity of the HPM attack, and to estimate the direction to the source.
- The system shall be robust against the detected threats, i.e. it must not be damaged even at very high field strength.

During the test campaign, the antenna array was placed on a tripod at different distances to the sources. In an exhaustive approach, several sources have been used (Fig. 4) in the frequency range of [200 MHz – 9 GHz]. The radiated electromagnetic field amplitudes were in the range of 10 V/m to a few hundred kV/m with different kinds of frequency spectrums (ultra-wide band, wide band, narrow band and ultra-narrow band). The measurements and assessments showed that the expected performances can be met with this type of detection system (Table I).

An important outcome of the measurements with ultra-wide band sources was the response of the detection system to pulses which are shorter than the detector's rise-time. As expected, in this case the full height of the pulse is not measured, which leads to an underestimation of the actual field strength. To account for this effect, a correction procedure based on the shape and width of the envelope signal has been identified, which can be applied in the intensity calculation.

For all high power sources used in the test campaign the RF signal and detector response have been recorded with high-speed digitizers. Based on these exemplary waveforms an attack scenario generation tool is being developed to allow the simulation of HPM attacks for the upcoming testing activities of the PROGRESS SMS prototype.

TABLE I. REQUIREMENTS FOR HPM DETECTION PERFORMANCE

Parameter	Requirement	Verified
Frequency range	500 MHz – 8 GHz	yes
Polarization dependence	independent	yes
Direction finding accuracy	± 15°	partly[a]
Dynamic range	60 dB	yes
Min. pulse width	20 ns	yes
Max. pulse repetition rate	1 kHz	yes[b]

[a.] In anechoic chamber, to be verified in real environment.

[b.] Verified by bench test, not with HPM source.

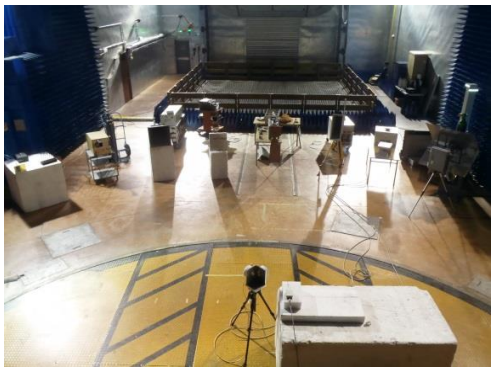

Fig. 4. Characterization of the detecting device to a sample group of electromagnetic sources (HPM and low power sources) in Hypérion (the CEA-Gramat large test facility dedicated to IEMI).

IV. PROTECTION BY DESIGN

The detection system in connection with the Security Control Centre and its associated capabilities for system reconfiguration is answering partly to the protection needs. In order to reduce risk and to improve the GNSS system resilience, a set of complementary protection tools is studied in the project, for instance tools such as:

- New encryption tools dedicated to the uplink (communication between ground-based infrastructure and satellites),
- Training of people in charge of security for better understanding and actions for these unusual threats,
- Guidelines leading to strengthened design of infrastructures, applicable to new ones but also to existing ones.

Protection by design against HPM includes protections to HPM front-door and back-door attacks. Back-door attacks are assessed in the PROGRESS project through numerical simulations based on a finite differences in time domain code. The main objective is to define protection that can be easily implemented on existing and future buildings. Simulations within the PROGRESS framework have been carried out on an actual building. A numerical model has been established from this building (Fig. 5) including details such as the hardware implemented in server rooms dedicated to operations similar to those used for GNSS. The building model has been illuminated by an electromagnetic source, located on the road nearby and operated at the frequency f = 1GHz. Fig. 6 shows attenuations increase of at least 11 dB inside the server rooms of a protected building compared to an unprotected one. The results show that the improvement of protection can be derived from the implementation of simple rules such as:

- Adding a conducting grid mesh between the car park/road and building,
- Using glasses with embedded thermal protection,
- Using reinforced concrete walls with a high density of metal bars,
- Increasing the distance between car park/road and building.

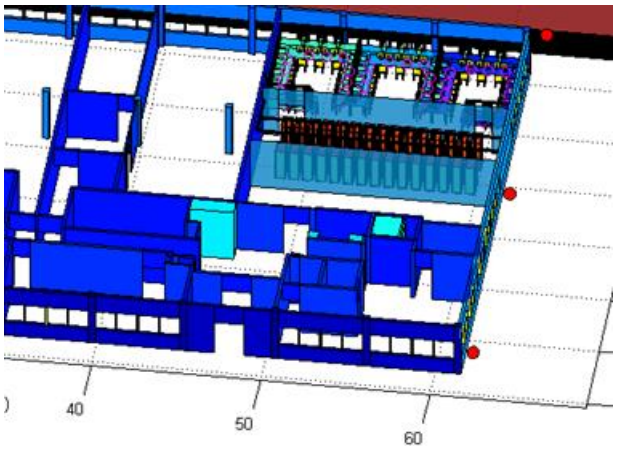

Fig. 5. Numerical model for electromagnetic assessments. Upper right rooms include servers similar to those used for GNSS operations.

