HPEM-Empfindlichkeit von intelligenten Stromzählern als Komponenten des Smart Grid

M. Sc. Marian Lanzrath[1], Dr. Thorsten Pusch[1], Dipl.-Ing. Michael Jöster[1], Dr. Michael Suhrke[1]

[1]Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen INT

1 Einführung

Die elektrische Energieversorgung ist die wichtigste kritische Infrastruktur unserer Gesellschaft. Die ständige Verfügbarkeit der Stromversorgung ist Grundlage der modernen, durchoptimierten Industrie und aller Dienstleistungen, die heutzutage ohne digitale Informationsverarbeitung nicht mehr denkbar wären. Im privaten Umfeld ist die ständige Verfügbarkeit von Strom aus der Steckdose eine Selbstverständlichkeit, über die wir gar nicht mehr nachdenken.
Die Sicherung der Verfügbarkeit von elektrischem Strom ist demnach essentiell wichtig. Durch umweltpolitische Entscheidungen geht der Trend in der Erzeugung weg von fossilen Brennstoffen und zentral gelegenen Großkraftwerken hin zu in der Fläche abschöpfbaren erneuerbaren Energien. Die Umstellung der Erzeugung hat Einfluss auf die Netzregelung, denn diese muss von einer bedarfsorientierten, zentralen Kraftwerksregelung hin zu einer angebotsangepassten, dezentralen Verbraucher-Erzeugerregelung umgewandelt werden. In der Regelung müssen beispielsweise wetterbedingte Verfügbarkeitsschwankungen der erneuerbaren Energiequellen berücksichtigt werden. Damit bei der dezentralen Verteilung von Erzeuger und Verbraucher weiterhin ein stabiles Stromnetz zur Verfügung gestellt werden kann, soll dem flächendeckenden Stromversorgungsnetz ein IT-Kommunikationsnetz überlagert werden, das dem aufkommenden Echtzeit-Kommunikationsaufwand gewachsen ist. Die flächendeckende kommunikative Vernetzung von Erzeuger und Verbraucher bietet Potential für ein neues Regelungskonzept, das Demand-Side-Management (DSM). Hierbei sollen ausgewählte elektrische Verbraucher in Haushalten und Industriebetrieben bei Bedarf zum Lastausgleich automatisch zu- oder abgeschaltet. Ergänzt um diese Erweiterung wird ein solches künftiges Stromnetz auch Smart Grid („intelligentes Stromnetz“) genannt.
Im Smart Grid wird im Vergleich zum aktuellen Stromnetz die Anzahl verbauter elektronischer Geräte vervielfacht. Es sollen elektronische Zähler, IT-Knoten, Kommunikationsgateways, Messsensoren und auch moderne Fernwirktechnik verbaut werden. Damit stellt sich die Frage nach der Funktions- und Ausfallsicherheit auf einer neuen Ebene, insbesondere, wenn man Möglichkeiten zur bewussten, schädlichen Fremdeinwirkung auf moderne Elektronik komplexer Bauart in Betracht zieht. Es wurden in den vergangenen Jahrzehnten bereits umfangreiche Versuche unternommen, die Verwundbarkeit von Elektronik durch elektromagnetische Felder hoher Leistung (HPEM, „High Power Electromagnetics“) zu untersuchen [1],[2]. Im Fraunhofer Institut für Naturwissenschaftlich-Technische Trendanalysen (INT) wurden unter anderem gezielt Kommunikations- und Überwachungssysteme sowie PC’s auf ihre Störempfindlichkeit gegenüber HPEM hin untersucht [3],[4],[5],[6]. Kriminelle nutzen bereits Hochfrequenzquellen, um mit Hilfe von IEMI („Intentional Electromagnetic Interference“) IT- oder Sicherheitssysteme in ihrer Funktion zu beeinträchtigen.

Betrachtet man das Smart Grid im Lichte dieser Entwicklungen, so lassen sich fehlerhafte Informationen und Totalausfälle von Elektronik als eine erhebliche Gefährdung für die Stromversorgung und die Netzregelung identifizieren. Eine Manipulation des Stromnetzes durch IEMI ist denkbar und sollte als Gefährdungspotential bei der zukünftigen Netzplanung berücksichtigt werden.
In diesem Beitrag werden HPEM-Empfindlichkeitsuntersuchungen an intelligenten Stromzählern (Smart Meter) vorgestellt, welche von Energieversorgern eingesetzt werden. Die Smart Meter werden aktuell nur zu Abrechnungszwecke eingesetzt und haben keinen Einfluss auf die Netzstabilität, sie bilden jedoch ein leicht zugängliches Ziel für Angreifer, welches zusätzlich eine der am häufigsten verbauten Komponenten im intelligenten Stromnetz ist. Die Untersuchungen der Smart-Meter bilden eine Grundlage für weitere Untersuchungen an kritischen Netzkomponenten.

