MPE
Quality, Reliability, Performance

Company Bulletin
for EMC, EMP & TEMPEST Protection
Issue 7

The IEMI Threat and a Practical Response

William Turner
Senior Design Engineer
MPE Ltd

IEMI Threat

With the increasing use of electronics to control every aspect of modern life, from smart grids to driverless cars, Intentional ElectroMagnetic Interference (IEMI) is a threat gaining concern. Various initiatives have been set up to address the needs of specific market areas, and new standards are being worked on.

However it is worth understanding what is being protected against and how that compares and contrasts with other EM protection standards. Figure 1 below 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 and networking systems, GPS, etc.

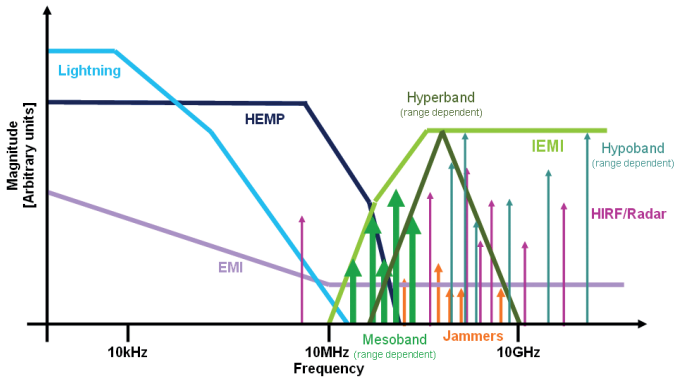

Figure 1 - Comparison of IEMI and other EM disturbances
(image by courtesy of QinetiQ)

It can be seen that IEMI differs from most other EM threats in that it typically occupies a narrow frequency band, dependent upon which specific malicious source is being used. This contrasts with other threats such as lightning and HEMP (high-altitude EMP) which are very broadband in nature.

The other notable difference is the area of the spectrum occupied – IEMI 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

MPE
Quality, Reliability, Performance

Company Bulletin
for EMC, EMP & TEMPEST Protection
Issue 7

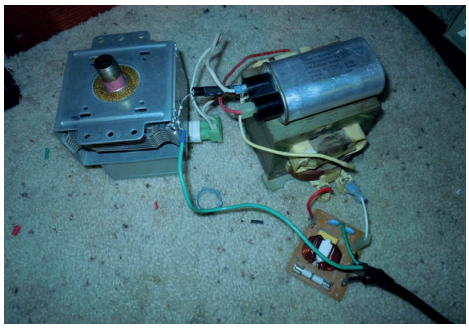

Figure 2 - Microwave oven as an IEMI source
(image by courtesy of QinetiQ)

Figure 3 - Diehl briefcase mesoband UWB source

conductors, where lower frequencies are able to travel long distances with minimal attenuation.

Methods of Threat Delivery

The biggest problem with protecting against IEMI is that the sources can vary massively between different aggressors and the way any attack is 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. IEC 61000-4-36 defines categories of aggressors as Novice, Skilled and Specialist. These definitions are based on their capability, and IEC 61000-4-36 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 pictured in Figure 3.

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, this would be capable of disruption or damage at a greater distance.

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. Plentiful information on both systems is available in the public domain. Although it would be obvious if a large truck with antenna was 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 either distance from threat to target in radiated systems, or to incoming power and comms cables for injected conducted disturbances.

Effects on Operations

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 paper. Readers are encouraged to review the many papers and presentations on the subject.

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 rendering the 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, and it may appear obvious: the greater the interference, either as a conducted or radiated disturbance, the more likely effects will be seen and the more severe they will be.

It has been shown many times that a radiated or conducted disturbance will cause damage at higher power levels, but at lower power levels can cause only minor upsets or even no significant effect at all. This makes disturbance attenuation key to protection.

Asset Protection

While 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. So often it is not possible to influence that characteristic, especially where third-party equipment is concerned, so one must look instead at how those assets can be protected by external measures.

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 shouldn't be considered 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's plausible it could be subject to interference from a malicious individual with some pulse generator plans from the internet. It's plausible that a company of national significance could be subject to organised terrorists, with whatever equipment and skills their organisation possesses.

Bearing this in mind, there are a few different strategies one could adopt for protection. The obvious and technically naïve strategy 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 that could be experienced during an IEMI attack (V/m against kV/m), and typically EMC directive conducted compliance focuses on the lower bands – when SMPS and similar switching

MPE
Quality, Reliability, Performance

Company Bulletin
for EMC, EMP & TEMPEST Protection
Issue 7

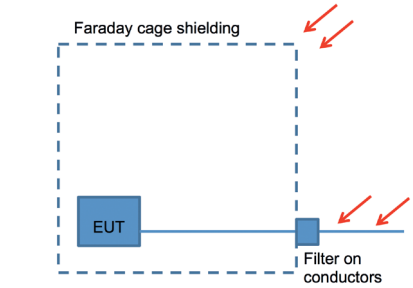

Figure 4 - Classical protection method

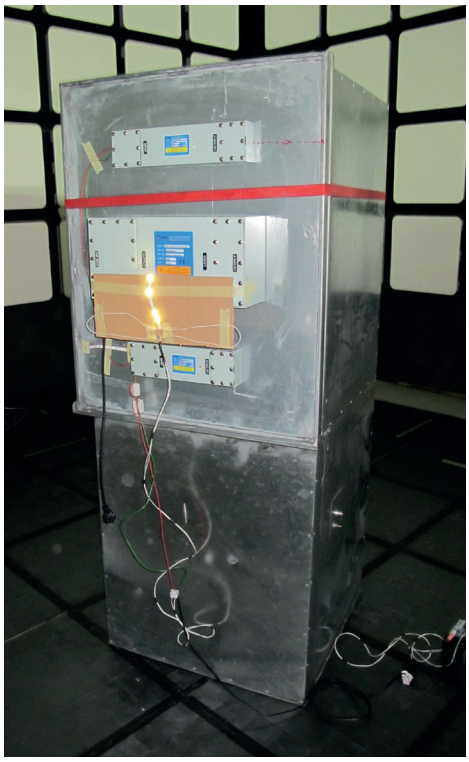

Figure 5 - MPE filters subjected to IEMI attack

noise problems do not arise at the higher bands where an IEMI threat exists. ESD protection only has limited relevance: as 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 approach shown in Figure 4, 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 a minor disruption isn't tolerable. 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 comms.

