High Power Microwave effects on alarm systems and components

***Jostein Godø*[1], *Odd H. Arnesen*[2], *Mats Bäckström*[3], *Brian A. Kerr*[4], *Ernst Krogager*[5]**

[1]Norwegian Defence Estates Agency, PO box 405, Sentrum, N-0103 Oslo, Norway, jostein.godo@forsvarsbygg.no

[2]Norwegian Defence Research Establishment, PO box 25, N-2027 Kjeller, Norway, odd-harry.arnesen@ffi.no

[3]Saab Communication, SE-581 88 Linköping, Sweden, mats.backstrom@saabgroup.com

[4]QinetiQ, Bldg B. Lovell Rm 123, Malvern Technology Centre, St. Andrews Road, Malvern, Worcestershire, WR14 3PS UK, bakerr@qinetiq.com

[5]Danish Defence Acquisition and Logistics Organization, Lautrupbjerg 1-5, DK-2750 Ballerup, Denmark, krogager@mil.dk

Abstract

This paper presents a compilation of results from a series of high power microwave (HPM) radio frequency interference (RFI) effects trials on alarm systems and components. The test objects represent a wide range of alarm and sensor technologies. Some HPM tests have been undertaken on some items in isolation and on the centrals with the detectors and card readers connected. The majority of the results are from the joint Nordic (DK, FI, NO, SE) HPM susceptibility experiments achieved at the Swedish Microwave Test Facility (MTF) combined with other Norwegian trials. Please note that due to commercial sensitivities that all brand names and the levels that the results were achieved at, are omitted due to classification restrictions.

1. Introduction

Security protection has always been an important issue, either against enemies, criminals or as it has been focused on in recent years, terrorism. Physical security measures can keep an intruder out for a certain time, depending on the intruder's resources and determination. Sustaining security requires some form of warning system and a reaction force and frequently these are normally electronic alarm or surveillance systems.

A huge variety of electronic alarm systems are available world wide. Usually alarm systems consist of one or more sensors, a central, and in larger systems sub-centrals, presentation unit and alarm centrals can also be integrated with automatic access control. The alarm sensors can be either PIR detectors (i.e. detecting heat changes when an intruder passes), seismic detectors (i.e. potentially detecting attempts to break through a wall), magnetic door detectors (i.e. detecting the opening of doors), and smoke detectors, etc. The output from the alarm sensors are sent to a central, which provides a message to the presentation unit, which could be a personal computer (PC) display in a surveillance centre, a bell or a SMS. Communication between the different units can be on dedicated cables, closed/open networks or via wireless communication. The quality and complexity of the alarm systems can vary considerably depending on the technology utilised and the exact makeup of the alarm system will depend on the expected threat and the size of the area to be protected.

2. The HPM threat

In recent years an increased level of awareness and attention has been paid to the potential threats posed by HPM RFI threats to the critical/important electronic systems within the main civilian infrastructure. Such system which could be targeted could be telecom, radio, television, financial systems, and computer systems/networks etc along with the alarm/warning systems which could also be susceptible to HPM RFI. Hence, it is possible that HPM RFI could be used against the alarm/warning systems, and then the key target(s) could then be attacked with either HPM RFI and/or other means before the reaction force is able to react and control the situation. There is an increased awareness of this type of threat reflected within the scientific community and in the public arena.

There is a distinct lack of RF immunity requirements and standards which protect electronic systems against HPM RFI treats and it is possible for a perpetrator to come physically close to the potential system which could be attacked. The EMC standard for alarm systems (EN 50130-4) sets the acceptance level to 10 V/m at frequencies up to 1 GHz. Fortunately, this paper indicates that the representative alarm systems and components which were tested in these studies are not particularly vulnerable to HPM RFI. However, an attacker does not need to have access to complex HPM sources since it is possible to get hold of commercially available radar transmitters or even simple "home-built" RF devices and they may be able to get extremely close to the electronic system(s) which they intend to interfere with.