2 Hochleistungselektromagnetik

Dieser Abschnitt befasst sich mit einer kurzen Erläuterung der für die durchgeführten Untersuchungen relevanten Konzepte sowie der zugehörigen Testumgebung.
Erfolgt der Energietransport über Wellenausbreitung im Raum, so spricht man von feldgebundener Einkopplung. Die Einkopplung in ein Gerät kann dann sowohl direkt über Gehäuseöffnungen als auch indirekt über angeschlossene Kabel erfolgen. Wie in verschiedenen Untersuchungen festgestellt wurde, überwiegen oberhalb von einigen 100 MHz bis zu einigen GHz oft Störungen durch direkte Einkopplung in das elektronische Gerät, unterhalb dominiert meist die Einkopplung über Kabel, beginnend bei einigen zehn MHz. Bei leitungsgebundener Einkopplung, also dem direkten Energieeintrag in Verbindungskabel und Zuleitungen, können oftmals Störungen bis etwa 1 GHz erzeugt werden [7]. Oberhalb von 1 GHz nimmt die Störanfälligkeit ab, was auf eine mit der Frequenz steigende Signaldämpfung der Leitungen zurückzuführen ist.
Die Untersuchungen der Smart Meter wurden auf einem genormten BCI-Messplatz (Bulk Current Injection) nach DIN EN 61000-4-6 im Frequenzbereich von 140-1000 MHz für leitungsgebundene Einkopplung, sowie in einem 3-Streifen-TEM-Wellenleiter nach DIN EN 61000-4-20 im Frequenzbereich von 140-7500 MHz für feldgebundene Einkopplung durchgeführt. Der verwendete TEM-Wellenleiter am Fraunhofer INT ist für ein maximales Testobjektvolumen von etwa 2 x 2 x 3 m³ geeignet.
Als elektromagnetisches Störsignal wurde ein schmalbandiges, gepulstes Mikrowellensignal („High Power Microwave“ HPM) mit 1 kHz Wiederholfrequenz und 1 µs Pulsbreite verwendet. Für die Untersuchungen stehen im Labor Leistungsoszillatoren für den Frequenzbereich 140-3400 MHz mit maximal 35 kW Pulsleistung sowie TWT-Verstärker mit 5 kW Pulsleistung für den Frequenzbereich von 4-8 GHz zur Verfügung.
Konstruktionsbedingt benötigt der Leistungsoszillator eine Mindestansteuerung für die Pulserzeugung, diese wurde bis zur Maximalamplitude rampenförmig gesteigert. Damit mehrere Zählerstände während des Tests bei einer festen Testfrequenz ausgelesen werden konnten, wurde die Rampenlaufzeit auf 150 s festgelegt.

3 Prüflinge und Versuchsaufbauten

In den folgenden Abschnitten werden die untersuchten Zähler sowie die spezifischen Versuchsaufbauten betrachtet.

3.1 Testobjekte: Smart Meter

In Abbildung 1 sind in Deutschland gebräuchliche elektronische Zählermodelle dargestellt, die wir Empfindlichkeitsuntersuchungen unterzogen haben. Bei dem linken Zählermodell handelt es sich um einen elektronischen Zähler für die Montage auf einem Zählerkreuz, bei dem rechten Zähler um einen eHz (elektronischer Haushaltszähler) für die Montage auf einem eHz-Adapter.

Abbildung 1: Untersuchte Smart Meter

Die beiden Testobjekte unterscheiden sich stark in Größe, Bauform sowie Kommunikationsschnittstelle. Testobjekt 1 ist in etwa doppelt so groß wie Testobjekt 2, wobei es sich im unteren Teil von Testobjekt 1 um eine Abdeckkappe für den Anschlussbereich handelt. Bei Testobjekt 2 handelt es sich hingegen um einen eHz, welcher mit Hilfe von stromführenden Messern auf der Rückseite auf einer entsprechenden Anschlussplatte im Zählerschrank eingerastet wird. Testobjekt 1 kommuniziert über eine leitungsgebundene RS-485-Schnittstelle mit dem Gateway, Testobjekt 2 verfügt über eine w-MBUS Kommunikationsschnittstelle.

