POTENTIAL IEMI THREATS AGAINST CIVILIAN AIR TRAFFIC

D. J. Serafin [(1)] , Dr D. Dupouy [(2)]

[(1)] DGA/DET/CEG, Centre d'Etudes de Gramat, 46500, Gramat, France
Email : dominique.serafin@dga.defense.gouv.fr
[(2)] As [(1)] above, but Email :didier.dupouy@dga.defense.gouv.fr

1 INTRODUCTION

Intentional EMI take an increasing importance in our daily environment, due to the evolution of the technology (higher power EM sources, more EM sensitive electronics) combined with the emergence of new kinds of criminal activities involving EM tools. Civilian infrastructures and systems particularly, first because of a supposed lower level of protection (compared to military one's), secondly because of a greater psychological impact on the population, could be preference targets for EM terrorism. Starting from general considerations and theoretical assumptions, this paper deals with potential IEMI threats applied to civilian air traffic, using basic data coming from open literature.

2 GENERALITIES

The general principle for the use of an EMI source (or RF weapon) against selected targets is based (see Fig. 1) on 3 different aspects: the generation of the EM waves, their propagation between the radiating part of the IEMI source and the target, and their interaction with its. Depending of the characteristics of the produced EM waves, the RF weapon can be classified as a narrowband, wideband (damped sines) or ultrawideband (UWB) system [1]. In this paper, we focus on RF weapons providing EM waves in a frequency band ranging from 0.2 to 5 GHz.

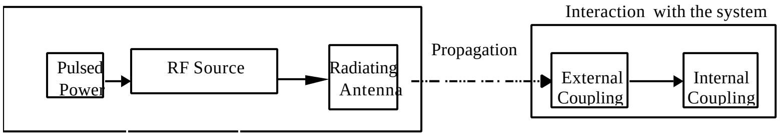


Fig. 1 . General philosophy for an RF attack

Standard narrowband RF weapons are constituted by a pulsed power source (capacitor bank storage coupled to a Marx generator for example) providing high energy electron beam, a microwave tube transforming the input energy electron beam into an output high frequency wave (magnetron, klystron, reltron, vircator, BWO,…) and an antenna forming the radiating part of the system (parabolic reflector, horn antenna,…). Typical narrowband RF weapon characteristics, coming from open literature [2], are reported on Table 1. Wideband and UWB RF systems, designed to produce very short duration pulses of very high power, use different power sources (explosive device generator based on the flux compression principle for example), with sophisticated techniques (closing switches, pulse sharpening process,…) and specific antennas (see [3] for IRA design).

Table 1 : Typical characteristics of a RF weapon

Energy at the output generator (En)	100 J – 10 kJ	Pulse Repetition Frequency (PRF)	single shot to some 100 Hz
Output Power Microwave Source (P_{source})	100 MW – some GW	Duration of illumination (Tmax)	up to a few seconds
Performance of the Microwave Tube (1/R)	some % – some 10 %	Frequency range	200 MHz – 5 GHz
Pulse Width (Δ T)	some 10 ns – some 100 ns	Antenna Gain	15 – 40 dB

The rms electric field (or the density power dPI) at the target level location is simply calculated from the usual radar theory equation (1) where P_{source} is the output power microwave tube (W), G is the antenna gain (unitless), S_{11} is the antenna mismatching factor (unitless) and d is the distance source - target (m).

$$\mathrm{dPI\,(W/m^2)} = \frac{\mathrm{P_{source}.G.(1-|S_{11}|^2)}}{4p\ \mathrm{d^2}} = \frac{E^2(V/m)}{377\,\Omega} \qquad (1)$$

The incident energy couples to the internal elements of the target trough two common ways : front door coupling (via antennas, sensors,…) and back door coupling (penetrations through the apertures). The possible effects of RF coupling on electronics equipment range into five categories, depending of the characteristics of the stresses : no effect, interference (disappearing when the threat ceases), disturbance (with recovery of the system without external intervention), upset (recovery requiring a manual reset) and damage (latchup leading to components destruction, thermal or dielectric breakdown…). But finally, the most important is to know the impact on the mission the equipment is supporting.

