MANAGING EDITOR
Alistair Winning
alistair.winning@imlgroup.co.uk

ASSISTANT EDITOR
Alistair Hookway
alistair.hookway@imlgroup.co.uk

GROUP PUBLISHER
Andrew Quenault
andrew.quenault@imlgroup.co.uk

PRODUCTION
Sara Clover
sara.clover@imlgroup.co.uk

DIRECTOR
Neil Whitaker
neil.whitaker@imlgrioup.co.uk

DESIGN
Graham Rich Design
www.grahamrichdesign.co.uk

HEAD OFFICE
IML Group, Blair House,
184/186 High Street,
Tonbridge, Kent TN9 1BQ

Tel: 01732 359990
Fax: 01732 770049
E-mail: pbsi@imlgroup.co.uk

Printed by Buxton Press. Panel Building and Systems Integration is a controlled circulation journal published twelve times a year. Completed print or online registration forms will be considered for free supply of printed issues, website access and online services. Annual subscription for non-qualifying readers is UK £121, EU £146, Airmail £212. Single copy is £12.

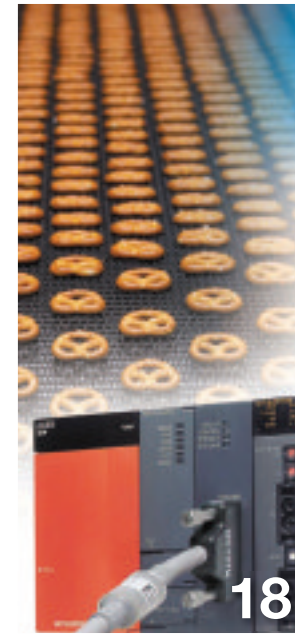
www.pbsionthenet.net

Circulation:
Tel: +44(0)1732 359990
Email: subscriptions@imlgroup.co.uk
ISSN 1750-1059

pbsi Panel Building & System Integration

Contents

General



Safeguarding your electronic systems against the clear & present threat of IEMI

With the increasing use of electronics to control so many aspects of modern life, Intentional ElectroMagnetic Interference (IEMI) is becoming a threat of real concern for defence and security, in both the public and private sectors.

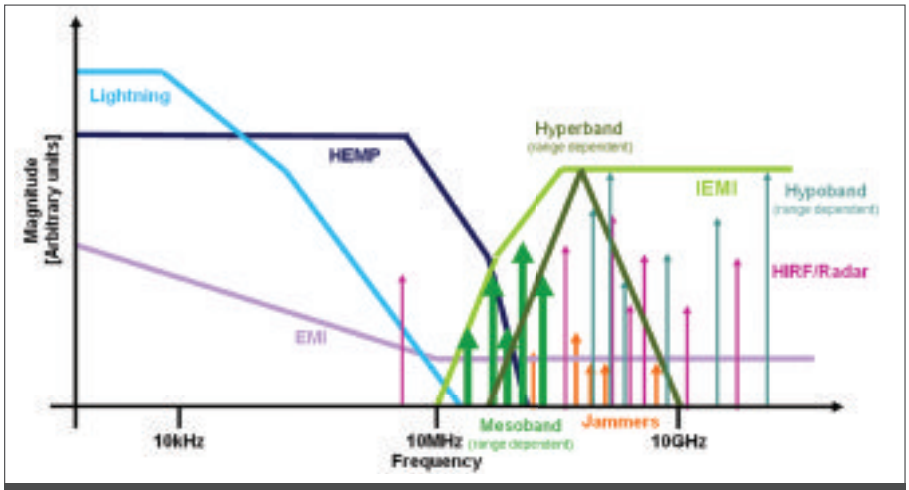


Figure 1 – Comparison of IEMI and other EM disturbances

Often misdiagnosed as hacking in cyber-space, such deliberate interference working on a physical level can disrupt the operation of any systems based upon electronics. High-value systems at risk include critical national and international infrastructure such as military bases, public utilities, the European rail network, smart grids, governmental bodies with remote data centres, emergency service 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 data centres in the private sector.