3.2 Versuchsaufbau BCI

Für die BCI- sowie die Wellenleiter-Untersuchungen mussten individuelle Versuchsaufbauten konzipiert werden. Abbildung 2 zeigt das Prinzipschaltbild des BCI-Versuchsaufbaus, bei dem über eine Netznachbildung (LISN) ein Standard-Zählerschrank mit dem Stromnetz verbunden wurde. Die untersuchten Zähler mit den benötigten Kommunikationsgateways wurden innerhalb dieses Zählerschrankes installiert.

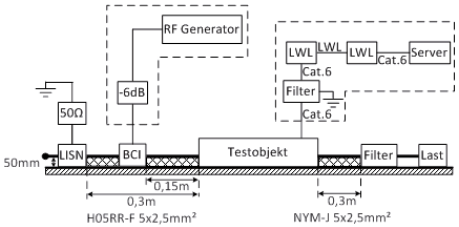

Abbildung 2: Prinzipschaltbild BCI-Aufbau

Abbildung 3: BCI-Aufbau

Die Abbildung 3 zeigt den realen Versuchsaufbau am BCI-Messplatz. Hinten rechts ist erkennbar, dass am Ausgang des Zählerschranks über Netzfilter elektrische Verbraucher zum Betrieb des Zählers unter Messbedingungen angeschlossen wurden. Die BCI-Einspeisezange wurde auf dem eingangsseitigen Kabelbaum mit 15 cm

Abstand zum Zählerschrank installiert. Über Ethernet-Filter und Glasfaserstrecken wurden die Gateways zur Auslesung mit einem PC verbunden.

3.3 Versuchsaufbau TEM-Wellenleiter

In Abbildung 4 ist der entsprechende Versuchsaufbau für die Wellenleiter-Untersuchungen dargestellt. Bei diesen wurde ebenfalls eine Netznachbildung für die Einspeisung des Stromnetzes verwendet. Um eine Direkteinkopplung auf die Peripherie zu minimieren, wurde diese außerhalb des Wellenleiters positioniert.

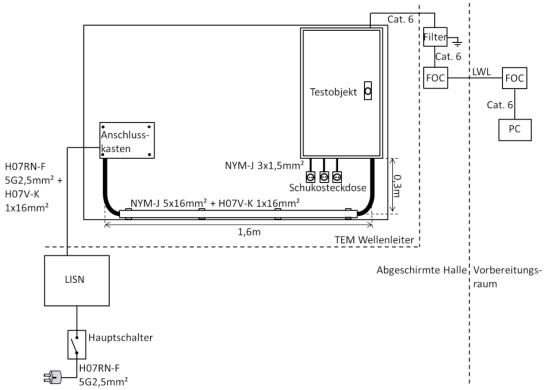

Abbildung 4: Prinzipschaltbild TEM-Aufbau

Bei den Empfindlichkeits-Tests wurden zwei Polarisationen des Aufbaus jeweils mit senkrechter und waagerechter Orientierung des äußeren Kabelbaumes zwischen Anschlusskasten und Testobjekt untersucht (siehe Abbildung 5 und Abbildung 6). Bei senkrechter Ausrichtung liegt der Kabelbaum parallel zur Hauptkomponente des elektrischen Feldes im Wellenleiter, hierbei ist eine erhöhte Einkopplung in den Prüfling über den Kabelbaum zu erwarten. Bei waagerechter Ausrichtung liegt der Kabelbaum senkrecht zur Hauptkomponente, die Einkopplung erfolgt vor allem direkt in den Prüfling.

Abbildung 5: TEM-Aufbau senkrecht

Abbildung 6: TEM-Aufbau waagerecht

4 Testergebnisse

Im folgenden Abschnitt werden die Ergebnisse der Untersuchungen vorgestellt. Bei der BCI-Methode wird der substituierte Strom im Kalibrieradapter dargestellt. Für die

Wellenleiter-Untersuchungen wird die elektrische Feldstärke am Ort des Prüflings in Abhängigkeit von der Frequenz angegeben. Der hinterlegte Bereich gibt den untersuchten Bereich von Störsignalamplituden in a.u. (arbitrary units) an. Die Markierungen über der Frequenzachse zeigen die getesteten Einzelfrequenzen.

