IEMI Detection

Setting up relevant detection threshold

Ribière-Tharaud N., Joly J.-C., Laparro C.
CEA, DAM, GRAMAT
F-46500 Gramat, France
nicolas.ribiere-tharaud@cea.fr
Schutz M., Lenoir B.,
Inoveos
F-19100 Brive-la-Gaillarde, France

Abstract— This paper presents the work carried out in order to set up the detection threshold (DT) of an Intentional Electromagnetic Interference (IEMI) detector developed with cost and performance requirements for the protection of civilian critical infrastructures (CCI). Considering actual electromagnetic environments (EME), the chosen DT has to ensure efficient detection and to avoid multiple false alarms.
(key words) Critical Infrastructure, IEMI, Vulnerability, Detection, Threshold detection level, Protection.

I. INTRODUCTION

Several research projects have been funded 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™ [3] and the EMPRIMUS [4] detectors. The prototype presented in [5] is a compact IEMI sensor with good abilities dedicated to signal discrimination but at low cost in order to facilitate wide deployment on CCI. This paper aims at describing the whole process established to take into account the electromagnetic environments (EME) and to reduce the false alarm rate.

II. DETECTION SYSTEM

The considered detection system includes four high dynamic range RF receiving channels combined to protection components in order to resist to high-level electromagnetic fields. Each channel covers one part of the detector whole frequency range (0.1 – 8GHz). Received signal on each channel is sent to a signal-processing unit. Signal processing allows recovering detected signal level (few V/m up to few 10^{th}kV/m), repetition rate (mono pulse to ~100kHz), pulse width (1ns to 1ms), and impacted frequency channels.

III. SIGNAL DISCRIMINATION

Wide detection capabilities and resilience are mandatory detection system characteristics. However, in an increasingly saturated EME it is also required to be able to discriminate the variety of possible IEMI [6]. The signal discrimination is achieved through two complementary approaches:

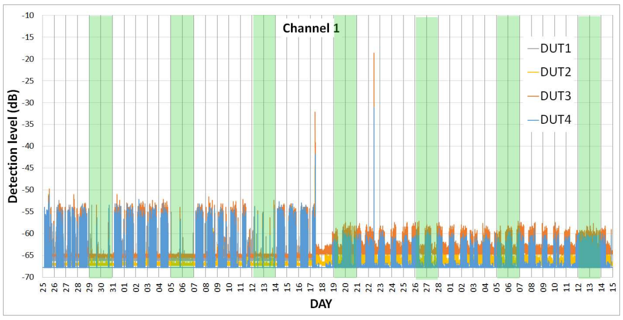

Figure 1. Detected EME in working area, 4 Detectors Under Test (DUT). Green frames highlight days off

1) EME characterization done by the detector itself. It consists in a specific detection mode where the electromagnetic field viewed from each detector channel is stored on long user-defined period (Fig. 1). A threshold can then be chosen at a level greater than the maximum electromagnetic field stored avoiding thus to trigger alarms related to the ambient electromagnetic field.

2) A rudimentary waveform analysis based on a set of criteria (electric field level, repetition rate, pulse duration, bandwidth). The detector is in the detection mode. In case of detected signal, an analysis relying on comparison of the measured signal characteristics to waveforms considered as unusual is achieved to trigger or not the alarm.
Both approaches have been assessed in laboratory and real conditions (several weeks, Fig. 1 and 2) to confirm the approaches relevance in terms of low false alarm rate and detector performances and repeatability.

Figure 2. Testing detector results dispersion

REFERENCES

[1] N. Ribière-Tharaud, and al., “PROGRESS project: Vulnerability and protection of GNSS ground-based infrastructures” EUROEM, London, 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, London, 2016
[4] Emprimus, LLC, www.emprimus.com
[5] N. Ribière-Tharaud, and al., “Affordable IEMI detection system for critical infrastructure protection”, AMEREM, Santa-Barbara, 2018
[6] A. Kreth, and al., “Characteristic HPEM Signals for the Detection of IEMI Threats”, Ultra-Wideband, Short-Pulse Electromagnetics, 10, Springer, 2014