Generation dependence of ICT device IEMI vulnerability

C. Adami, B. Jörres, M. Jöster, T. Pusch, M. Suhrke, A. Taenzer*

**Fraunhofer INT, Euskirchen, Germany, thorsten.pusch@int.fraunhofer.de*

Abstract

Immunity of electronic devices against (I)EMI may be subject to generational changes since baseline technologies constantly evolve. We submitted mobile phones from time frames spanning sixteen years in total as well as two succeeding generations of tablet computers to HPM pulses in order to probe their robustness. Such devices are widely used in critical infrastructures, thus risking to present targets for IEMI attacks. While rising device complexity and miniaturization may imply problems, average immunity of newer devices has in parts even improved, possibly due to inner EMC concerns.

Keywords: IEMI, HPM, susceptibility, cell phone, tablet.

1 Introduction

Critical infrastructure operation relies in many parts on modern communication technology, while device functionality rapidly evolved over the last decades. In practice, e.g. industrial SCADA systems are controlled by tablet-like devices, fire fighters resort to smartphone apps helping to forecast propagation of noxious gas clouds, while the military procures commercial-off-the-shelf hardware in order to provide soldiers with accrued situational awareness. We set out to investigate what effects evolutionary steps in design and technology might have on the vulnerability of such systems against IEMI, more specifically High Power Microwave (HPM) exposure.

In this vein, we identified a few development areas where important changes occurred over the last few years:

- Device functionality is continuously added upon
- Hardware and IC structures are shrinking
- Touchscreen interfaces replace mechanical keys
- Basic wireless network technology is supplemented by new standards (3G, 4G, etc., as well as 5 GHz WiFi), increasing the number of frequency bands
- Globalized markets call for universal hardware solutions, operational in all local frequency bands

2 Test devices and experimental programme

Our approach to Device Under Test (DUT) selection has been the following: Nine mobile phones from manufacturing years 1997-2000 had previously been tested onsite according to our standard methodology, featuring just 2G mobile network technology. We decided to make a comparison with a similar batch of contemporary devices, specifically subsequent hardware generations of medium-class smartphones dating from 2012/13. These operate on additional frequency bands, pertaining to 3G and WiFi networks as well as satellite navigation services. We included tablet computers as well, the lines being blurred between device categories. Some of these 2013/14 specimen include 4G technology. All in all, we started our investigations with at least 5 devices in each group.

We performed vulnerability tests on all DUT within a tapered open TEM waveguide, test frequencies ranging from 150 MHz to 3450 MHz. Pulsed signals of 1 µs length and 1 kHz repetition rate were applied, the field strength ranging well above standard EMC. We recorded failure thresholds as evidenced under monitoring during a power ramp.

3 Results and discussion

We observed some instances of permanent damage, almost universally tied to front door coupling, i.e. the test frequency lying in one of the communication bands. The touch screen as input interface has proven a weak spot on modern devices, many phantom touches were observed. With the tablets, significant failure clustering in frequency ranges delimited by basic enclosure resonances could be observed.

In general, the newer phones performed at least on par, if not better than the older ones when averaging over well-defined frequency bins, compare Fig.1. We conclude that design measures meant to improve inner EMC and being imperative due to the plethora of supported (and surrounding) wireless services possibly account for this effect, as evidenced by a particular robustness *within* communication bands. Above 2.5 GHz, the tablet devices were less immune on average than the other two device groups.

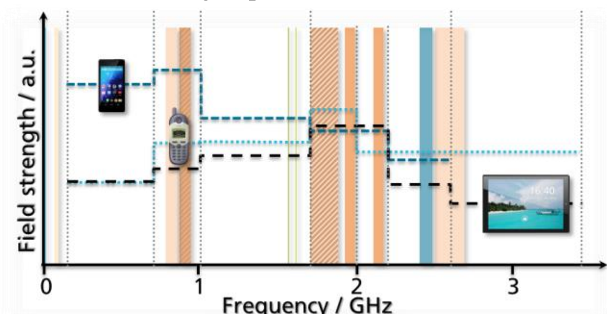

Figure 1. Failure thresholds averaged over bins covering in-band and out-of-band frequencies.

Further investigations into additional device generations provide even deeper insight into generation dependency of IEMI susceptibility.