Assessment of Electromagnetic Field Threats to a Military Airport

D. V. Giri[(1)] and F. M. Tesche[(2)]
(1) Pro-Tech, 410 Washington Street, # 1, Wellesley, MA 02481, USA
(2) EMConsultant, USA

*Corresponding author, E-mail: Giri@DVGiri.com

Abstract

A recent area of concern is how to insure the continued functioning of critical elements of societal infrastructure amid increasing forms of terrorist activities. One new threat is the use of an HPEM source to create intentional electromagnetic interference (IEMI). This threat involves deliberately illuminating a facility or sub-system with a sufficiently intense EM field, to cause an interruption in the normal operation of the facility's electrical equipment. This effect is similar to electronic jamming, which has been used for years, but technological advances in high-power radio frequency (RF) sources and antennas now makes it possible to not only jam (or interrupt) equipment, but also to permanently damage (burn-out) equipment [1].

1. Introduction

This presentation, based on [2] describes the results of an assessment of the possible effects of an attack on a military airfield in Switzerland, using a high-power electromagnetic (HPEM) source. While such electromagnetic (EM) weapons systems are not commonplace today, there have been documented cases in the past of their being used for criminal activity. Moreover, with the rapid increase of EM source technology, it is possible that such EM weapons could pose more of a threat to critical elements society's infrastructure in the future. A general overview of the EM assessment methodology process is provided. Assessments can be performed at several levels of detail. Starting with a description of the airport, the type of assessment conducted at the airport is discussed. Important EM systems are identified. We also describe EM vulnerability estimates for various types of airport equipment, which are needed for performing an assessment. The characteristics of EM fields that could be used to target, are discussed. The nature of the EM environment is summarized, together with the details of the antennas and various source generators that might be used to produce these fields. Several EM attack scenarios that are envisioned at the airport are presented. This analysis provides an indication of the possible EM environments that could be used in such attacks, and it discusses the possible effects on the airport operations.

Civil aviation has become an integral component of present-day societies. It promotes an economic base for a community, assists and encourages trade, and is vital for the health, safety and welfare of the general public. Yet, we all know some of its vulnerabilities even from very low-level electromagnetic emitters. For example, cell phone use is prohibited in at least the takeoff and landing phases of a flight, due to its potential adverse effects on navigational electronics on-board the aircraft. Other passenger electronic devices (PED) such as lap-top computers, DVD players etc., have been known to cause interference and are prohibited during the take-off and landing phase of a commercial flight. In addition to these low-level emitters, both military and civilian aircrafts are routinely required to operate under adverse electromagnetic environments (EME), such as

- Natural- lightning electromagnetic pulse (N-LEMP)
- Electrostatic discharge (ESD)
- Electromagnetic environment in and around airports
- Intra-system electromagnetic interference (EMI)
- Inter-system EMI.

2. High Intensity Radiated Fields (HIRF) Fields

These HIRF certification levels are plotted in Figures 3 and 4 are important because if an intentional RF weapon system produces a HIRF level that exceeds the above levels by an order of magnitude, serious consequences may become possible.

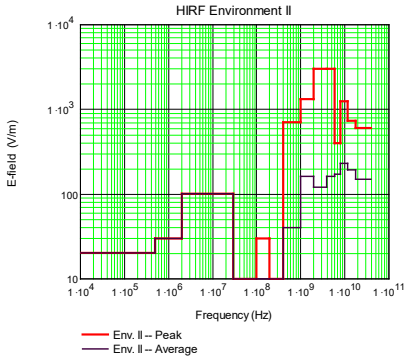

Figure 1 HIRF Type II Environments (effective September 2007).

From the examples cited above and the FAA / JAA standards it is safe to conclude that unintentional electromagnetic signals can pose a threat to aviation. It is entirely possible that RF terrorism [3 and 4] can bring such threats with intentional electromagnetic signals.
Furthermore, airports cannot run without networked computers operating in unison. Ground components such as, passenger terminals, air-traffic management (ATM) and airport vehicles are also subject to potential RF threats. There may not be a loss of life as in the case of loss of aircraft, but severe disruption of aviation services can be the price to pay. A coordinated RF attack on several passenger terminals aimed at disrupting networked computers [5, 6 and 7] can have serious psychological and economic consequences.