3 CIVILIAN AIR TRAFFIC : POTENTIAL TARGETS.

An airport area could be a selected target for EM terrorism due to the high concentration of electronics equipment likely to be perturbed by EM threats, so producing broad chaos. In this theoretical approach, the main areas considered for a terrorist RF attack are the airport terminal, including registration and transit areas, the traffic control tower, the parking areas for the planes, and the touch down and take-off runways.

Potential targets inside these areas include communication and navigation systems devoted to flight aircraft and safety (ground stations and on board systems, with their antennas, receivers, transmitters,…), as well as computer networks (registration, airport occupancy management, traffic control,…) or service vehicles travelling on the multiple runways. For on board systems, only COM or NAV systems running in the band covered by the RF threat (0.2 to 5 GHz) are considered here : ILS Glide Slope (0.33 GHz), DME and TCAS (0,95-1,2 GHz), ATC (1-1,1 GHz), GPS (1,22-1,57 GHz), RA (4,2-4,4 GHz) and MLS (5-5,2 GHZ).

4 APPROACH DESCRIPTION.

A rigorous approach would consist in identifying critical equipment in the main areas, and for given operations, developing fault trees for example, then quantifying the susceptibilities of these critical equipment to the RF threat considered here. In our approach, where the RF threat is only considered in terms of radiated fields, we make the following assumptions :

- the terrorists use the RF weapon to cause as chaos as possible, but without particular knowledge of the criticity and the sensitivity of the aimed equipment (no specific output frequencies are considered),
- the minimum EM fields to generate on aircraft, considering on board systems and equipment, must be higher than those given by the certification HIRF environment. Taking account of the worst case requirements for JAA certification with an additional 6 dB margin [4], we retain an external E peak electric field value of 6 kV/m (or 9.5 W/cm^2) for our frequency range. After assessing the attenuation of the incident fields through the structure of the plane, the effects of the residual fields on the internal equipment will be estimated, either from the knowledge of their susceptibility levels given by existing standards specifications, or from experimental tests previously reported.
- ground based equipment, usually located inside Faraday cages, are not considered in this study, because of apparently high levels of EM fields to generate to perturb them,
- electric fields between, typically 1 to 10 kV/m (depending on the characteristics of the pulse) are necessary to induce perturbations (or more) on computer networks [1] [5],
- for vehicles moving on the airport area, available data point out that electric fields of some tens of kV/m could damage them [6].

The main characteristics of the estimated electric fields to generate in order to induce perturbations (or more) by back door coupling on potential targets considered inside an airport are summarized on table 2.

Table 2. Characteristics of electric fields to be generated by a narrowband RF weapon.

	E_{rms} or dPI	Frequency range	PRF
On board equipment	6 kV/m (≈ 9,5 W/cm^2)	0,5 – 5 GHz	1 – 250
Vehicles on the airport area	15 kV/m (≈ 60 W/cm²)	1 – 3 GHz	1 – 1000
Computer networks in terminal areas	1 to 10 kV/m (0,25 to 25 W/cm2)	0,4 – 5 GHz	1 – 1000

5 EM TERRORIST ACTIONS SCENARIOS CONSIDERED

Two basic threat scenarios are considered : a small RF weapon concealed inside a suitcase, placed near terminal computer network (with a range limited to a few tens of meters), and a truck-mounted RF weapon, which could be located near an airport with direct view on the runways (with a range extended to 1000 meters).

5.1 Small weapon inside a suitcase.

The target aimed is the computer network of the registration desks, inside the airport terminal. The source considered comes from a RF broadband weapon hidden in a suitcase, located at about 20 meters from the target, and able to produce the requires E-field level to cause perturbations or more (see left part of Fig. 2). The design of such a weapon could be that one described in [1], with batteries coupled to a Marx generator operating at 400 kV, radiating a peak power of 250MW with a multiturn cylindrical coil antenna, so able to deliver a peak E-field of about 6 kV/m at the required distance, with a center frequency near 400 MHz. This compact autonomous system, which radiates omnidirectionally, can operate by remote control, with a PRF of some Hz, during several minutes.