So, in response to the threat, a number of initiatives have been undertaken to assess the needs of vulnerable areas, and new Standards are being devised. Numerous papers have been written on the disruptive and damaging effects of IEMI attacks on electronic systems, and covering that in detail is beyond the scope of this piece. What can be said here is that the effects can vary from the very subtle errors in data streams and microprocessor instruction operation through to system lockups, hard resets and even permanent damage which render a system beyond repair.

The exact effect of a particular aggressor's action against a particular system is very case-specific and would require thorough analysis. However there is one general rule that applies: the greater the interference – either as a conducted or radiated disturbance – the more likely effects will be seen or the more severe they will be.

Frequencies used in IEMI attacks

To offer protection, one must first understand what is being protected against and how that compares and contrasts with other EM protection Standards. Figure 1 shows the frequency and comparable magnitudes of the various EM threats. Please note that EMI refers to the typical background EMI that can be experienced from benign intentions such as radio and TV broadcasting, radar, microwave, networking and GPS systems.

IEMI differs from most other EM 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.

With the increasing use of electronics to control so many aspects of modern life, Intentional ElectroMagnetic Interference (IEMI) is becoming a threat of real concern for defence and security, in both the public and private sectors.

Figure 2 – Microwave oven as an IEMI source

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 aggressor, as will the ways in which any attack may be launched. IEC 61000-4-36 is the Standard for IEMI immunity test methods for equipment and systems and should be considered essential reading for anyone attempting to protect against IEMI. This Standard defines categories of aggressors as Novice, Skilled and Specialist, based on their capability, and gives examples of the types of attack one could anticipate from those categories.

Generally, Novice attacks will be short-ranged or require some direct access and take the form of technologically very simplistic and low-cost methods such as modified microwave ovens, ESD guns or even EM jammers that can be bought online for a hundred Euros. Although unsophisticated, such attacks should not be underestimated and could easily cause persistent disruption or damage without leaving an evidence trail of an attack. An example of what can be constructed from rudimentary everyday components is shown in Figure 2.

The next category of skilled aggressors comprises those with good understanding and experience or who have access to commercially available equipment.That equipment could be something like the Diehl pulser.

This is an off-the-shelf "interference source" capable of emitting a 350MHz damped sine wave output and 120kV/m at 1m continuously for 30 minutes. With an appropriate antenna, it is capable of disruption or damage at a greater distance.

In the Novice and Skilled categories, one could also anticipate conducted attacks where access is possible, involving direct pulse or continuous wave injection onto the power and/or communication lines. These should not be underestimated and 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.

The third category of Specialist is in the realms of research laboratories and high-end military programs with accordingly high capabilities. This covers systems such as the Boeing CHAMP missile and the Russian-developed RANETS-E, which is capable of a 500MW output and range of 10km.

Although it would be obvious if a large truck with antenna were parked outside, or a missile had been launched overhead, a Specialist aggressor's equipment can be much more subtle than that, especially if fixed equipment can be set up nearby – in a building across the street or even an adjoining room. This allows complex equipment to be set up and an attack to go unnoticed for a long time, or perhaps not be noticed at all.

This raises the most critical question concerning protection from IEMI – access. Access is in terms of distance either from threat to target in radiated systems, or to incoming power and communications cables for injected conducted disturbances.

Strategies to protect your assets

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 by external measures.

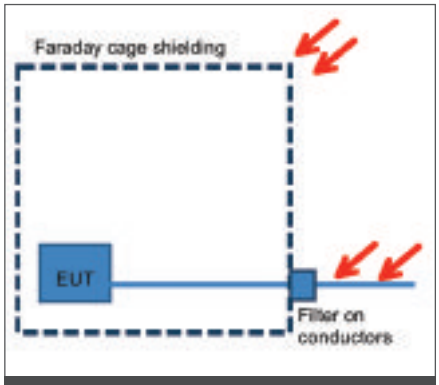


Figure 3 – Classical protection method

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

To offer protection, one must first understand what is being protected against and how that compares and contrasts with other EM protection Standards.

