

IEMI – Bedrohungspotenzial von Flughäfen

Dipl.-Ing. Melanie Rohe, Hochschule Hannover, Elektro- und Informationstechnik
Dipl.-Kfm. Benjamin Cimander, FIS GmbH - Kelsterbach
Prof. Dr.-Ing. Michael Koch, Hochschule Hannover, Elektro- und Informationstechnik

1. Einführung

Moderne Kommunikationstechnologien und IT-Infrastrukturen sind notwendige Voraussetzungen für die sichere und reibungslose Abwicklung des Betriebes. Schnelle Informationsübermittlung, durchgängiger Zugriff auf Datenbanken sowie die Leitung des Verkehrsablaufes mit Hilfe vernetzter IT-Systeme sind für den effektiven und sicheren Betriebsablauf entscheidend. Eine Funktionsstörung, ein Ausfall oder die Zerstörung einzelner Systemkomponenten kann zu einem Ausfall des gesamten Netzes und somit zu erheblichen Störungen des Betriebsablaufes, bis hin zu katastrophalen Unfällen führen.

In diesem Beitrag wird eine Gefährdungsanalyse von Flughäfen gegenüber elektromagnetischen Bedrohungsformen durchgeführt. Dazu wird zunächst auf die Infrastruktur von Flughäfen eingegangen. Dabei wird anhand der Betrachtung mehrerer Flughäfen verdeutlicht, dass jeder Flughafen andere Schwachstellen aufweist und individuell analysiert werden muss. Anschließend werden zwei Formen elektromagnetischer Wirkmittel unterschieden: High Power Microwave (HPM) und Ultra Wide Band (UWB-Pulse). Insbesondere wird der Aufbau solcher Störquellen vorgestellt und daraus resultierend auch der nötige Aufwand und das dafür erforderliche technische Know-How verdeutlicht. Anhand einer Risikoanalyse werden die Störquellen nach diesen Kriterien und zusätzlich nach Kostenaufwand bewertet. Nach diesen Betrachtungen erfolgt ein Überblick über die notwendigen technischen und organisatorischen Maßnahmen, die im Fall eines elektromagnetischen Angriffs auf IT-Netze getroffen werden müssen.

2. Infrastruktur eines Flughafens

In den kommenden Abschnitten werden die Infrastrukturen von drei deutschen Flughäfen betrachtet und die wesentlichen kritischen Systeme hervorgehoben.

2.1 Flughafen Hannover

Neben den öffentlichen Verkehrsmitteln wie die S-Bahn, die sich direkt unter den Terminals befindet, stellen insbesondere die Serverräume, die Überwachungskameras sowie die Check-In Schalter kritische Systeme dar (Abbildung 1). An diesen Punkten wurden auch Messungen mit verschiedenen Antennenformen durchgeführt, um das gesamte Spektrum von 150 MHz bis 3 GHz abzudecken.



Abbildung 1 Kritische Systeme: a) Bereich vor dem Serverraum und b) Überwachungskameras

Da sich diese Systeme im öffentlich zugänglichen Bereich des Flughafens befinden, stellen sie im Wesentlichen eine potenzielle Störsenke für elektromagnetische Bedrohungsformen dar. Insbesondere der Serverraum ist verwundbar, da er nur durch eine Kalksteinwand vom öffentlichen Bereich getrennt ist. In vergangenen Untersuchungen [1] wurde gezeigt, dass diese zwar eine gewisse Schirmdämpfung (SE: Shielding Effectiveness) aufweisen, aber trotzdem eine ausreichende Feldstärke innerhalb des Raumes generieren, um die Netzwerke zu stören. Für die Berechnung der elektrischen Feldstärke E_2 innerhalb des Serverraumes kann die Schirmdämpfung herangezogen werden.