4.1 Bulk-Current-Injection (BCI)

Bei den BCI-Tests konnten für beide Testobjekte bei Frequenzen bis etwa 800 MHz Störungen erzeugt werden, oberhalb von 800 MHz zeigten die Prüflinge im getesteten Frequenzbereich bis 1000 MHz keine Auffälligkeiten mehr. Es ist erkennbar, dass bei beiden Modellen im unteren Frequenzbereich bis etwa 500 MHz bei Testobjekt 1 und 400 MHz bei Testobjekt 2 insbesondere die Messsensoren gestört wurden. Oberhalb dieser Frequenzen kam es hauptsächlich zu temporären Störungen der Kommunikation oder Störungen bis zu einem Bedienereingriff. Unterhalb von 300 MHz zeigte Testobjekt 1 im Unterschied zu Testobjekt 2 kaum Störungen. Auffällig bei Testobjekt 2 war, dass im oberen Frequenzbereich häufig Beschädigungen der Zähler verursacht wurden.

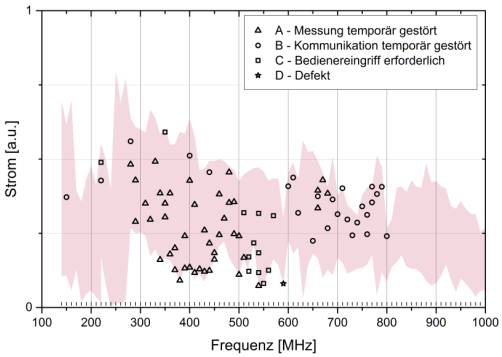

Abbildung 7: Störschwellen für Zähler 1 bei leitungsgebundener Einkopplung

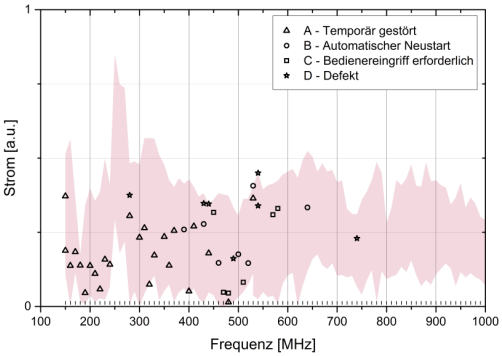

Abbildung 8: Störschwellen für Zähler 2 bei leitungsgebundener Einkopplung

4.2 TEM-Wellenleiter

Eine Abschätzung zeigt, dass die im TEM-Wellenleiter ermittelten Störschwellen konsistent mit denen aus den BCI-Tests sind. Bei senkrechter Ausrichtung des

Kabelbaums im Wellenleiter konnte Testobjekt 1 wie in den BCI-Tests erst ab 300 MHz, jedoch bis 2500 MHz gestört werden. Es kam, wie bei der BCI-Methode, im unteren Frequenzbereich bis etwa 500 MHz zu Störungen der Messsensoren. Im oberen Frequenzbereich wurden wieder hauptsächlich die Kommunikation gestört oder Bedienereingriffe hervorgerufen. Vereinzelt kam es hierbei auch zu Defekten an der Hardware. Die in den BCI-Tests nicht beobachteten Störungen im Frequenzbereich von 800 bis 1000 MHz deuten auf direkt gestrahlte Einkopplung in den Prüfling hin. Zwischen 300 und 800 MHz dominiert die Einkopplung über den Kabelbaum.
Bei Testobjekt 2 wurden wie in den BCI-Tests Störungen bereits ab der niedrigsten Testfrequenz von 140 MHz bis etwa 700 MHz sowie zusätzlich im mit der BCI-Methode nicht getesteten Bereich 1200-1800 MHz erzeugt. Im oberen Frequenzbereich kam es hauptsächlich zu Störungen, die einen Bedienereingriff erforderten. Im unteren Frequenzbereich konnten neben temporären Störungen auch Defekte verursacht werden. Die vergleichbaren Ergebnisse beider Methoden für beide Testobjekte im unteren Frequenzbereich deuten wieder darauf hin, dass die gestrahlte Einkopplung hier vorwiegend über den Kabelbaum erfolgt.