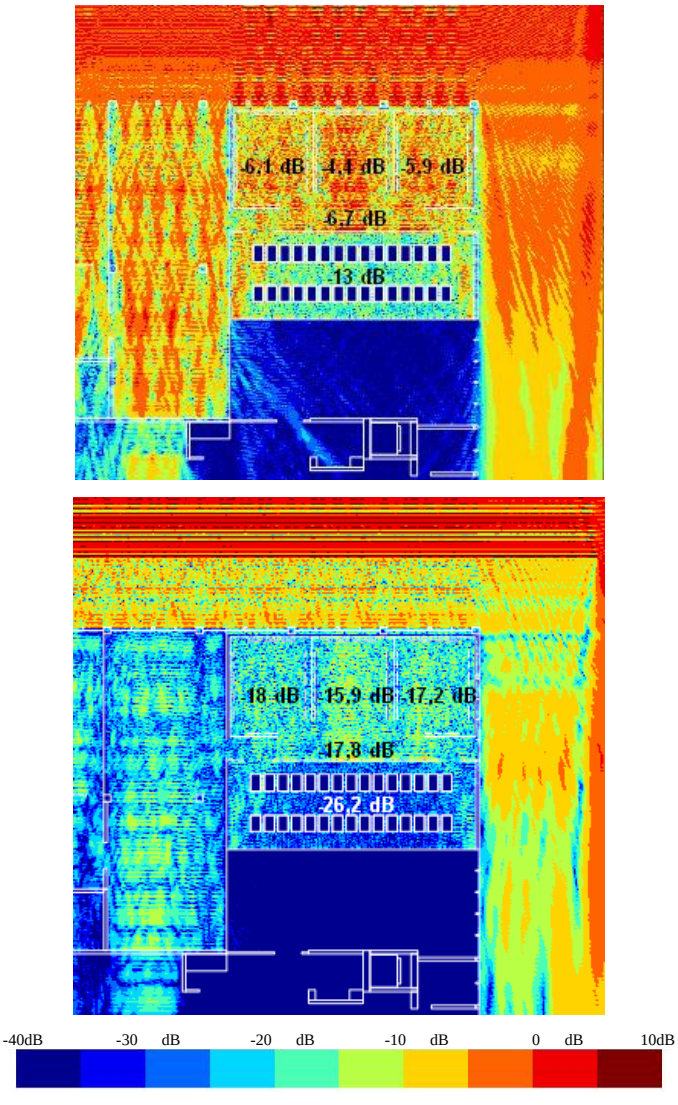

Fig. 6. Attenuation of the electromagnetic field radiated inside the building by a source located in the nearby car park. Unprotected building (top), Building with thermal protection glasses and a grid mesh between building and road (bottom).

The numerical approaches contribute to the project objectives in several aspects: (1) assessing the threat level, (2) enabling to provide guidelines for implementing protection by design, and (3) providing data related to the relevant scenarios used for testing the SMS prototype.

V. Summary

In the framework of the PROGRESS project a detection system for different kinds of threats against GNSS ground-based infrastructures has been developed. Our approach for the detection of HPM attacks has been detailed in this paper and results from the detector characterization have been presented. Numerical simulations for the assessment of EM field attenuation inside buildings have been performed, which allow to compare the shielding effectiveness of several protective measures. A set of guidelines for improved infrastructure protection against IEMI is derived from the results. Further work in the PROGRESS project will focus on the integration and the evaluation of the whole SMS prototype.

Acknowledgment

PROGRESS has received funding from EU FP7 under grant agreement Contract No. 607679. 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 for any use that might be made of data including opinions appearing herein. The project started on 1st May 2014 and is due to be completed by 30th April 2017.

References

[1] PROGRESS Deliverable D1.1 - Economic & societal framework. SP1-Cooperation-607679-PROGRESS report, 2014. http://www.progress-satellite.eu/

[2] N. Ribière-Tharaud, “PROGRESS: Protection and Resilience Of Ground based infRastructures for European Space Systems”, European CIIP Newsletter Volume 9 issue 1, 2015.

[3] IEC 61000-1-5, Technical report, “Electromagnetic compatibility (EMC) – Part 1-5: General – High power electromagnetic (HPEM) effects on civil systems”.
IEC 61000-2-13, International standard, “Electromagnetic compatibility (EMC) – Part 2-13: Environment – High-power electromagnetic (HPEM) environments – Radiated and conducted”.

[4] F. Sabath, “What can be learned from documented intentional electromagnetic interference attacks?”, General Assembly and Scientific Symposium, 2011 XXXth URSI.

[5] C. Adami et al., “HPM detection system for mobile and stationary use”, EMC Europe 2011.

[6] D.B. Jackson, T.R. Noe, G.H. Baker III, “High dynamic range, wide bandwidth electromagnetic field threat detector”, in Ultra-Wideband, Short-Pulse Electromagnetics 10, pp. 355-368, Springer, 2014.

[7] C. Kasmi, J. Lopes Esteves, M. Renard, “Design of an IEMI-attack detector involving the internal resources of a COTS computer”, Future Security 2014.

[8] A. Kreth, T. Peikert, B. Menssen and H. Garbe, “Characteristic HPEM Signals for the Detection of IEMI Threats”, in Ultra-Wideband Short-Pulse Electromagnetics 10, pp. 379-392, Springer, 2014.