Safeguarding against the threat of IEMI

With electronics being such a part of everyday modern life, Intentional ElectroMagnetic Interference (IEMI) is becoming a threat of real concern for defence and security, in both the public and private sectors. Here William Turner, senior design engineer at **MPE** explores the need for protection

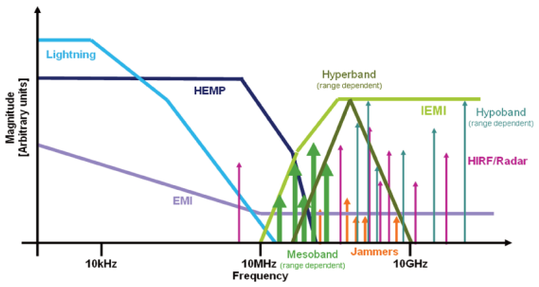

Figure 1:
Comparison of IEMI and other EM disturbances

Deliberate hacking of a machine or system can seriously disrupt its operation. High-value systems at risk include critical national and international infrastructure such as military bases, public utilities, rail networks, the smart grid, governmental bodies with remote datacentres, emergency services response centres and telephone exchanges, not to mention financial institutions such as banks and stock or commodity exchanges and all types of control rooms and datacentres in the private sector. In response to these threats, a number of initiatives are being undertaken to assess the needs of vulnerable areas, and new standards are continually being devised.

IEMI (Intentional ElectroMagnetic Interference) differs from most other EM (ElectroMagnetic) threats in that it typically occupies a narrow frequency band, depending on which specific malicious source is being used. This contrasts with other threats such as lightning and HEMP (High-altitude EMP), which are essentially broadband in nature.

The other notable difference is the area of the spectrum occupied: IEMI-radiated threats are almost never below 10MHz, as the coupling efficiency of such a threat would be much reduced. Instead the frequencies used tend to be much higher, to improve the effectiveness and penetration of any attack. The exception to this is for pulses directly injected into power and communications conductors, where lower frequencies are able to travel long distances with minimal attenuation.

The technically naïve approach is to assume that, because all equipment must be to the standard of the EMC Directive, it is adequately protected. However the various EMC Directive immunity tests are all significantly below the levels and frequency that could be experienced during an IEMI attack (V/m as compared with kV/m), and typically EMC Directive conducted compliance focuses on the lower bands – where SMPS and similar switching noise problems exist which do not arise at the higher bands where most IEMI threats exist.

TYPES OF IEMI ATTACK

The biggest problem with protecting against IEMI is that its sources can vary massively between different types of attack, as will the ways in which any attack may be launched. Conducted attacks may involve direct pulse or continuous wave injection onto the power and/or communication lines. These can have a huge impact on systems, with effects such as: triggering of safety protection devices or disruption of switched mode PSUs, causing power cuts as well as physical denial of services (DoS) by flooding xDSL or ISDN systems. The ultimate threats are high-power pulses that bring about physical damage to equipment.

Whilst the internal resilience of equipment is a key part of IEMI protection, it is known to vary even between equipment made by the same manufacturer. Therefore it is often not possible to influence that characteristic, especially where third-party equipment is concerned: hence one must look instead at how those assets can be protected.

As can be seen in Figure 1, there is little frequency overlap between traditional threats and IEMI. One should bear this in mind when planning the protection strategy for a system. However, it does not mean that existing protection systems or even infrastructure are completely useless, just that they should not be regarded as the whole solution.

Bearing this in mind, there are different strategies that can be adopted for protection. You cannot assume that all equipment to the standard of the EMC Directive has sufficient protection. That is because EMC Directive immunity tests are all significantly below the levels and frequency likely to be encountered during an IEMI attack, and typically EMC Directive conducted compliance focuses on lower bands rather than the higher ones where IEMI threats proliferate. Meanwhile ESD protection has limited relevance: since it only mandates no permanent damage, disruption is acceptable.

Figure 2:
Diehl briefcase mesoband UWB source

Figure 3:
MPE filters subjected to IEMI attack

To go to the other extreme and apply the traditional metal box/Faraday cage solution shown in Figure 3, as often seen in high-end military applications and EMC test chambers. This assumes no inherent resilience in any equipment and is the same strategy adopted for MIL-STD 188-125 HEMP (nuclear EMP) protection on critical military infrastructure, where even minor disruption is unacceptable. For IEMI protection applications where that same "work-through" requirement exists, then this really is the only guaranteed solution: one would simply need to ensure that the shield performed up to at least 18GHz, and the same for the filters on incoming power and communications lines.

TESTING POWERLINE FILTERS

MPE recently tested its filters against the Diehl pulser pictured in Figure 2. The LEDs were positioned both inside and outside the shielded cabinet. At this stage it was only a qualitative test, with the power source outside filtered using one of MPE's HEMP filters. The effects were very clear, with no LEDs being damaged inside the cabinet even at very short ranges from the Diehl source: however, most of the LEDs outside suffered failure at this and greater distances.

There are plans to do more detailed quantitative tests against this and other IEMI sources, including the often touted modified microwave oven. Nevertheless, knowing that the same filter construction has been proven in 40GHz filtering/shielding applications and the energy from IEMI is still below that of MIL-STD 188-125 (150kV 2500A conducted), the outcome is expected to again be positive and to show that standard MPE HEMP filters also protect against IEMI. The assessment is likely to take a similar approach to that of HEMP filter testing described in IEC 61000-4-24, where residual currents and voltages are measured on the protected side of the filter against a known incoming pulse.

MPE
www.mpe.co.uk
T: 0151 6329111