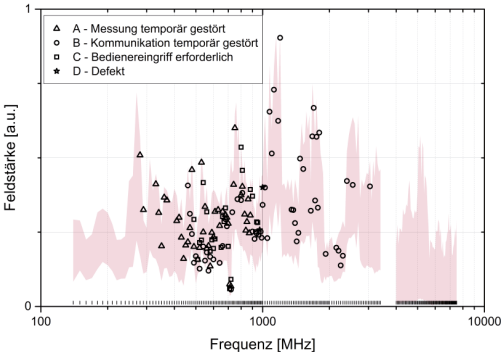

Abbildung 9: Störschwellen für Zähler 1 bei feldgebundener Einkopplung, senkrechte Ausrichtung

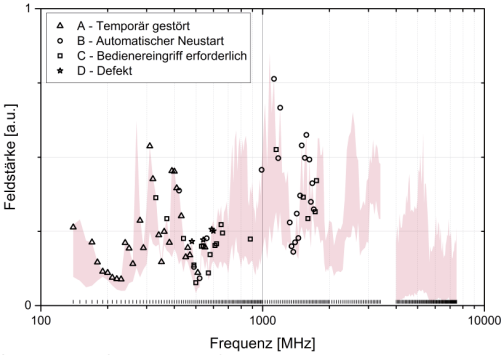

Abbildung 10: Störschwellen für Zähler 2 bei feldgebundener Einkopplung, senkrechte Ausrichtung

Eine waagerechte Ausrichtung des Kabelbaums senkrecht zur Feldrichtung führt bei Testobjekt 1 wie erwartet zu einer starken Reduzierung der störbaren Frequenzen. Es können zwei Frequenzbereiche, in denen sich die Störungen konzentrieren, eingegrenzt werden. Der erste liegt zwischen 400 und 800 MHz, der zweite zwischen 1400 und 2000

MHz. Im unteren Frequenzbereich sind wieder hauptsächlich die Messsensoren betroffen, im oberen hingegen kommt es hauptsächlich zu temporären Störungen der Kommunikation. Der Wegfall der Störungen zwischen 800 und 1000 MHz deutet auf den Einfluss des internen Aufbaus des Prüflings auf die Einkopplung bei verschiedenen Ausrichtungen hin, die Reduktion der Störungen bei niedrigen Frequenzen unterstützt die Interpretation als Einkopplung über den Kabelbaum.
Bei Testobjekt 2 befindet sich die untere Störgrenze bei 160 MHz, die obere jetzt nahezu ohne Lücke bei etwa 1100 MHz, sie reduziert sich nur in geringem Maße im Vergleich zur senkrechten Ausrichtung. Hier spielt wieder der interne Aufbau des Prüflings eine Rolle. Wie auch bei den vorherigen Messungen werden im unteren Frequenzbereich vorrangig die Messsensoren gestört. Ab 500 MHz kommt es wieder häufig zu Störungen, die einen Neustart erforderlich machen oder Defekte erzeugen. Der Vergleich der Störungen oberhalb von 700 MHz in den verschiedenen Testkonfigurationen deutet wieder auf direkte gestrahlte Einkopplung in den Prüfling hin.

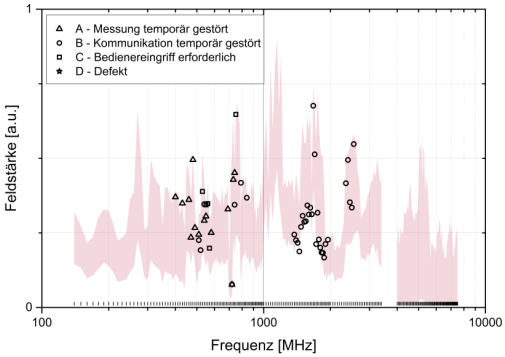

Abbildung 11: Störschwellen für Zähler 1 bei feldgebundener Einkopplung, waagerechte Ausrichtung

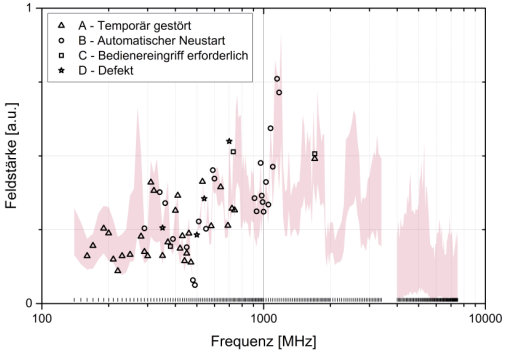

Abbildung 12: Störschwellen für Zähler 2 bei feldgebundener Einkopplung, waagerechte Ausrichtung

