# Affordable IEMI detection system for critical infrastructure protection

Ribière-Tharaud N., Albuisson N., Joly J.-C.,
CEA, DAM, GRAMAT,
F-46500 Gramat, France

Schutz M., Lenoir B.,
INOVEOS SARL
F-19100 Brive-la-Gaillarde, France

***Abstract*—**This paper presents an Intentional Electromagnetic Interference (IEMI) detector developed with cost and performance requirements for the protection of civilian critical infrastructures (CCI). The developed sensor is described and assessments for efficient deployment are presented.

Critical Infrastructure, IEMI, Vulnerability, Detection, Protection (key words)

## I. INTRODUCTION

Several projects have been funded in order to improve the security of CCI considering events such as terrorist attacks, natural events and others. These projects raised the need of monitoring solutions involving several kinds of sensors and among them IEMI detectors have been studied [1][2]. Some have also been developed and tested in other frameworks, such as the TotEM$^{TM}$ and the EMPRIMUS detectors [3][4]. The approach proposed here is to provide a compact IEMI sensor with good abilities dedicated to signal discrimination but at low cost in order to facilitate wide deployment on CCI.

## II. IEMI DETECTION SOLUTION

### *A. IEMI detector requirements*

An efficient protection system has to raise an appropriate level of alarms. In the case of IEMI, a wide variety of aggressions (waveforms, frequencies, repetition rate, electromagnetic field levels…) have to be considered [5] and it is also known that the significant growth of electromagnetic applications in the civilian domain is feeding a risk of confusion for threat detection purposes. A balance has thus to be found between having an accurate electromagnetic measurement device (following Table 1 requirements) and an affordable device as a subpart of a wider security solution involving numerous sensors.

TABLE I. MAIN TECHNICAL REQUIREMENTS

| ***Parameter*** | ***Value /Characteristics*** |
|---|---|
| Frequency | [0.1 – 8]GHz |
| Repetition rate | Monopulse to ~100kHz |
| Waveform discrimination | UWB, Wide Band, NarrowBand, bandwidth << 1% |
| Electric field level | [10 V/m – few 10$^{th}$ kV/m] |
| Pulse length | 1ns to 1 ms |

### *B. Low cost IEMI detector principle*

The principle is based on cheap components coming from the civilian electronic market associated to measurements on several frequency channels (Figure 1) [6]. The prototype tests have shown that requirements are met.

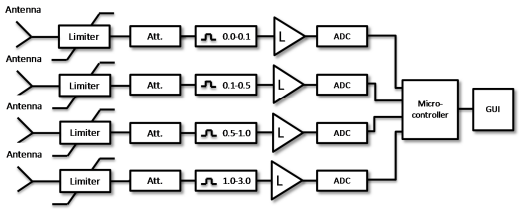


Figure 1. 4 channel detector example.

Figure 2. 4 channels IEMI detector.

## III. DEPLOYMENT ON CCI

The relevance of the detector and of its deployment has been studied through numerical and experimental assessments. Scenarios involving relevant buildings and IEMI sources have been simulated using FDTD algorithms and the results are compared and used for establishing deployment recommendations in terms of number and locations.

## REFERENCES

[1] N. Ribière-Tharaud, and al., "PROGRESS project: Vulnerability and protection of GNSS ground-based infrastructures" EuroEM 2016, London, July 2016.
[2] J. F. Dawson, and al., "A Cost-Efficient System for Detecting an Intentional Electromagnetic Interference (IEMI) Attack", International Symposium on Electromagnetic Compatibility (EMC Europe 2014), Sweden, September 2014
[3] D. Herke, L. Chatt, B. Petit and R. Hoad, "Lessons Learnt From IEMI Detector Deployments", EuroEM 2016, London.
[4] Emprimus, LLC, www.emprimus.com
[5] A. Kreth, and al., "Characteristic HPEM Signals for the Detection of IEMI Threats", Ultra-Wideband, Short-Pulse Electromagnetics, 10, Springer, 2014
[6] Nicolas Ribière-Tharaud, "Ultra Wideband signal detection", European Patent EP3157181B1, December 2017.