$$SE_E (dB) = 20 \log \left(\frac{E_1}{E_2} \right) \quad (1)$$

Für die leistungsbezogene Schirmdämpfung gilt:

$$SE_P (dB) = 10 \log \left(\frac{P_1}{P_2} \right). \quad (2)$$

In [1] ist die Schirmdämpfung verschiedener Materialien wie zum Beispiel Gipskarton oder Kalksandstein angegeben. Wird davon ausgegangen, dass es sich bei der Wand des Serverraumes um Kalksandstein der Wandstärke 150 mm handelt, ist eine Schirmdämpfung von 5 - 9 dB angegeben. Die von der Firma Diehl BGT Defence entwickelte Quelle DS110 in Kofferform hat eine Ausgangsspannung von $U_1 = 220$ kV bei 350 MHz. Nach (1) kann davon ausgegangen werden, dass in einer Entfernung von 6m eine Feldstärke von ca. 40 kV/m gemessen wird. Durch die Kalksandsteinwand wird damit ein elektrisches Feld der Stärke $E_2 = 15$ kV/m bei 9 dB Schirmdämpfung innerhalb des Serverraumes hervorgerufen. Allerdings haben die IT-Systeme einen gewissen Abstand zur Wand und befinden sich meistens in metallischen Gehäusen. Diese sind aber nicht vollständig verschlossen, sondern müssen auf Grund der hohen Wärmeleistung offen sein. Trotzdem kann eine ausreichende Feldstärke vorhanden sein, um Subsysteme zu stören. Die Ausfallsschwellwerte verschiedener Systeme können zwischen 2 und 18 kV/m liegen [2]. In Abbildung 2 ist ein Beispiel für den Aufbau eines Servers dargestellt.



Abbildung 2 Serverschrank

Neben dem Monitor stellen auch insbesondere die Kabel potenzielle Störquellen dar. Außerdem wird aus der Abbildung 1 a) deutlich, dass ein Kabel aus dem Serverraum durch die Wand direkt nach außen zu einer Steckdose führt. Über dieses Kabel können sich ebenfalls Störströme in dem Energieversorgungsnetz ausbreiten. Zusätzlich fallen die Überwachungskameras im Terminal in der Abbildung 1 b) auf.

2.2 Flughafen Frankfurt

Der Flughafen Frankfurt hat eine ganz andere Größenordnung und gehört zu den größten Flughäfen Deutschlands. Er weist damit eine andere Infrastruktur auf, als der Flughafen Hannover. Einen sehr guten Überblick liefert die Abbildung 1-3.



Abbildung 1-3 Luftaufnahme des Frankfurter Flughafens

Sie zeigt deutlich, dass Überwachungssysteme wie der Tower und das Instrumentenlandesystem (ILS) aus dem öffentlichen Bereich nicht zugänglich sind. Daher stellt die elektronische und elektrische Infrastruktur (z.B. Energieversorgungsnetze) der Terminals und die öffentlichen Verkehrsmittel den wesentlichen Schwachpunkt dar.

2.3 Flughafen Düsseldorf

Die Abbildung 1-4 gibt einen Überblick über den Flughafen Düsseldorf (DUS).



Abbildung 1-4 Luftaufnahme des Düsseldorfer Flughafens

Aus der Abbildung 1-4 geht deutlich hervor, dass sich der Tower direkt an der Zufahrtstraße befindet und damit eine potenzielle Angriffsfläche bietet. Weiterhin ist aufgefallen, dass der Fernbahnhof, eine Zufahrtstraße sowie der Skytrain sich direkt hinter der Start- und Landebahn befinden. Sie sind lediglich durch einen einfachen Maschendrahtzaun vom öffentlichen Bereich getrennt. Das Instrumentenlandesystem hat eine Entfernung von ungefähr 30m zum Zaun. Elektromagnetische Störquellen in mobiler Form haben eine Reichweite von ca. 50m und stellen damit eine Bedrohung dar.

3. Elektromagnetische Wirkmittel

In diesem Paper werden im Wesentlichen zwei elektromagnetische Wirkmittel unterschieden: Ultra-Wide-Band (UWB) und High Power Microwave (HPM). Die Eigenschaften dieser Pulsformen werden in den kommenden Abschnitten näher erläutert.

