Preserving Information Security at Data Centres

Electrical and electronic equipment can give off unintended electromagnetic emanations which can be reconstructed as intelligible data

By: Paul Currie, Director, MPE Ltd

Countermeasures are designed to preventing eavesdropping on data radiated as signals via conducting lines such as power, telephone or control line cables.

In defence parlance, the countermeasures applied to prevent intelligence interception are known as hardening, and TEMPEST hardening represents one aspect of total facility protection from electromagnetic threats.

Figure 1: Modern Data Centre

In the 21st century TEMPEST countermeasures are now becoming as important for information security in the civilian world as in the military arena. Examples of sites at risk would be Western embassies in hostile parts of the world, and data centres handling sensitive personal and financial information, where power line cables are vulnerable to electronic eavesdropping.

In particular, electronically secure data centres are nowadays commonplace, processing and storing vast amounts of information for Government offices, local authorities, the armed forces and police, public utilities, banks, healthcare providers, insurance companies and online retailers. There would be serious repercussions on many levels if any such organisations should allow entrusted information to be compromised.

Red & Black Zones

Confidential data – or devices containing or processing such data – are usually referred to as "red". This implies merely that you don't want the data to escape. Conversely, non-confidential data and equipment are termed "black". Sensitive or classified data that has been suitably encrypted is also regarded as black. A device processing red data, yet incorporating adequate protection to contain emissions, can be black too. Meanwhile a cable carrying black data that passes close to red equipment, and thus has the potential to pick up red data, can