HPEM Tests of Communication Devices

Ch. Adami, M. Joester, M. Suhrke, H.J. Taenzer
Electromagnetic Effects and Threats
Fraunhofer Institute for Technological Trend Analysis INT
Euskirchen, Germany
michael.suhrke@int.fraunhofer.de

***Abstract*—Intentional Electromagnetic Interference (IEMI) can be used to support illegal activities ranging from robbery up to terroristic attacks. The general idea is to use High Power Electromagnetics (HPEM) beyond the Electromagnetic Compatibility (EMC) immunity of handheld communication devices to compromise their functionality. In particular, smart phones and tablets could be in focus of such an attack as those devices are increasingly used to control and communicate in critical infrastructures. Fraunhofer INT did HPEM vulnerability tests with a selection of smart phones and tablets showing disturbances in a wide frequency range.**

HPEM; IEMI; Electromagnetic Threat; smart phones; tablets; communication systems

I. INTRODUCTION

Smart phones and tablets more and more find their way into the control of critical infrastructures. HPEM tests of mobile phones in the past showed a high vulnerability against HPEM fields [1]. The new technology offers more frequency bands for communication, Wi-Fi and touch sensitive displays, why they are more susceptible to HPEM. Fraunhofer INT conducted HPEM vulnerability tests of eight smart phones and four tablets.

II. TESTING

A. Test Objects

Fraunhofer INT conducted vulnerability tests of four low-cost smart phones with 240 x 320 pixel displays, four devices from the mid-range price segment with 1280 x 720 pixel and four tablets with 7 inch and 10 inch displays. All devices run with Android system software except one Blackberry and one with Windows Phone 8.

B. Test Setup

The tests were set up in the TEM waveguide of Fraunhofer INT with a frequency range from 150 MHz to 3.4 GHz. A GSM/UMTS connection with the smart phones was not possible during the tests. The Wi-Fi connection of the smart phones was used to establish a mobile radio connection. A Wi-Fi network with two Wi-Fi routers was installed inside the shielded test facility whereupon router #1 functioned as the access point (DHCP server) and router #2 as in bridge mode to check the Wireless Distribution System during the tests. The connections between the routers and the PCs outside of the shielded hall were fiber optic cables together with media converters.

The first two smart phones were tested in two different setups corresponding to different operation modes of the smart phones.

In setup #1 the smart phone had a Wi-Fi connection with the Wi-Fi network inside the shielded hall. The front side of the smart phones with the internal camera was oriented to the waveguide input and the camera signal was transferred out of the shielded hall via the Wi-Fi connection. In setup #2 a video was played on the DUT during HPEM field application. Both smart phone displays were monitored with an RF hardened camera.

III. TEST RESULTS

The tests in both setups #1 and #2 show that HPEM can disturb smart phones and tablets in a broad frequency range. The RF field triggered unwanted operations on the touch sensitive display. The Wi-Fi data transfer was interrupted in a broad frequency range, also outside the Wi-Fi spectrum. In some cases the transfer had to be started all over again. During the tests one DUT has been broken.

Fig. 1 gives an overview of normalized susceptibility thresholds for two smart phones. The failure frequencies vary from 280 MHz to 2.46 GHz.

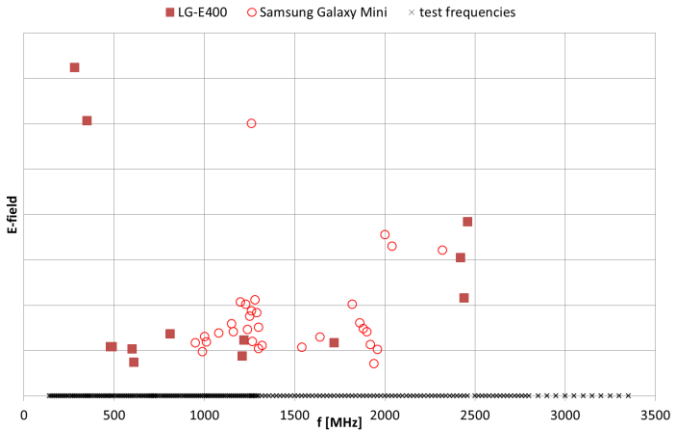

Figure 1. Susceptibility threshold of two smart phones.

REFERENCES

[1] Braun, Ch. and Schmidt, H.-U., " Effects of microwave irradiation on modern Telecom devices - failure thresholds of five mobile phones " AMEREM 2002, Annapolis, 2002.