3.1 Ultra-Wide-Band (UWB)

Der UWB Puls zeichnet sich durch eine Kurve sehr kurzer Anstiegszeit und Pulsdauer aus. Dabei wird die Anstiegszeit zwischen den Punkten der 10% und 90% der maximal erreichbaren Amplitude gemessen. Moderne Pulsgeneratoren erreichen eine Anstiegszeit von 100 ps und können eine Ausgangsspannung von bis zu 50 kV generieren. Die Anstiegszeit charakterisiert den Frequenzbereich des UWB Pulses, der sich über mehrere GHz erstrecken kann. Das hat den wesentlichen Vorteil, dass mit zunehmender Wahrscheinlichkeit die Schwachstelle eines IT-Netzes getroffen und damit gestört werden kann.

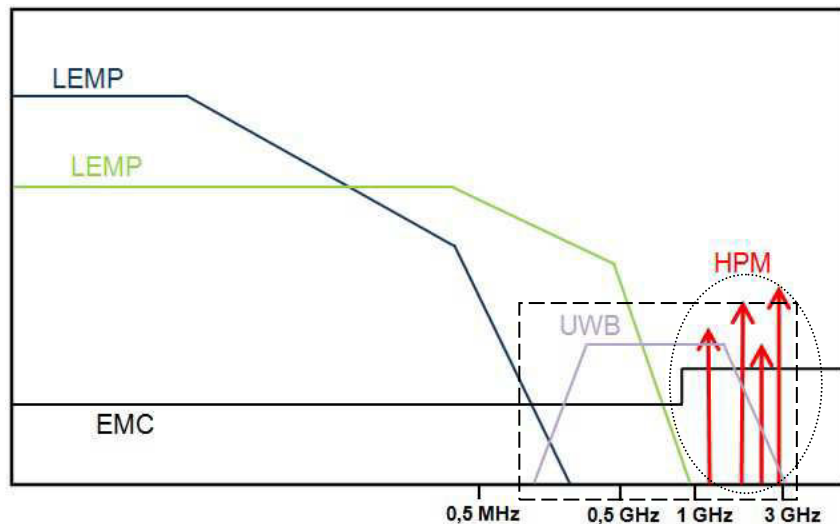


Abbildung 5 Spektrum verschiedener Pulsformen

Aus anderen Veröffentlichungen [2] und eigenen Messungen [3] geht deutlich hervor, dass gängige Systeme wie PCs, Kommunikations- und Überwachungssysteme empfindlich auf Pulse reagieren, die einen Frequenzbereich zwischen 200MHz und 2 GHz abdecken. Neben dem Frequenzbereich ist auch die maximal generierbare Amplitude ein wichtiger Faktor. Bei einem Puls mit Ultra Wide Band Charakteristik verteilt sich die gesamte Leistung über das genannte Spektrum. Abbildung 5 gibt einen Überblick über die Spektren verschiedener Pulsformen, wobei das eines UWB Pulses durch die gestrichelte Linie gekennzeichnet ist.

3.2 High Power Microwave (HPM)

HPM-Quellen zeichnen sich dadurch aus, dass sie bei einer bestimmten Frequenz eine sehr hohe Amplitude der elektrischen Feldstärke aufweisen. HPM-Quellen werden häufig im Frequenzbereich von 1GHz bis 3GHz betrieben.

Das Grundprinzip ist die Wandlung kinetischer Energie eines Elektronenstrahls in die elektromagnetische Energie einer Mikrowelle durch die Wechselwirkung zwischen elektromagnetischen Wellen und geladenen Partikeln. Im kommenden Abschnitt wird unter anderem der Aufbau einer HPM-Quelle beschrieben. Auf der rechten Hälfte der Abbildung 5 ist der Frequenzbereich einer HPM-Quelle durch eine gepunktete Linie markiert.

4. Aufbau von Wirkmitteln

Dieser Abschnitt umfasst den Aufbau von UWB- und HPM-Wirkmitteln, die in den vergangenen Kapiteln ausführlich beschrieben wurden.

4.1 UWB

Wie bereits in Abschnitt 3.1 verdeutlicht, entspricht ein UWB-Signal einem Puls sehr kurzer Anstiegszeit und damit einer großen Bandbreite. Die Abbildung 6 zeigt die grundlegende Funktionskette.