3. HPM test series

The initial HPM RFI testing of alarm systems and components was a Nordic HPM trial in May 2004. The rationale behind the trial was to provide the DK, FI, and NO personnel with first hand experience of HPM RFI testing. The Swedish participants funded the operation of the MTF source, whilst the other nations provided the bulk of the test objects. Further trial was carried out at the MTF in 2006. As previously mentioned, this paper will focus on the findings from irradiation of alarm systems and components, but further results from these trials are published elsewhere [1-5].

These experiments were carried out at three spot frequencies: 1.3 GHz, 2.857 GHz and, 9.3 GHz. The calibrated peak field strengths at a test distance of 15 meters and other pulse parameters are shown in Table 1. In most cases an RF burst length of 10 seconds was used and some tests were undertaken with burst lengths of 1 second and also 3 seconds in order to determine if the duration of the irradiation changed the effects observed. At all frequencies used there were two different combinations of pulse waveforms used (a) low PRF with a long pulse length and (b) a high PRF with a short pulse length.

Table 1 Frequencies and pulse parameters in tests in May 2004.

Freq. (GHz)	Max. RMS field (kV/m)	PRF / Pulse length (Hz / μs.)		Polarization
		Long	Short	
1.3	29.0	390 / 4.5	950 / 1.0	Horizontal
2.857	17.5	200 / 4.5	950 / 1.0	Vertical
9.3	7.8	95 / 3.8	95 / 0.4	Vertical

4. Test objects

The test objects used during the 2004 Nordic trial focused on in this paper were an old alarm central with a seismic detector and a smoke detector, a newer central without sensors, PIR sensors and magnetic door sensors not connected to any central but powered, a card reader, and a Perimeter Defence Scenario with surveillance system of cameras and IR detectors connected wireless to a central which was not radiated. The wireless connection was kept outside of the main RF beam.

The test objects used during the other test series were other alarm centrals with detectors coupled by wire and wireless, proximity card readers connected to centrals and electric locks.

5. Results

The test results showed that the alarm central which utilised wireless communication with its sensors, was relatively easy to disrupt by RF jamming. When the central was radiated by a small portable RF source, it did not receive any signals from its sensors, and it was possible to physically pass the sensors without an alarm being initiated. The test conducted with the central which utilised wire connections between its sensors was radiated with an RF beam in a similar way as undertaken during the previous test assessment, and this system worked as usual, and it was able to detect what it was supposed to before, during and after the RF assessment.

The perimeter defence/alarm system also used wireless communication. However, when that system was illuminated with RF and the communications links degraded, the monitoring system would indicate that there were problems with the system, for example, the display images turned from colour pictures to black and white images, or large white pixels would appear in the picture, or a free running image without monitor synchronization was observed and then finally message was displayed when the communication link was totally lost. In some cases this system would

also alarm from the IR sensors when the external interfering RF was turned off and this could happen in such a way that it appeared to be a random effect, and at higher electric field strengths this effect was not always observed. Another sign of RF interference on this system was the white stripes which crossed the screen when the camera was irradiated with RF. Due to the cost of these systems described above they did not go through to destructive testing.

The first indication of RFI disruptive effects on the old alarm system was when the tamper alarm was triggered during S-band RF illumination. During L-band RF illumination the control display was filled with a repeated single digit, although it was still possible to operate the system. During increased electric field exposure the display filled with another digit, but during this test the central lost its program and it could not be restarted.

A newer alarm central was exposed to S-band RF and its clock was reset, whilst during L-band RF exposure the central was frequently switched off, and it had to be disconnected from its power supply prior to restarting. During repeated RF exposure the central started to indicate that its power supply was at a low voltage, and finally the display became unreadable.

Table 2 Results from testing an alarm central. The electric-field strengths are shown as Arbitrary Units (AU).