3. A Topological View of an Airport

A civilian airport is a facility where three components of air transportation system come together [8], as illustrated in Figure 2.

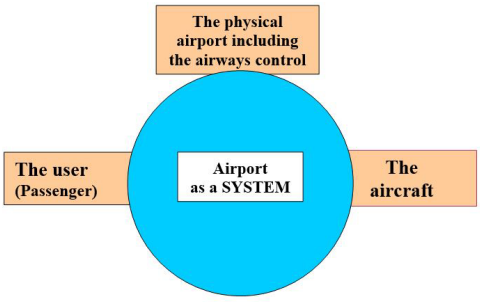

Figure 2. A system theoretic view of an airport

A typical airport operation includes, but not limited to, the following:

• Air Traffic Control • Telecommunications • Meteorology • Approach and Landing Aids • Runway Lighting • Air Field Inspections • Air Operations in Bad Weather Conditions • Power System Management • Passenger Service • Baggage Operations • Ground Handling • Airport Security	• Baggage Operations • Emergency Management • Personnel Requirements • Fire-Fighting Equipment and Readiness • Access Control • Authorized Ground Vehicles • Foaming the Runway when Needed • De-icing the aircraft when Needed • Airport Terminal Operations • Noise Control Strategies, etc • Licensing and Certification issues • Noise Control Systems

From an electromagnetic viewpoint, the following systems are of present interest to us.

- RF interfaces
- Power
- Telecommunication including navigational aids
- Air Traffic Management/Equipment(ATM/ Equipment)

4. Summary

The site survey that has been performed has resulted in a set of key places of the airport, where it would be desirable to measure the operating RF environment. This task has involved going to these parts of the airport and measure the EM environments that typically exist at different times of a typical day at the airport without involving the use of any kind of transmitters, but consists of only passive sensors, network analyzers / oscilloscopes. The passive sensor acts like a broad band receiving antenna over a frequency range of (1MHz to 4 GHz) and measures the RF environment. We have also made a determination of RF threat scenarios including electromagnetic coupling to selected systems such as aircraft in glide slope, control tower etc.The results of the measured data will feed into a determination of what it takes to disrupt the airport operation. Given the public access and proximity to the glide path of the aircraft, control tower, etc., we can then go on to determine what type (frequency, power levels, antenna aperture, directivity etc.,) of an RF weapon that can be potentially disrupt airport operations. Are such mobile RF weapons feasible, given the state-of-the-art in source technology? What are the consequences for aircraft and airport operations?

We can analyze several attack methods and several scenarios have been quantified. (Weapon type and characteristics, propagation losses, field on target)

References

[1] R. L. Gardner, “Electromagnetic Terrorism. A Real Danger” Proceedings of the XI th Symposium on Electromagnetic Compatibility, Wroclaw, Poland, June 1998,

[2] D, V, Giri, F. M. Tesche, P. F. Bertholet and M. Nyffeler, “A Preliminary Assessment of Radio Frequency Threats to Airports”, Interaction Note 634, 28 January 2020.

[3] W. A. Radasky, M. A. Messier and M. W. Wik, “Intentional Electromagnetic Interference (IEMI) - Test and data implications,” in Proceedings Zurich Symposium, Switzerland, February 2001.

[4] The URSI “Resolution of Criminal Activities using Electromagnetic Tools”, International Radio Scientific Union, General Assembly, 1999.

[5] R. Hoad, et al, 'Trends in EM susceptibility of IT Equipment', IEEE Transactions on EMC, Vol. 46, No. 3, August 2004.

[6] R. Hoad, et al, 'An Investigation into the radiated susceptibility of IT Networks', Conference Proceedings of EMC Europe, September 2004, Eindhoven, The Netherlands.

[7] R. Hoad, A. Lambourne and A. Wraight, 'HPEM and HEMP susceptibility assessments of computer equipment', EMC Zurich in Singapore, Singapore, Asia, February 2006.

[8] N. Ashford, H. P. Martin Stanton and C. A. Moore, Airport Operations, second edition, McGraw Hill, 1997.