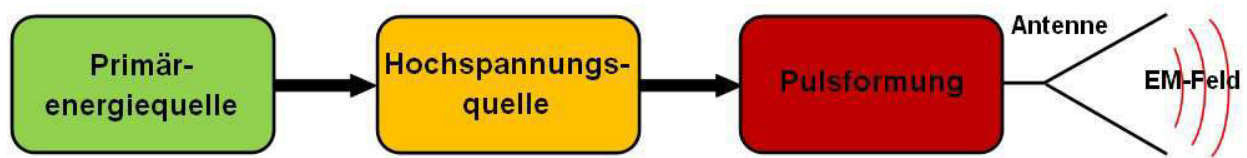


Abbildung 6 Funktionskette einer UWB-Quelle

Als Primärquelle kann zum Beispiel ein 24V Akku-Pack genutzt werden (Abbildung 7 a). Die Ausgangsspannung der Batterie kann über einen Marxgenerator verstärkt werden. Bei einem Marx-Generator werden mehrere Kondensatoren parallel aufgeladen und anschließend über Funkenstrecken seriell entladen. Durch die Funkenstrecken sind die Kondensatoren in Reihe geschaltet (Abbildung 7 b). Das bedeutet, dass sich die Spannungen der einzelnen Kondensatoren addieren und am Ausgang des Marx-Generators einige kV abgegriffen werden. Die Ausgangsspannung wird anschließend in einem HV-Kondensator zwischengespeichert. Um einen kurzen Puls zu erzeugen, muss die Ausgangsspannung geformt werden. Das kann zum Beispiel über eine Funkenstrecke erfolgen (Abbildung 7 c). Der bei der Pulsformung abgegebene elektromagnetische Puls wird anschließend über eine Antenne in den freien Raum abgestrahlt (Abbildung 7 d) [4].

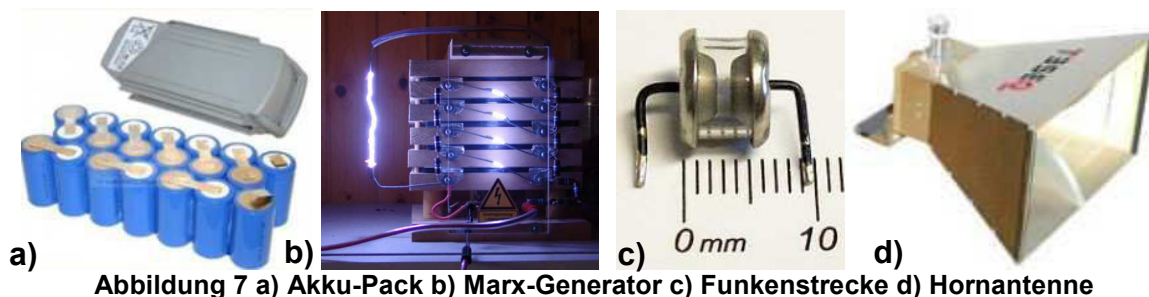


Abbildung 7 a) Akku-Pack b) Marx-Generator c) Funkenstrecke d) Hornantenne

Bei der Zusammenführung der Komponenten muss die Anpassung berücksichtigt werden. Dies betrifft insbesondere den Übergang von der Pulsformung zur Antenne. Es muss darauf geachtet werden, dass der gesamte elektromagnetische Puls in den Raum über die Antennenstruktur abgestrahlt wird.

Vom Wehrwissenschaftlichen Institut für Schutztechnologien und ABC-Schutz wurde ein elektromagnetisches Wirkmittel aus gängigen elektrischen Komponenten gefertigt und in einem Aktenkoffer verbaut. Die selbstgebaute Störquelle erreicht eine Ausgangsspannung von 12 kV und hat eine Reichweite von ungefähr 8 m. Für die Fertigung sind Grundkenntnisse der Elektrotechnik völlig ausreichend. Die Kosten für das Material betragen ca. 1000 €.

