INVESTIGATION OF THE IMPACT OF VARIOUS IEMI SOURCES TO ELECTRONIC PASSPORT READERS

Alexander Preinerstorfer[1], Christian Adami[2], Michael Joester[3], Thorsten Pusch[4], Michael Suhrke[5], Roman Bumerl-Lexa[6], Nikita Kolosnev[7], and Georg Neubauer[8]

[1] *alexander.preinerstorfer@ait.ac.at,* [6] *roman.bumerl-lexa@ait.ac.at,*
[8] *georg.neubauer@ait.ac.at*
Austrian Institute of Technology GmbH, Safety & Security Department,
2444 Seibersdorf (Austria)

[2] *christian.adami@int.fraunhofer.de,* [3] *michael.joester@int.fraunhofer.de,*
[4] *thorsten.pusch@int.fraunhofer.de,* [5] *michael.suhrke@int.fraunhofer.de*
Fraunhofer Institute for Technological Trend Analysis INT, Dept Electromagnetic Effects and Threats, Appelsgarten 2, 53879 Euskirchen (Germany)

[7] *nikita.kolesnev@regula.lv*
Regula Baltija Ltd., 97 A. Pumpura Str., Daugavpils LV5404 (Republic of Latvia)

Abstract

Intentional electromagnetic interference (IEMI) has risen to a serious threat for operators of critical infrastructures (CI). In this context, the European Union has funded three projects which deal with this problem. Passport control systems on airports are potential targets for such attacks. As part of cooperation between the EU projects HIPOW and FASTPASS, it was possible to start a test campaign for exposing electronic passport readers to high-power electromagnetic (HPEM) signals to find susceptibilities in these systems. The campaign had shown that it is possible to disturb such document readers with signals from powerful generators at various frequencies.

Keywords: IEMI, electromagnetic threats, protection of critical infrastructure, aviation security.

1 INTRODUCTION

The level of electromagnetic attacks for terroristic or criminal purpose has increased in the last decades to a non-negligible level. The societal dependence on electronic equipment such as telecommunication systems, IT networks, wireless communication, etc. increases steadily. These systems are commonly vulnerable to signals from IEMI sources. If electronic equipment is exposed intentionally to such signals, the term intentional electromagnetic interference (IEMI) has to be taken into account. Only a few examples of attacks by IEMI sources are documented in the open literature because of security and partially economic reasons. Attacks against ICT- and alarm systems were documented several times, e.g., the use of communication jammers to deactivate alarm systems of cars but also attempts on shops such as jewelry stores or banking networks were reported. Furthermore, large-scale attacks on telephone networks with up to several 100,000 affected persons took place [1]. To face up the problem of IEMI, the European Union has funded three projects in this topic under the 7th Framework Programme.

The project HIPOW [2] has the main goal to develop detection and protection concepts for critical infrastructures against electromagnetic threats. STRUCTURES [3] has the aim to analyze possible effects of electromagnetic attacks against critical

infrastructures. The third project is SECRET [4] which has the aim to assess the risks and consequences of electromagnetic attacks on the rail infrastructure, to identify preventive and recovery measures and to develop protection solutions to ensure the security of the rail network. The project FASTPASS [5] is also funded by the European Union under the 7th Framework Programme. The main goal of the project is to develop and establish a harmonized, modular reference system for all automated border crossing points by a user-centric approach and eventually serves as an industry standard for the implementation of automated border control (ABC) systems. Due to a coincidence of several objectives in HIPOW and FASTPASS, the idea was born to investigate the vulnerability of document readers used at airports or other areas where border crossings take place against HPEM signals.

2 BACKGROUND – IMPACT OF IEMI SOURCES ON AUTOMATED BORDER CONTROL SYSTEMS

Several infrastructures were embarrassed in their operation due to electromagnetic attacks in the past. Unclassified publications have so far not reported IEMI attacks on border control systems, but this does not exclude at all that such attacks did not already take place or may occur in the future. Motivation of criminals or terrorists to choose the critical infrastructure (CI) airport as potential target could be:

(1) Criminals want to blackmail providers of critical infrastructures and/or governmental institutions.
(2) Attackers want to bypass security zones by disturbing border control systems.
(3) Terrorists want to immobilize the critical infrastructure airport.
(4) Curiosity, some individuals in the society want to create chaos and so they see distortion of electronic components at an airport as a challenge.

