# A Resilience based Approach to HPEM Threat Mitigation

Richard Hoad[1] Ph.D, Barney Petit[1],

[1] QinetiQ Ltd.
Cody Technology Park
Farnborough, Hants, UK
rhoad@qinetiq.com

***Abstract***— This paper introduces the concept of a Resilience based approach rather than a protection-lead approach to High Power Electromagnetic (HPEM) threat mitigation. It is shown that a resilience based approach is much more intuitive and is how the risk from the majority of common threats are mitigated. The resilience approach and a framework for the management of HPEM resilience is being developed for an update to IEC 61000-5-6.

## I. THE PROTECTION-LEAD APPROACH

The earliest standards for High-altitude Electromagnetic Pulse (HEMP) protection of facilities were developed for military use [1]. This is at least partially because the HEMP threat was first acknowledged by the military sector who required a zero-disruption or 'work-through' solution for the HEMP threat. Military HEMP protection standards generally require a high degree of protection, mainly due to the requirement to work-through HEMP events, and also due to the inclusion of significant protection margin so that degradation in the protection performance does not impact the ability of the facility to work-through.

However, military electronic equipment tends to operate in a well bounded-networked manner and is resilient by design. Military facilities that are HEMP protected tend to be continuously staffed with trained professionals who may have dedicated responsibilities for maintenance of the HEMP protection. The protection-lead approach is known to be very effective as long as the 'as-built' protection performance is maintained and continuously assured.

## II. A RESILIENCE APPROACH

A protection-lead, work-through, approach described above can be cost intensive, inefficient and very difficult to apply for modern applications and facilities for a variety of reasons which will be discussed in the presentation.

A definition of resilience, used here, is: *'The ability of a system to anticipate, withstand, respond to and recover from a transient electromagnetic disturbance(s) in a timely and efficient manner'*. Note that this definition of resilience includes the requirement for protection (withstand) but other attributes are added. A key change here is a shift in emphasis implied in the protection-lead approach from 'shall continue to work-through', to a 'shall be capable of timely recovery' emphasis in the resilience based approach. For the resilience based approach there is an implied acceptance that the mission or function of a system or facility may be affected or disrupted and therefore that prompt restoration and recovery are likely to be required.

A simple model that describes the necessary attributes that can be used to develop a framework based approach for a resilience based approach is shown in Figure 1. This model is derived from existing, authoritative and peer reviewed principles and practices developed for cyber threats described in the National Institute of Standards and Technology (NIST) Cyber Security Framework [2].


Figure 1 Resilience model

The resilience based approach is intuitive and is used for many other types of common threats. Consider for example the risk of a fire to populated building.

The emphasis in this scheme is in reducing the consequential impact, restoring function and returning to normal operations as quickly as possible. People are not required to work-through the fire.

## III. SUMMARY

The resilience based approach is consistent with the practices employed by many modern critical facilities who, for business continuity reasons, often have a clear response and recovery strategy.

The resilience approach and a framework for the management of resilience to HPEM threats is being developed for an update to IEC 61000-5-6 [3] and will be discussed in the presentation.

## REFERENCES

[1] R. Hoad and W. Radasky, 'Progress in High Altitude Electromagnetic Pulse (HEMP) Standardization', IEEE Transactions On Electromagnetic Compatibility, Special Issue on HEMP, Vol. 55, No. 3, June 2013

[2] NIST, "Cyber Security Framework," [Online]. Available: https://doi.org/10.6028/NIST.CSWP.04162018 . [Accessed 2022]

[3] IEC 61000-5-6 Ed. 2.0: Electromagnetic compatibility (EMC) – Part 5-6: Installation and mitigation guidelines – Mitigation of external EM influences (in development)