4.2 HPM

Für ein HPM-Wirkmittel kann das Magnetron verwendet werden. Abbildung 8 zeigt den typischen Aufbau dazu [4]. Ein Magnetron besteht aus einer Kathode zylindrischer Form, die ringförmig von einem Anodenblock umgeben ist. In die Anode wurden Hohlräume und Schlitze gefräst. Wird eine Spannung angelegt, verlassen die Elektronen die Kathode und bewegen sich auf die Anode zu. Parallel zur Kathode existiert ein Magnetfeld, sodass die Elektronen durch die Lorentzkraft abgelenkt werden. Damit kreisen die Elektronen um die Kathode. In den Hohlräumen bildet sich ein elektromagnetisches Feld aus, sobald die Elektronen an den eingefrästen Schlitzen vorbeikommen.

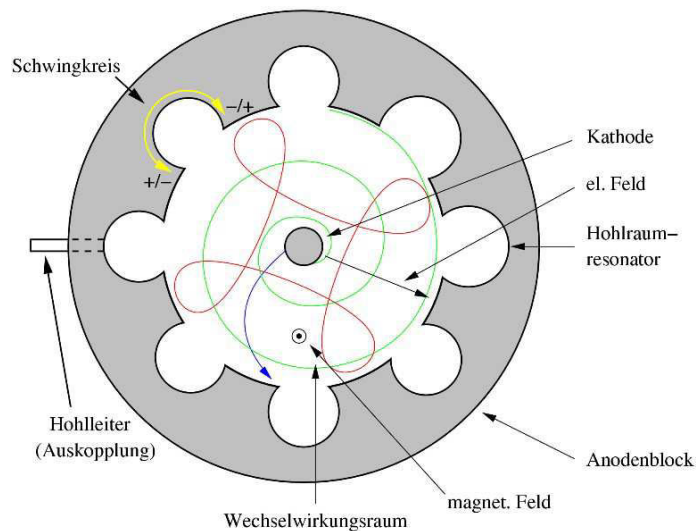


Abbildung 8 Aufbau eines Magnetrons

Das führt dazu, dass die elektromagnetischen Felder auf die im Wechselwirkungsraum kreisenden Elektronen zurückwirken. Einige Elektronen werden beschleunigt und andere wiederum abgebremst. Die dadurch gebildeten Elektronenwolken verstärken die hochfrequente Schwingung.

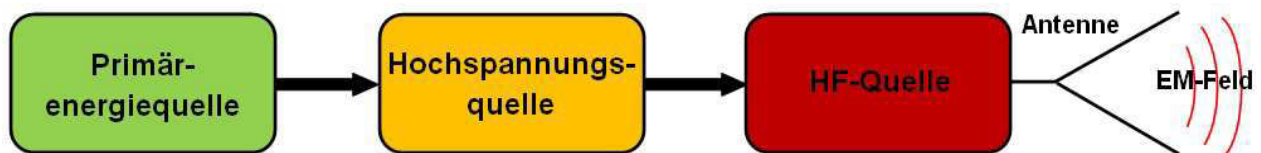


Abbildung 9 Funktionskette einer HPM-Quelle

Abbildung 9 zeigt die Funktionskette einer HPM-Quelle. Dabei sind die Primärquelle und die Hochspannungsquelle identisch zur UWB-Quelle. Als HF-Quelle wird das in Abbildung 8 dargestellte Magnetron eingesetzt. Auch da muss die die Antennenanpassung berücksichtigt werden.

5. Technische und organisatorische Maßnahmen

Sind im Störfall Check-In-Computer in einem bestimmten Bereich des Flughafens betroffen, so werden die Passagiere in andere Terminals umgeleitet. Zeitgleich versuchen die Techniker das Problem zu beheben. Wesentlich kritischer ist es, wenn das Buchungssystem betroffen ist. Dann wird es schwierig bis unmöglich die Flugzeuge ohne Verspätung mit allen Passagieren an Bord starten zu lassen. Das führt zu einem hohen wirtschaftlichen Schaden des Flughafens [5]. Gleiches gilt auch für den Ausfall von Überwachungssystemen (zum Beispiel das Radar). Die Deutsche Flugsicherung (DFS) versucht dann auf alternative Systeme zurückzugreifen. Sollte dies nicht möglich sein, muss gegebenenfalls ein anderer Tower übernehmen oder Flüge müssen umgeleitet werden. Unter Umständen muss der Flugbetrieb eingeschränkt oder eingestellt werden. Für die Aufklärung dieses Szenarios sind verschiedene Sicherheitskräfte zuständig. Der Bereich innerhalb des Flughafengeländes ist das Einsatzgebiet der Bundespolizei, die von Luftsicherheitskontrollkräften und Luftsicherheitsassistenten unterstützt wird. Außerhalb der Begrenzung des Flughafengeländes ist die Landespolizei für die Sicherheit