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.

What one does need to consider is the type of IEMI threat likely to be experienced. For example, it is unlikely that a small company in the UK will suffer an attack from a Boeing CHAMP missile directly overhead, but it is plausible it could be subject to interference from a malicious individual with some pulse generator plans from the internet. Feasibly, a company of national significance could be targeted by organised terrorists, with whatever equipment and skills their organisation possesses.

Bearing this in mind, there are different strategies one could adopt for protection.

As mentioned above, one 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.

The second approach is 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

A vital part of the filtering solution is the surge suppression performance against pulse-type IEMI attacks, which can have very high power content and fast rise times.

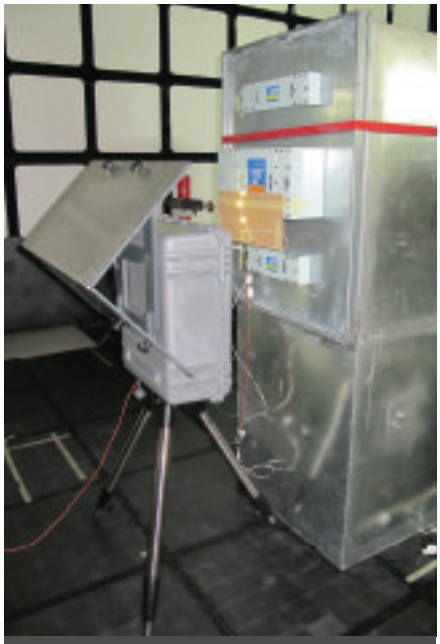


Figure 4 – MPE filters subjected to IEMI attack

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 for their IEMI shielding performance

As confirmation of this principle, MPE recently tested its filters against the Diehl pulser to try out the hypothesis. As shown in Figure 4, 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.

Weighing up the costs of shielding solutions

For lesser applications taking this approach, one would only need adequate shielding and filtering to the appropriate level for the anticipated threat. The reality is that such a shield wouldn't be worth providing unless it was giving at least an overall 60dB reduction. This approach could be scaled appropriately to what is desired to be protected: if only a server cabinet is deemed critical, then only that needs shielding and filtering. The downside of such protection is the cost – for a cabinet alone, it could run to over £1000.

Protecting a large, high-end military facility can cost in excess of £100,000 in filters and more than £1m in shielding and architectural work, even if done at the point of construction. Retrofit would add even further to the costs. Such a facility would also require significant maintenance, adding to the bill. This cost can be very off-putting for all but the most critical of applications.

Staged protection scheme

Another approach to the problem is to assess what protection is already there, the threats that are likely to be a problem, what really needs protecting, and to apply a staged protection scheme. This concept doesn't rely on a single component providing huge signal

attenuation, but on multiple smaller and often incidental components to give a similar attenuation at a much reduced cost. This is a tailored solution to suit individual scenarios and equipment.

It is here where the EMC Directive (and other regulatory EMC Standard) immunity tests become useful: they provide a good base-line for building upon with other protection methods. Caution should be exercised here, as there is a danger of "building on sand". The EU "CE" mark is a self-certification system, meaning that a CE mark is only as trustworthy as the company placing the mark upon the product.

One only has to look at the many analyses of USB phone chargers and LED lighting systems to know that many products do fall far short of the Standard (not just for EMC) when put to test. Assuming that the regulatory immunity can be trusted, then a typical attenuation of 60dB might be required from perhaps 10MHz to 1GHz. It becomes less clear above this frequency, as many items of equipment stop testing at 1GHz, and so the base equipment immunity is often unknown above this.