As confirmation of this principle, MPE recently tested their filters against the Diehl pulser pictured in Figure 3 to test this hypothesis. At this stage it was only a qualitative test with LEDs positioned both inside and outside a shielded cabinet, with the power source outside and 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. However, 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 MPE standard HEMP filters also protect against IEMI. The assessment is likely to take a similar approach to that of HEMP 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.

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 – a cabinet alone 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 offputting for all but the most critical of applications.

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

MPE
Quality, Reliability, Performance

Company Bulletin
for EMC, EMP & TEMPEST Protection
Issue 7

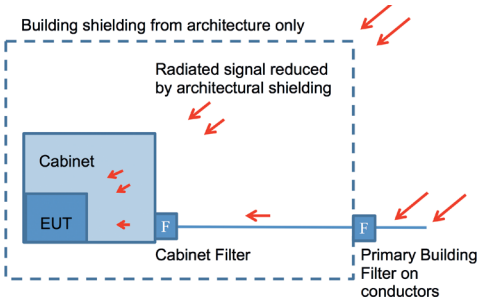

Figure 6 - Staged protection

components to give a similar attenuation at a much reduced cost. The concept is shown in Figure 6. This is a tailored solution to suit individual scenarios and equipment. Some buildings can provide 10dB of shielding simply due to the materials used and their construction style. The distance an aggressor could get to any target could be quite long. Perhaps the site has an extensive perimeter with security, or only a specific room needs to be protected in a large building, and this gives a natural attenuation to any radiated or conducted attack originating off-site.

Equipment cabinets and cases should also be taken advantage of. A typical commercial EMC cabinet compared to a unshielded rack could provide 30dB of attenuation up to1GHz and could still be providing some up to perhaps 5GHz.

The conducted protection should try to coincide with the shielding to avoid bypass coupling and make the most of the inherent shielding protection. If the building has very good shielding, then a large incoming filter at the entry point would be best: but if it is very poor and the cabinet or individual equipment is carrying the majority of the shielding, then this is where the filtering should be located.

Distributed filtration can be used with several lower performance filters in place of a single high attenuation filter. Some of those filters could be part of the original equipment, but bear in mind that, although most equipment has incoming power filters, these are often only low frequency for EMC compliance and not really suitable for IEMI protection. Also the combination of filters in the system should cover the entire frequency spectrum of concern. This requires assessment against the probable threats and tolerable disruption: there is a standardised way to define these in the appendices of IEC 61000-4-36.

A vital part of the filtering solution is the surge suppression performance against pulse-type IEMI attacks, which can have very high energy 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 high energy surge suppression of lightning protectors, typically spark gap or varistor types. These only operate in the microsecond timescale: although some of the technologies can in theory operate far faster than this, in practice they don't when used in lightning applications. It makes any lightning protection very ineffective against IEMI.

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 IEC 61000-4-24 is nearing publication, which defines a range of performance criteria for HEMP protection on civilian applications based on more relaxed residuals than the Mil-Std (it also includes the Mil-Std as the special case).

Threat Detection

If the system in question can tolerate interruptions or damage without serious unrecoverable consequences, and the business case is not currently good enough to invest in protection, there is an intermediate step before protection that is complementary to it even when installed.

This takes the form of detection of any incidents and profiling it in the specific scenario, with an aim to gather evidence for the purposes of the cost/benefit analysis of protection systems and for logging IEMI attacks or disruptions to positively identify threats against system faults. This has the added benefit of logging unintentional EMI effects in the increasingly crowded spectrum.

This approach has only become viable recently thanks to a shift in the philosophy of detection systems. Traditional IEMI monitoring equipment is very large, expensive and complex, requiring highly skilled staff to operate. These can give a full profile of any attack or threat detected, with analysis of the specific source in real time, etc. However the cost and maintenance of such a detection system can approach or exceed that of system protection, making detection an irrelevant and costly intermediate step for general use.

To make logical sense, what is required is a detection system of lower cost and complexity. Fortunately MPE and our technical partner have been developing a solution, and we are now at the pre-production prototype stage. This differs from the traditional detection approach by simply detecting anything that causes a large enough EM disturbance and logging it in the time domain.

Figure 7 - Demonstration of available analysis

MPE
Quality, Reliability, Performance

Company Bulletin
for EMC, EMP & TEMPEST Protection
Issue 7

By logging the disturbance in enough detail in the time domain, offline analysis can then be performed, removing the need for complex analysis, and thus cost, within the detector. By keeping the costs low, multiple detectors could be installed, giving a far more detailed view of the threat. Information that this could give to the analyser includes increased accuracy on wave shape and triangulation of the threat source, and attenuation provided by existing buildings, infrastructure or shielding.

This solution gives the two desired outcomes from detection: an evidence trail for any cost/benefit assessments for stakeholders to invest in protection, and the time-stamping of disturbances to be correlated with any CCTV or other evidence in legal proceedings.

Summary

It has been shown that the IEMI threat is real regardless of industry 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 only where necessary.