5.2 Weapon truck-mounted in the airport neighborhood.

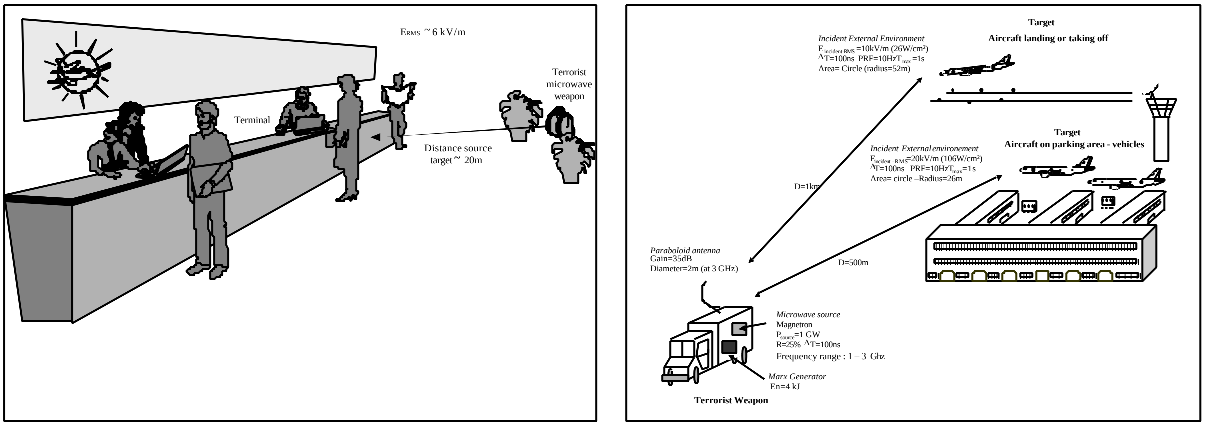
The targets considered here are aircraft either running on the runways near the park areas, or during landing or taking off operations. The RF source must be able to produce, in the considered frequency band, peak E-fields of about 10 kV/m at a distance of 500 meters in the first case (corresponding to P_{source}•G = 800 GW) or at 1 km in the second case (P_{source}•G = 3 TW).

Using, for narrowband pulses, a parabolic antenna with typical characteristics (G = 35 dB, -3 dB beamwidth = 6°), the illuminated surface is a circle with a diameter of about 50 m at 500 meters (and 100 m at 1 km). In these conditions, the RF power of the source must be P_{source} = 250 MW (or P_{source} = 1 GW) to have the desired E-field value at d = 500 m (or at d = 1 km).

A possible choice to obtain these values is a magnetron, operating between 1 and 3 GHz, with P_{source} = 1 GW and providing repetitive pulses with PRF = 10 Hz, pulse width Δ T = 100 ns during Tmax = 1s.
Prime power consists in batteries, then coupled to a Marx generator; the energy power E_n necessary to fulfilled the previous parameters are given in (2), where all the parameters are explained in table 1.

$$E_n = P_{source} \bullet R \bullet \Delta T \bullet PRF \bullet T_{max} \qquad (2)$$

For our application, taking R = 4 (corresponding to a 25% efficiency for the electrical / microwave conversion), the energy delivered by the Marx generator must be about 4 kJ. This scenario is summarized on right part of Fig.2.



E_{RMS} ~ 6 kV/m
Terrorist microwave weapon
Terminal
Distance source target ~ 20m
Target
Aircraft landing or taking off
Incident External Environment
$E_{incident-RMS}$ =10kV/m (26W/cm²)
ΔT=100ns PRF=10HzT_{max} =1s
Area= Circle (radius=52m)
Target
Aircraft on parking area - vehicles
Incident External environement
$E_{incident-RMS}$=20kV/m (106W/cm²)
ΔT=100ns PRF=10HzT_{max}=1s
Area= circle –Radius=26m
D=1km
D=500m
Paraboloid antenna
Gain=35dB
Diameter=2m (at 3 GHz)
Microwave source
Magnetron
P_{source}=1 GW
R=25% ΔT=100ns
Frequency range : 1 – 3 Ghz
Marx Generator
En=4 kJ
Terrorist Weapon

