An Overview of Some Site Specific IEMI Risk Assessment Tools

B. Petit, R. Hoad, A. Fernandes and G. Eastwood
DEW & E3 Capability Group,
QinetiQ Ltd.
Farnborough, Hampshire, UK
bjpetit@qinetiq.com

***Abstract*—.With the reduction in cost and wider availability of Intentional Electromagnetic Interference (IEMI) systems, a greater risk is posed to Critical National Infrastructure (CNI). QinetiQ are working with CNI providers to understand the risk posed to their sites and how to mitigate this risk. This is being done through Technical Visual Assessments of sites to determine the inherent protection and to offer advice on hardening where relevant. QinetiQ have developed a number of tools to aid this work. This paper describes these tools and how they are being applied to help to understand the risk from IEMI to CNI.**

Keywords- IEMI, Electromagnetic Compatibility, Critical National Infrastructure

I. INTRODUCTION

With the reduction in cost and wider availability of Intentional Electromagnetic Interference (IEMI) systems including jammers, the risk to Critical National Infrastructure (CNI) has increased. These IEMI systems are becoming more prevalent and pose a risk to the electronic control systems used within CNI, as well as the vital signals that CNI sites need to operate, for example the timing signals received from Global Positioning Systems (GPS) via satellite. If the operation of CNI sites is compromised, the consequences could be drastic and far-reaching. This makes it very important to understand the risk posed by IEMI systems to the sites, as well as how to mitigate and protect against potential effects.

QinetiQ have been working with CNI providers within the UK to assess the sites used to control and operate CNI. Through this work QinetiQ have been able to offer advice on vulnerabilities and how to mitigate the risks.

II. RISK ASSESSMENT TOOLS

In order to easily illustrate to CNI owners and operators where the risk from IEMI impinges on the facilities, QinetiQ have developed a risk visualisation tool known as PhoS. The tool accepts a plan view of the site. Details gathered from a Technical Visual Assessment (TVA) of the site such as the specific locations of critical electronic systems (usually control rooms, or other central processing facilities) together with an assessment of the protection (attenuation) of the physical boundaries are entered into the tool and indicated on the plan.

QinetiQ have developed and are continuing to evolve an attenuation database of building façade materials and other physical perimeter materials and have recently been adding to the database with measurement data. QinetiQ have built databases of both the IEMI threat environments and effects criteria.

The risks are assessed by comparing the IEMI 'threat environment', which covers a wide parameter space including frequency range and time domain parameters, with the estimated level required to exceed immunity and drive an effect at critical electronic systems.

QinetiQ have focused on the IEMI threat from readily available IEMI source technologies classifying threat actors by technical capability into novice, skilled and specialist groups. QinetiQ have considered both 'front door' effectors (jammers) and 'back door' effectors in different delivery formats, man-portable, vehicle borne and fixed installation, as well as the possibility of a malicious insider.

The risk boundaries indicated by the tool are based on immunity, upset (50% probability) and damage (50% probability). An example visualisation from the PhoS tool is shown in Figure 1.

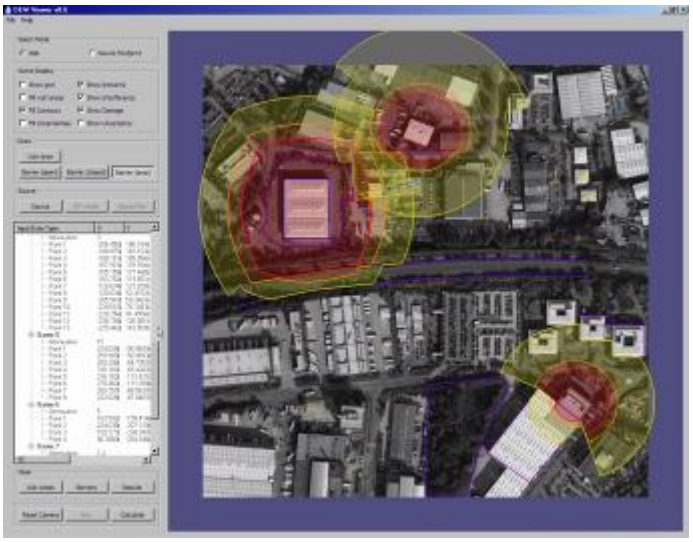

Figure 1 – Example Visualisation from the PhoS Tool

The visualisations produced by the tool have been found to help to easily guide the CNI owner/operator to the magnitude of the risk to a particular facility from IEMI and further indicate where best to include pragmatic protection.