Why should the attacker use an IEMI source?

- Easy access to airport gates with small- to medium-sized IEMI sources.
- Multiple attacks as well as attacks in parallel at different locations are easily achievable (e.g., various communication jammers combined with an HPEM suitcase).
- Low level of knowledge and budget necessary to obtain and handle IEMI sources (at least for low- to medium-power sources).
- Vulnerability of electronic components to field levels higher than common EMC levels is given.

To estimate the impact of electromagnetic attacks on ABC systems and in particular electronic passport readers, a risk analysis such as STRIDE and DREAD can be implemented. A relevant input for this risk analysis is the classification of the threat level of IEMI sources. Depending on costs, size and know-how of the attacker, a classification scheme of IEMI sources ranging from Low Tech to High Tech is shown in Tab. 1:

Low-Tech	Medium-Tech	High-Tech
Costs: < 1000$ Size: suitcase Easy to obtain and construct	Costs: 1000–100,000 $ Size: suitcase Experienced engineer	Costs: > 100,000 $ Size: van or truck Research groups

Table 1: Classification of IEMI sources by technological challenge.

The harming level and the related costs due to an electromagnetic attack depend on the applied IEMI source, the number of attacks, the duration of the disturbance or destruction, the redundancy of the border control system and the criticality of the attacked components. Consequences could vary from temporal distortions to enduring malfunctions of one or multiple components of infrastructures. The results from the test campaign could be used in a risk analysis.

3 TEST METHOD AND MEASUREMENT SETUP

The hereby described HPEM test methods conducted by the Fraunhofer Institute for Technological Trend Analysis INT are not conventional EMC test methods for commercial products. The applied tests should simulate two IEMI environments and include:

- Pulsed high-power microwave (HPM) signals in the frequency range from 150 MHz to 3425 GHz with a pulse width of 1 µs and a pulse repetition rate of 1 kHz
- CW and pulsed signals at a frequency of 13.56 MHz (RFID chip operating frequency of electronic passport readers).

The signals are generated by powerful sources and are fed into a TEM waveguide shown in Fig. 1 in which the test objects were placed. In this campaign, the devices under test (DUT) were two document readers from different manufacturers. The readers are designed as compact-sized plastic boxes with no moving internal parts. Components of the electronic passport readers are, e.g., an RFID reader or diverse LEDs for reading biometric and personal data from various media such as passports, driving licenses or identification cards.

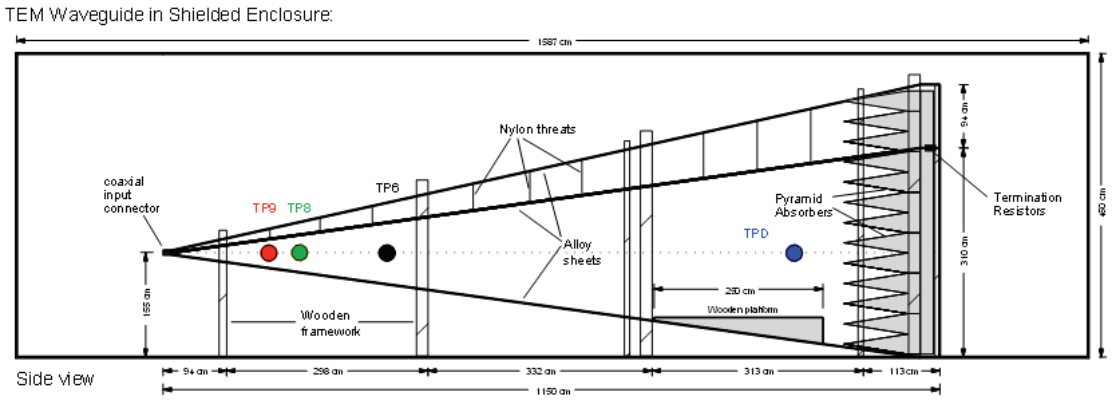

Figure 1: Fraunhofer INT TEM waveguide with its physical dimensions.

The tests were performed using a standard notebook, the Passport Reader Demo Application Software, the original power supply and a test passport and gave information about the performance of the equipment during exposure to IEMI signals. Fig. 2 shows the measurement setup at Fraunhofer INT. The power supply cables of the document readers and the data connection cables from the notebook to the document readers were shielded with copper foil to avoid backdoor coupling failures. Exposure of the document readers was performed at several points in the TEM waveguide to get a large range of electrical field strength. Thus, the test from small to high peak values was possible.