Protection against pulse-type IEMI attacks

A vital part of the filtering solution is the surge suppression performance against pulse-type IEMI attacks, which can have very high power content and fast rise times. Those rise times can be in the order of nanoseconds or even picoseconds, billionths or trillionths of a second.

Compare this to the most common type of surge suppression – lightning protectors, typically spark gap or MOV varistor types.

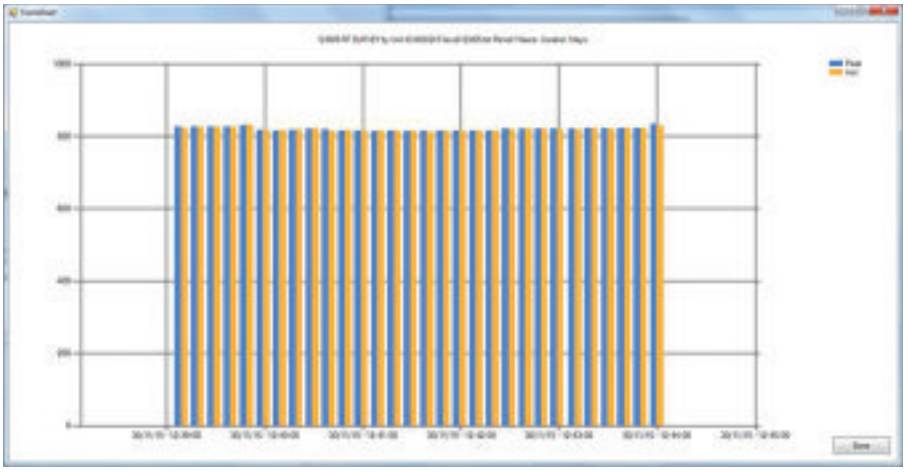


Figure 5 – Demonstration of available analysis

These typically only need to operate in the microsecond timescale for lightning: although some of the technologies can operate far faster than this, in practice they don't when used in lightning applications, due to many factors including installation and connectivity styles. This makes any lightning protection very ineffective against IEMI, except for the very slow conducted pulses, i.e. those already in the lightning area of the frequency spectrum.

This is where the crossover with HEMP is important: the MIL-STD 188-125 E1 pulse also has a fast rise time in the nanosecond scale and energy content far exceeding that of any likely IEMI attack. As the performance won't suddenly cease at the top of the HEMP spectrum, this means that a MIL-STD HEMP protection device will protect against all but the fastest conducted pulses seen with IEMI threats. Nevertheless MIL-STD HEMP devices, as previously discussed, are expensive and quite likely excessive in all but the most sensitive and critical cases where HEMP protection is also likely to be a concern.

Therefore in most cases what is desired is in effect a lower cost and performance HEMP filter, with performance stretching to at least 18GHz. Fortunately, the update of IEC 61000-4-24 is nearing publication. It will define a range of performance criteria for HEMP protection on civilian applications which are based on more relaxed residuals than the MIL-STD (it also includes the MIL-STD as the special case) but are still required to respond to the same nanosecond timescale pulse.

This provides a good basis for specification of IEMI surge suppressors and conductor filtering, as it requires demonstration of all the key attributes – fast pulse response, prevention of shielding bypass and ability to handle the power levels expected during such an attack.

In summary

Evidence shows that the IEMI threat is real, regardless of application – whether in security or defence, public or private sector – and that existing protection systems cannot be assumed to be adequate and in most cases will be found wanting by a well-planned attack.

The steps required to effectively and adequately protect against the risk of IEMI are clear – understanding the nature of the threat, taking advantage of existing protection systems and supplementing them with IEMI-specific measures where necessary.

William Turner, MPE

Evidence shows that the IEMI threat is real, regardless of application – whether in security or defence, public or private sector – and that existing protection systems cannot be assumed to be adequate and in most cases will be found wanting by a well-planned attack.