verantwortlich. Bezüglich der Gefährdung durch elektromagnetische Wirkmittel muss das Personal des Flughafens nochmal gezielt geschult werden.

Aus technischer Sicht ist es sinnvoll für zukünftige Planungen der Infrastrukturen solche Szenarios mit zu berücksichtigen. Das umfasst zum Beispiel die gezielte Auswahl richtiger Komponenten wie Kabel, die vorab eine bessere Schirmung aufweisen (zum Beispiel CAT7). Maßnahmen wie die nachträgliche Installation von Schirmungen sicherheitskritischer Systeme sind zu kostenaufwändig. Eine weitere Möglichkeit zum Schutz kritischer Infrastrukturen ist die Installation von Sensoren, die die Störquellen orten. Sie unterscheiden Störsignale von der gängigen elektromagnetischen Umgebung. Die Störsignale sind allerdings nur über einen begrenzten Zeitraum vorhanden und müssen schnell erfasst werden. Das kann die Speicherkapazität des Überwachungssystems sprengen, da ein UWB Puls eine Pulsdauer von wenigen Nanosekunden aufweist. Außerdem müssen rechtliche Vorschriften wie die Wahrung der Privatsphäre berücksichtigt werden. Aktuell wird auf diesem Gebiet weiter geforscht.

6. Zusammenfassung

Neben der Betrachtung von drei Flughäfen wurde ein Serverraum des Flughafen Hannovers näher analysiert. Dabei zeigte sich deutlich, dass trotz des Wandmaterials noch ausreichend Feldstärke innerhalb des Raumes erzeugt wird. Damit sind die Systeme anfällig für elektromagnetische Störfelder. Außerdem wurde anhand des Aufbaus eines UWB- und HPM-Wirkmittels verdeutlicht, dass diese Störquellen mit dem Grundwissen der Elektrotechnik umgesetzt werden können. Die dafür benötigten Komponenten sind in sämtlichen Elektronikfachmärkten frei verfügbar und günstig zu erwerben. Die organisatorischen Maßnahmen umfassen die Benachrichtigung der zuständigen Sicherheitskräfte und deren Eingriff. Dies geschieht bei der Vermutung, dass es sich gezielt um eine bewusst hervorgerufene Störung handelt. Außerdem werden Techniker und Mitarbeiter der Deutschen Flugsicherung vor Ort bestellt, um das Problem zu beheben. Nachträgliche Installationen, die die Zuverlässigkeit der technischen Einrichtungen gewährleisten, sind zu kostenaufwändig. Diese Maßnahmen sollten bereits in der Planung berücksichtigt werden. Eine Verbesserung kann die Ausstattung des Flughafens mit einem Sensornetzwerk sein, das Störsignale von Nutzsignalen unterscheidet und ortet.

7. Literaturverzeichnis

- [1] Frenzel, T.: „Schirmung kritischer Infrastrukturen“, Dissertation, Leibniz Universität Hannover, 2011
- [2] Camp, M.: „Empfindlichkeit elektronischer Schaltung gegenüber elektromagnetischen Feldimpulsen“, Dissertation, Leibniz Universität Hannover, 2004
- [3] Rohe, M.: „Breakdown Behavior of a Wireless Communication Network under UWB Impact“, EUROEM 2012, Toulouse/France
- [4] Sabath, F.: „IEMI-Intentional Electromagnetic Interference“, Vorlesung WS 07/08, Leibniz Universität Hannover
- [5] EUROCONTROL: „European Airline delay cost references values“, University of Westminster for PRU, 2008