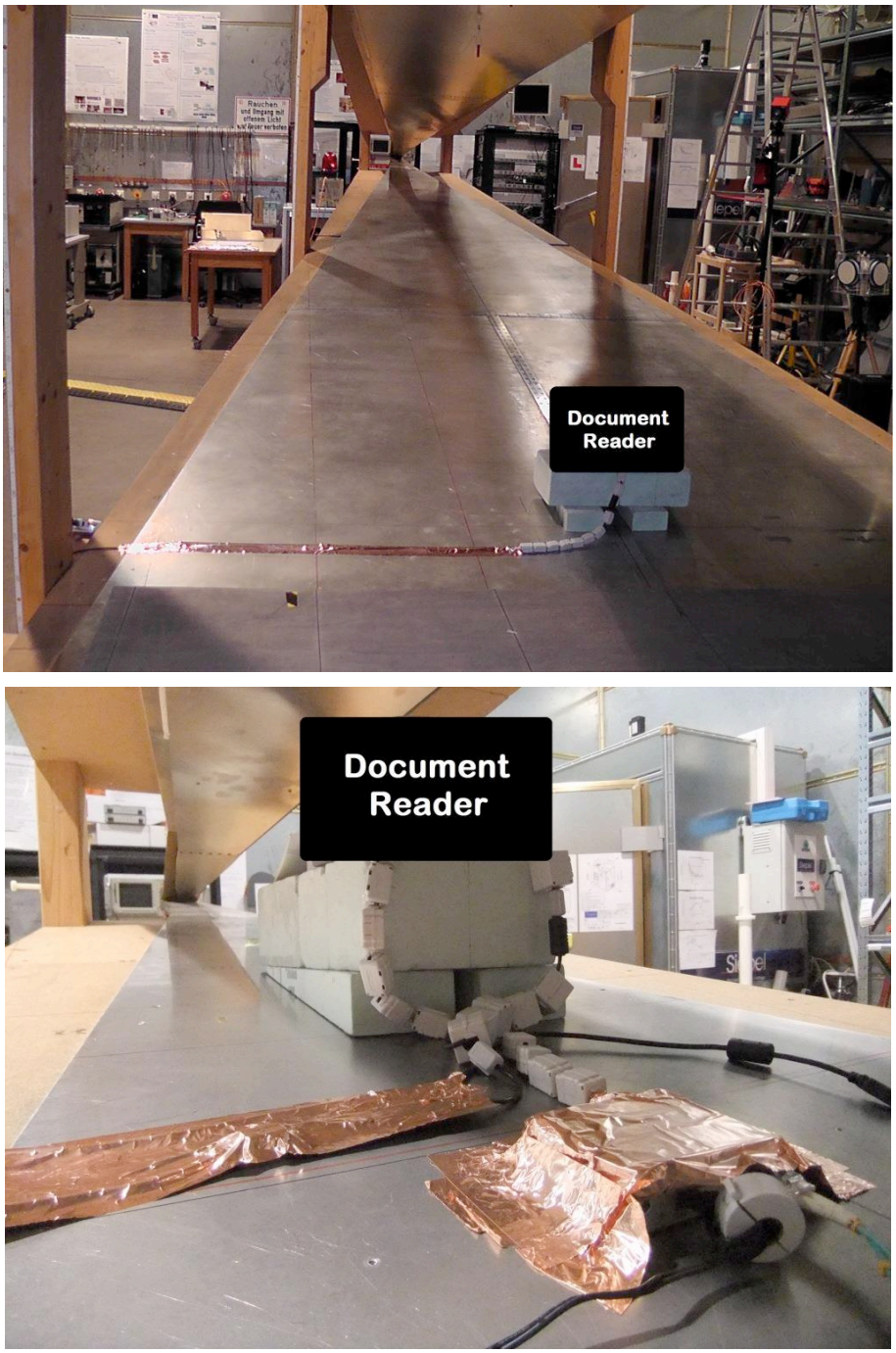

Figure 2: Document reader in the TEM waveguide at Fraunhofer INT.

4 ERROR DIAGNOSIS

A classification of errors arising due to HPEM exposure of the DUT is given in Tab. 2 going from no effect (Type A error) to damage (Type D error). Several errors were observed during the test campaign which mainly depended on the applied field strength as well as frequency in the waveguide also shown in Tab. 2.