Frequency PRF Duration	1 AU	2 AU	4 AU	6 AU	8 AU	11 AU
1,3 GHz low PRF 10 s	No reaction	No reaction	Needed long power disconnection before restart			
1,3 GHz low PRF 1 s			Clock reset	Blank display, clock not reset, restart with code		
1,3 GHz low PRF 10 s	Deadlocked, had to be restarted	Clock reset	Blank display, restart with code	Indicating low voltage	Had to disconnect power before restart. (no longer low voltage)	Display unreadable (last test)
1,3 GHz high PRF 10 s	No reaction	No reaction	Had to disconnect power before restart			
2,857 GHz high PRF 10 s	Clock reset	Clock reset	No reaction			
2,857 GHz low PRF 10 s	No reaction	No reaction	No reaction			

Another new central was tested at a different facility and that also exhibited the same RFI effects and had to have its mains power recycled before it restarted. When the central was exposed to slightly lower electric field levels it indicated that there was a system error and that the PIR sensors were triggered. Three separate PIR detectors (not connected to a central) were stopped after RF exposure, but it was not possible to monitor if they were triggered by the onset of RF radiation, although the seismic detector was triggered by the onset of microwave radiation. The first PIR detector was damaged early on during the S-band testing program although another type of PIR detector only needed a restart after the highest level of RF testing. After six months the PIR sensors functionally was retested and the defective sensors appeared to have recovered some of their functionality.

It was possible to visually monitor some of the PIR's during the RF tests and a range of effects were observed. In some cases the PIR's were triggered during RF exposure, and some PIR's were activated a short period after RF illumination.

The card reader tested in Sweden survived all the RF tests. During other HPM trials the card readers were connected to centrals and the proximity card readers worked until the central had lost its records of the cards. The card readers themselves worked but the central had failed. There was initially a temporary reset but the system then recovered and continued to work. At higher electric field strengths the central was deadlocked and needed to be shut

down for a period of time it would restart. After the last higher power RF tests the central was damaged but it recovered its functionally again after several weeks, before it worked again. One electric lock was damaged during the RF tests.

6. Summary

This HPM RFI investigation of electronic alarm and access control systems is in its early phase and only includes a limited number of control systems and components. However, these trials show that there is a wide range in RF robustness for different types of alarm systems. Wireless systems are especially susceptible to being interfered with and jammed in band radiation and the cheaper/simpler systems there was no indication of a malfunction or indication that the system was not working. Hence, a cabled system would appear to be more robust against this type of RF threat.

The card readers tested, including the proximity card readers appeared to be significantly more robust against these RF waveforms, .although this may be attributed to the fact that the RF frequencies used during the tests were out of band of the proximity reader. The weakest component for all of the systems tested were the centrals for the readers even though they were housed in an unshielded metal box. It is this component which should be located in a less vulnerable location and/or more adequately screened against RFI.

This also applies for the alarm centrals which should be hidden and better screened against RFI. During the HPM tests the trigger level for the PIR sensor was approximately the same as the disturbance level for the central and in relation to these tests during the Swedish test the seismic detector was triggered at a much lower level of RFI. Although no further studies were undertaken which adjusted the sensitivity of the seismic detector. In some of the trials with the PIRs, they were triggered at low electric field strengths, but they were not necessarily triggered at higher electric field strengths.

Hence, PIR sensors have a wide range of RF susceptibility levels and they can regain most of their functionality after being stored after a period of time post RFI testing, although they become more unreliable after repeated RF exposure.

7. Acknowledgments

This work was supported in part by the Swedish Armed Forces.

8. References

1. T. Nilsson, O. Lunden, M. Bäckström, HPM Susceptibility Measurements on WLAN and GPS Systems, EMC Europe Workshop, Rome, September 2005.

2. O.H. Arnesen et al., High Power Microwave Effects on Civilian Equipment, URSI General Assembly, New Delhi, October 2005.

3. O.H. Arnesen et al., IEMI against Modern Civilian electronic Technologies, EMC Zurich, Singapore 2006.

4. O.H. Arnesen et al., High Power Microwave Effects on Civilian Wireless Equipment, EMC Europe Workshop, Rome, September 2005.

5 O.H. Arnesen et al., IEMI susceptibility of data links in local area computer networks; wlan and fibre optics versus copper cable, EMC Europe Workshop 2007, Paris 2007.