5 Zusammenfassung

Die Tests in den verschiedenen Konfigurationen ergeben ein weitgehend konsistentes Bild der dominierenden Koppelpfade in verschiedenen Frequenzbereichen. Insbesondere trifft dies auf den Vergleich der Ergebnisse für Zähler 1 (Abbildung 7,9

und 11) zu. Bei senkrechter Ausrichtung gibt es einen nahtlosen Übergang zwischen leitungs- und feldgebundener Einkopplung. Bei waagerechter Ausrichtung sind eine Lücke zwischen den zwei Fehlerclustern sowie eine Reduktion der Störungsanzahl erkennbar. Zähler 2 (Abbildung 8,10 und 12) liefert keine so eindeutige Unterscheidung der Koppelpfade. Bei diesem Modell werden mittels BCI-Methode Störungen bis etwa 750 MHz erzeugt. Bei senkrechter Ausrichtung des Kabelbaumes kann eine Unterscheidung zwischen leitungs- und feldgebundener Einkopplung vorgenommen werden. Die waagerechte Ausrichtung des Kabelbaumes führt bei diesem Modell nicht wie erwartet zu einer signifikanten Reduktion der Störempfindlichkeit.
Bei allen Messungen ist ersichtlich, dass im unteren Frequenzbereich hauptsächlich die Messsensoren gestört werden. Im oberen Frequenzbereich kam es häufig zu Störungen, die einen Neustart der Anlage verursachen. Weiterhin weisen die verschiedenen Koppelpfade vergleichbare Störschwellen auf. Entgegen der Erfahrungen mit Untersuchungen anderer Elektronik wurden bei den Tests viele Geräte beschädigt.
Betrachtet man das Gefährdungspotential der ermittelten Empfindlichkeiten, so hat ein Ausfall des Zählers durch Beschädigung oder Softwareabsturz nicht zur Folge, dass die angeschlossenen Verbraucher spannungsfrei geschaltet werden. Bei den Zählern handelt es sich um ein reines Messsystem, das momentan von den Energieversorgern nur zu Abrechnungszwecken verwendet wird. Das Gefährdungspotential durch Störung eines Smart Meter könnte sich allerdings in Zukunft im Rahmen des Demand-Side-Management erhöhen. Hier sollen zur Netzregelung über die Smart Meter-Anbindung Endverbraucher zu- und abgeschaltet werden.
Für weiterführende Untersuchungen zur HPEM-Empfindlichkeit des Smart Grid, wurden Netzkomponenten einer übergeordneten Hierarchieebene identifiziert. Dabei handelt es sich um aktuell verwendete Netz-Fernwirktechnik sowie Schutzleitgeräte, welche von Energieversorgern für die Netzregelung sowie zur Netzüberwachung eingesetzt werden. Ein Ausfall dieser Komponenten könnte direkten Einfluss auf die Netzstabilität besitzen.

6 Literaturverzeichnis

[1] M.G. Backstrom, K.G. Lovstrand: „*Susceptibility of electronic systems to high-power microwaves: summary of test experience*", Electromagnetic Compatibility, IEEE Transactions on , vol. 46, no. 3, pp. 396-403, 2004

[2] W.A. Radasky, R. Hoad: „*An Overview of the Impacts of Three High Power Electromagnetic (HPEM) Threats on Smart Grids*", IEEE 978-1-4673-0717-8/12, 2012

[3] Ch. Adami, C. Braun, P. Clemens, H.-U. Schmidt, M. Suhrke, H.-J. Taenzer, U. Weber: „*High Power Microwave Susceptibility of IT Network Components*", Future Security 2009, pp. 400-410, 29.09.-01.10.2009

[4] C. Adami, C. Braun, P. Clemens, M. Jöster, M. Suhrke, H.-J. Taenzer: „*High Power Microwave Tests of Media Converters*", EMC Europe 2012, 17-21.09.2012

[5] M. Joester, C. Adami, M. Suhrke, H.J. Taenzer: „HPEM Tests of Security Systems" AMEREM 2014 Albuquerque, ID040, 27.-31.07.2014

[6] Ch. Adami, M. Joester, T. Pusch, M. Suhrke, H.-J. Taenzer: „*Generation dependence of communication device vulnerability to intentional electromagnetic interference (IEMI)*" Future Security 2015 Berlin, pp. 347-354, 15-17.09.2015

[7] IEC 61000-4-36:2014-11 Ed. 1.0: „*Electromagnetic compatibility (EMC) – Part 4-36: Testing and measurement techniques – IEMI immunity test methods for equipment and systems*"