Fig.2:Terrorist scenarios using a small weapon inside a suitcase (left) or a truck-mounted big weapon (right)

6 APPLICATION TO AN RF ATTACK AGAINST ON BOARD NAV SYSTEM.

We focus on a typical aircraft equipment, like an on board NAV system (GPS, DME, TCAS, ATC,…) typically composed by an antenna (on the top of the fuselage), a receiver (inside the avionics bay) and a control/command panel, display unit or computer, located inside the cockpit. Assuming the cockpit is a semi-protected zone providing a 6 dB mean attenuation (from 1 to 3 GHz) and the avionics bay is a protected one with a 20 dB mean attenuation performance for the same frequency band, the residual electric fields at the equipment level are (with a 10 kV/m incident peak E-field) E ≈ 5 kV/m (dPI ≈ 6,5 W/cm²) for the display unit located inside the cockpit, and E ≈ 1 kV/m (dPI ≈ 265 m W/cm²) for the NAV receiver, inside the avionics bay.

Vulnerability thresholds for these equipment, according to the expected effects and the kind and the shape of the threat, are difficult to assess. On a GPS system for example, the effects can be as various as a drop of luminosity or a disappearance of the computer's screen, a non permanent (or permanent) loss of the user's position or even a latchup damaging and stopping the GPS operation. Taking account of the typical values given on Fig.3 with some experimental results [5][7], as a first approach, we can deduce that possible interference could occur; for selected frequencies, destruction is more probable by front door coupling, due to the extreme sensitivity of aircraft navigation systems. Experimental tests, using various characteristics of the RF threat (pulse width, PRF, frequency,…) must be achieved to confirm these trends.

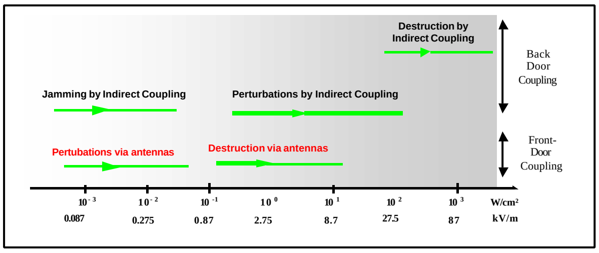


Fig. 3: Vulnerability thresholds of systems according to the effects induced and the type of coupling.

7 CONCLUSIONS

Based on theoretical assumptions and typical data coming from open literature, this paper describes a possible scenario of a terrorist EM attack against an airport, touching on the possible effects on typical on board aircraft system. Starting from general characteristics of an IEMI source, the scenario retained considers an RF truck-mounted weapon, aiming aircraft during take off and landing phases, able to produce a 10 kV/m peak E-field at 1 km. Assuming a "blind" weapon interacting with on board system by a back door coupling way between 1 and 3 GHz, and taking account of typical values of vulnerability thresholds for general systems and available experimental results, perturbations and permanent damages can possibly occur with the "reasonable" RF source characteristics considered here.

References

[1] Special issue on High-Power Electromagnetics (HPEM) and Intentional Electromagnetic Environments (IEME) *IEEE Transactions on EMC*, Vol. 46(3), August 2004.

[2] J. Benford and J. Swengle, "*High Power Microwaves*", Artech House, 1992.

[3] D.V.Giri, "*High-Power Electromagnetic Radiators, Non-Lethal Weapons and Applications*", Harvard University Press, 2004.

[4] "HIRF Standards for Aircraft Electrical and Electronical Systems". harmonized FAA/JAA Notices. EEHWG-WG 319. November 18, 1998.

[5] J.P.Percaille and D.Chastras, "HPM Susceptibility of PC", EUROEM 2004, 12-16 July 2004, Magdeburg, Germany

[6] M. Bäckström, "HPM testing of a car : a representative example of the susceptibility of civil systems", Workshop W4, 13th Int. Zurich Symposium and Technical Exhibition on EMC, February 1999.

[7] D. Dupouy, "Potential EM Threats : Evaluation of the vulnerability of a typical aircraft equipment", EM-HAZ-CEAT-REP-004 Report, March, 12, 2001.