Error Diagnosis	Effect	Description	Effects during exposure
Type A	No effect	System can fulfil its work without disturbances	
Type B	Interference	Effect during exposure, if exposure is removed the system works correctly again	- No picture - Failure in image recognition - No machine-readable zone (MRZ) - No RFID
Type C	Upset	Effect during exposure, human interaction is required to set the system in the initial state (e.g. resetting), afterwards the system works correctly again	- USB connection is disconnected - RFID could not be read out - Software error (crash)
Type D	Damage	Parts of the hardware are damaged or reprogramming occurred, device is unable to restart	

Table 2: Classification of occurred errors on document readers due to HPEM signals.

Fig. 3 gives an example of a correct optical readout of the used fake passport and a failed readout during exposure with HPEM signals.

Figure 3: Comparison of a correct readout (left) and a failed readout (right) during HPEM exposure.

Often, a reset (Type C) of the document readers was necessary to set the devices in the initial state. Total damage (Type D) was not observed during the tests. With small electrical field strength levels, there also often was no effect (Type A) to be observed. But mainly Type B errors occurred. In Fig. 4, it is easy to realize that failures were found in the whole tested frequency range.

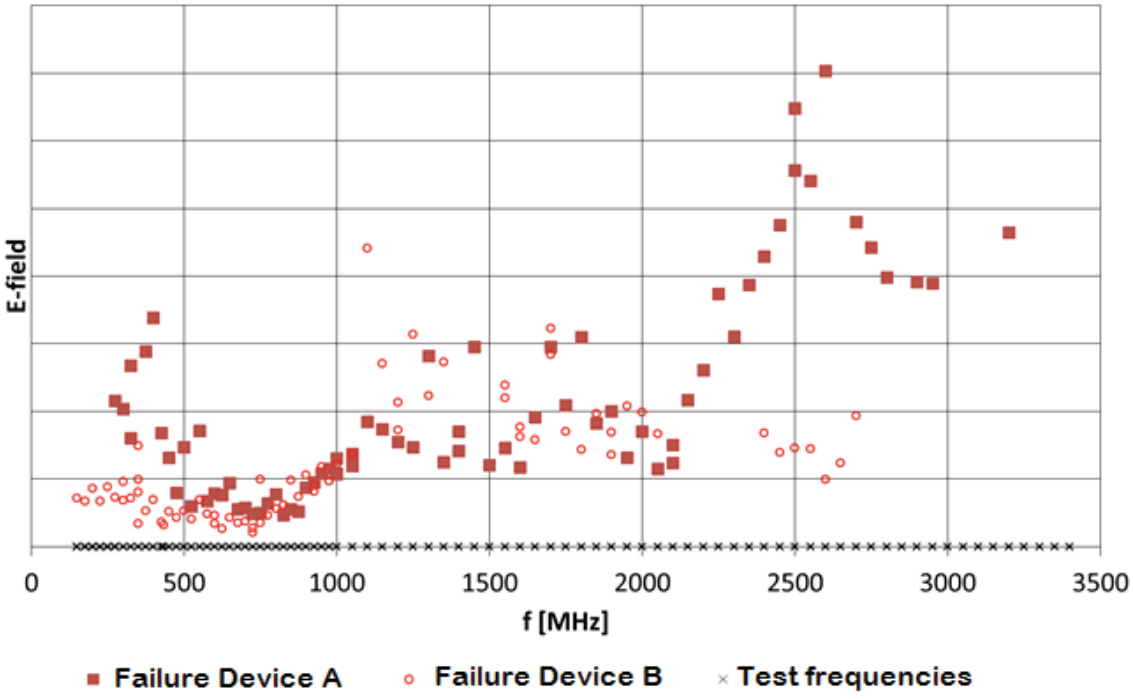

Figure 4: Failures of two different document readers during exposure with HPEM signals.

After testing two different document readers, an additional test with another polarization of the electromagnetic field was applied to one of the devices. Only a small frequency band around 1 GHz was chosen for this test. Similar results to the previous applied polarization of the electromagnetic waves were observed.

