

EMC Europe 2013

September 2-6, 2013 - Brugge, Belgium

Location : Crowne Plaza Brugge
Burg 10
Brugge 8000 Belgium

Monday, 02/Sep/2013 9:00 -12:30

Workshop

on EM attacks on critical infrastructures: Focus on the European projects

SECRET and STRUCTURES

STRUCTURES *Strategies for The impRovement of critical infrastrUCTure Resilience to Electromagnetic attackS*

SECRET *SECurity of Railways against Electromagnetic aTtacks*

Summary: Security and quality of life in industrialized countries depend on continuous and coordinate performance of a set of infrastructures (energy systems, ICT systems, transportation, etc.) which can be therefore defined as critical infrastructures (CI). In parallel, these infrastructures include a large number of telecommunication, command-control, electronic and informatics systems and subsystems vulnerable to electromagnetic interferences (HPM and EMP).

With the proliferation of wireless solutions for the general public, access to ElectroMagnetic (EM) emission systems has been democratized. With relatively basic electronics knowledge and the performance of electronic components and antennas available on the open market, these emission devices can be combined with amplifiers to increase the capacity of EM attacks.

The projects "SECRET" and "STRUCTURES" aim to study the potential impacts of EM attacks on such CIs, at assessing their impact for our defence and economic security, and at identifying innovative awareness and protection strategies and technologies.

This workshop will present the scopes of both projects, their respective approaches to assess the risks on CIs and the protection solutions studied.

Organizers: Virginie Deniau, IFSTTAR , 20 rue Elisée Reclus 59650 Villeneuve d'Ascq, France, virginie.deniau@ifsttar.fr, + 33 3 20 43 89 91,

Marco RIGHERO, ISMB, via Pier Carlo Boggio, 61 - 10138 Torino, Italy, righero@ismb.it, +39 011 2276 713

Program and speakers

- 9:00 - 9:10:** Introduction of the workshop
Aldo Bonsignore-IDS-a.bonsignore@idscorporation.com and,
Virginie Deniau-IFSTTAR-virginie.deniau@ifsttar.fr
- 9:10-9:40:** General presentation of STRUCTURES
(Marco Righero-ISMB)
- 9:40-10:10:** General presentation of SECRET
(Virginie Deniau-IFSTTAR)
- 10:10-10:40:** IEMI threats analysis conducted in STRUCTURES
(Stefan van de Beek – UT University of Twente)
- 10:40-11:00:** Coffee break
- 11:00-11:30:** Analysis and modelling methods assessment performed in STRUCTURES
(Kai Rathjen – HSU Helmut Schmidt University)
- 11:30-12:00:** EM attack scenarios and devices considered in SECRET
(Henri Philippe – SNCF - henri.philippe@sncf.fr , Flavio Canavero – Polito-
flavio.canavero@polito.it)
- 12:00-12:30:** Detection of EM attacks: approaches developed in SECRET
(Marc Heddebaut –IFSTTAR-marc.heddebaut@ifsttar.fr)

Abstract of the presentations

1- General presentation of STRUCTURES

(Marco Righero – ISMB Istituto Superiore Mario Boella)

Security and quality of life in industrialized countries depend on continuous and coordinate performance of a set of infrastructures (energy systems, ICT systems, transportation, etc.) which can be therefore defined “critical infrastructures”. The project “STRUCTURES” aims at analysing possible effects of Intentional ElectroMagnetic Interference (IEMI) attacks on such critical infrastructures; at assessing their impact for our defence and economic security; at identifying innovative awareness and protection strategies; and at providing a picture for the policy makers on the possible consequences (e.g. inputs to update standards).

2- General presentation of SECRET

(Virginie Deniau-IFSTTAR)

SECRET addresses the protection of railway infrastructure against Electromagnetic (EM) attacks. Railway infrastructure is an attractive target for EM attacks, because of its familiarity and ease of access, with extended economic, social and security consequences.

Today, the European rail network is evolving to harmonize the signalling management system. This is reflected by new integrated technologies, adequate procedures and centralization of command centres. The new technologies facilitate the implementation of a harmonized system and improve the network competitiveness. Protection solutions of this environment need to be found to ensure the security of the rail network, subject to intentional electromagnetic (EM) interferences, which can disturb a large number of command-control, communication or signalling systems.

In this context, SECRET aims to develop innovative solutions to reinforce the infrastructure and to prevent the European railway from the EM vulnerability resulting from the harmonisation process. This requires development of technologies in compliance with ERTMS and production of technical recommendations improving the European standardisation and the railway infrastructure resiliency. The work plan of the project extends over 36 months and is structured in five work packages in charge of the technical works as described below.

3- IEMI threats analysis conducted in STRUCTURES

(Stefan van de Beek – UT University of Twente)

Different High Power ElectroMagnetic (HPEM) environments are classified by several characteristics such as waveform, frequency coverage, and other output characteristics.

A list of available electromagnetic sources are presented and classified by technical attributes and non-technical attributes such as portability and availability. Combining the

technical and non-technical parameters will lead to an approximation of the risk that a source produces.

A brief overview of HPEM systems will be presented. The system architecture of narrowband and wideband sources will be shown.

Finally, the coupling path from source to victim is discussed. Front door coupling and backdoor coupling is defined for both radiated and conducted coupling.

4- Analysis and modelling methods assessment performed in STRUCTURES

(Kai Rathjen – HSU Helmut Schmidt University)

To identify the physical effects from the disturbance to the victim, the interaction sequence diagram proposed by C. E. Baum was used to categorize the physical effects: Electromagnetic interactions in complex systems are reduced to a sequence of “basic” elements, so ordering and simplifying the analysis; the “overall modelling problem” can be reduced to a sequence of “simpler” modelling steps, where the solution of the previous one will represent the source for the next one. All physical effects can then be classified in 6 categories: Source, Antenna, Propagation, Outside interaction, Field Penetration, Port of interest.

Within this framework, a number of basic modelling problems and coupling paths are identified and described. The computational chains suited to properly model these coupling paths are identified.

5- EM attack scenarios and devices considered in SECRET

(Henri Philippe – SNCF - henri.philippe@sncf.fr and Flavio Canavero – Polito-flavio.canavero@polito.it)

This presentation will present the current situation of the European railway network in terms of vulnerable technologies in case of EM attacks. The potential EM attack scenarios and EM attack devices to consider will be presented. Finally, this presentation will introduce the methodology developed in SECRET to analyse the potential impacts of EM attacks on railway network.

6- Detection of EM attacks: approaches developed in SECRET

(Marc Heddebaut –IFSTTAR-marc.heddebaut@ifsttar.fr)

This presentation will consist of three parts. The first part will present the power balance associated with different EM attack scenarios considered in the project. The second part will present the work being done to obtain models of the railway electromagnetic environment in "normal" conditions, ie in the absence of EM attacks. Finally, the third part will introduce the methods that are proposed to detect the presence of EM attacks.