be considered red.

The main types of TEMPEST leakage path are as follows:

1. Unintentional radiation from red equipment, strong enough to be picked up directly.

2. Coupling onto black equipment or cables. Red emissions can be picked up by black wires or equipment and propagated. The unwanted red data is described as parasitic. As black equipment and cables do not need to be protected, the parasitic red data can escape.

Figure 2: 5A to 100A TEMPEST powerline filters for data centres

3. By coupling onto an intentional emitter. A secure data storage device may be located close to an insecure radio transmitter. Secure data coupled on to the radio may be amplified and transmitted for all to hear.

4. By conduction. As your computer generates its ones and zeros, it will create tiny surges and glitches in the mains current supplying it. Given sensitive enough equipment, these could be interpreted by reading the mains cable from several miles away.

One solution is to create around the at-risk IT facility a hardened, "red" secured area or full Faraday cage lined with steel, aluminium or copper, backed up by the suppression of any conducted EMI which may contain intelligible information by filtering.

Where a cable has to pass through a red/black boundary, a filter can be inserted as an intended countermeasure to filter out all frequencies except the desired signal. It is normally a low-pass filter that blocks everything above a given frequency, on the basis that any parasitic red signal is likely to be of high frequency. This solution has obvious limitations, since any parasitic signals within the passband will still get through, and a low-pass filter cannot be used if the desired signal is itself of high frequency. A proper TEMPEST-grade filter must also prevent bypass coupling, where a radiated red signal bypasses the filter and couples onto the black side.

Because the propagation of unintentionally radiated emanations is relatively inefficient over distance, most red zones are situated in the normal building fabric, where potential eavesdroppers are denied opportunity by physical security measures.

The coupling of electromagnetic emanations onto cables and wires travelling into the black zone represents a more critical threat. This coupling and subsequent transmission down line can be very efficient, and information-bearing signals can be carried far beyond the building boundary, where they may be intercepted, analysed and reconstructed.

Electrical Filters at the Red / Black Boundary

The electrical infrastructure of any data centre will include power cables, telephone and data lines, and building management services wires. All of these can represent very efficient receptors of those emanations and signals circulating within the red zone. When these signals are carried far from the building boundary and beyond the