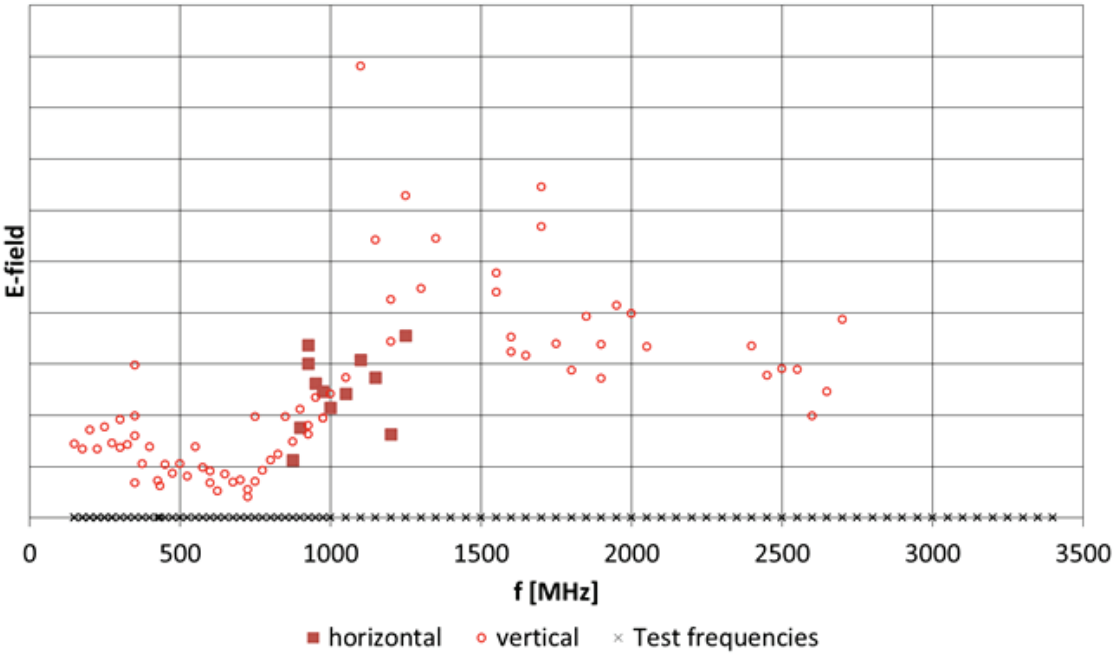

Figure 5: Failures of one of the two investigated document reader with two field polarizations.

Also, the tests at a frequency of 13.56 MHz showed failures during the readout of the passport. In particular, only the RFID readout showed failure behavior at this frequency.

The results from the test campaign are EU-restricted and are subjected to disclosing agreements, so far no detailed information about the applied electrical field strengths could be provided.

5 DISCUSSION

Critical infrastructures such as airports are potential targets for criminals and terrorists. The use of low-tech (or medium-tech) IEMI sources to harm such infrastructures is not unlikely to occur both due to the easy acquisition and low costs of IEMI sources and the easy access to airport gates. In the course of potential electromagnetic attacks, electronic document readers installed on electronic gates are one of the possible targets. The test campaign described in this paper investigated the vulnerabilities of document readers against HPEM signals and is dedicated to help hardening border control systems against electromagnetic attacks. Results of the campaign will be presented at the Future Security 2014 in Berlin.

ACKNOWLEDGEMENTS

The project FASTPASS has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under Grant Agreement No. 312583.

The FP7 Project HIPOW has received funding from the European Commission's Seventh Framework Programme (FP7/2012–2012) under Grant Agreement No. 284802.

REFERENCES

[1] Sabath, F. "What Can Be Learned from Documented Intentional Electromagnetic Interference (IEMI) Attacks?" XXXth URSI General Assembly and Scientific Symposium 2011. 2011.

[2] HIPOW (Protection of Critical Infrastructures against **Hi**gh **Pow**er Microwave Threats).
Project Homepage (2014): www.hipow-project.eu/ (Last access: June 15, 2014).

[3] STRUCURES (**Str**ategies for the Improvement of Critical Infrastr**uctu**re **R**ESILIENCE to **E**lectromagnetic Attack**s**).
Project Homepage (2014): www.structures-project.eu/ (Last access: June 15, 2014).

[4] SECRET (**Sec**urity of **R**ailways against **E**lectromagnetic A**t**tacks).
Project Homepage (2014): www.secret-project.eu/ (Last access: June 15, 2014).

[5] FASTPASS (A Harmonized, Modular Reference System for All European Automated Border Crossing Points).
Project Homepage (2014): www.fastpass-project.eu/ (Last access: April 29, 2014).