

HPEM and HEMP Susceptibility Assessments of Computer Equipment

R. Hoad, A. Lambourne and A. Wraight

QinetiQ, Electromagnetic Compatibility Group, Building A5, Room 1005,
Cody Technology Park, Ively Rd, Farnborough, Hants, GU14 0LX, UK

E-mail: emcfocus@qinetiq.com

Abstract

This paper provides a summary of recent susceptibility assessments conducted by the QinetiQ EMC group. These assessments have attempted to understand the susceptibility threshold of Commercial off the Shelf (COTS) computer equipment to High Power Electromagnetic (HPEM), High Intensity Radiated Field (HIRF) or High-altitude Electromagnetic Pulse (HEMP) environments. HPEM and HIRF environments were produced using the mode stirred reverberation chamber technique and the early-time HEMP environment was generated using the QinetiQ bounded wave HEMP simulator.

HPEM/HIRF susceptibility data is presented for the following test items:

- 486 66MHz
- 486 100MHz
- Pentium 3 667MHz
- Pentium 4 1.4GHz
- Pentium 3 667MHz computers with internal 10/100Mbps Ethernet cards
- Dual speed 10/100Mbps switching hub

HEMP susceptibility data is presented for four networked computer configurations of different specification/age including:

- 486 66MHz
- Pentium 1 200MHz
- Pentium 3 667MHz
- Pentium 4 2.6GHz

To simulate the real life installation the predominant network configuration for the time period was used. This meant that more recent networks used a 10/100Mbps hub and the older configuration used a token ring network. Many aspects of the systems were monitored for any upset or damage. Each computer communicated with the adjacent computer and the CPU was exercised throughout the testing. The keyboard and mouse were checked between tests to confirm correct operation. In the case of networked computer configurations, proprietary software was used to exercise the network traffic and CPU usage to enable the systems to be monitored for susceptibility.

These assessments have focused on the threshold of susceptibility of computer equipment and networks with variation in technology maturity. Technology trends have been established where possible and these will be presented and discussed during the presentation. The impact of EMC compliance on computer equipment immunity is also discussed. It is considered that the data presented in this paper will be informative to those seeking to protect systems and infrastructures from intentional and unintentional Electromagnetic Interference (EMI).