What is TEMPEST?

Bruce Gabrielson, PhD

What is TEMPEST

If you ask most people what TEMPEST means, they will probably quote the standard definition:

> *TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations, conducted or radiated, on complete equipment.*

While TEMPEST is certainty this, it is in reality the study of emissions in a much broader category, the study and detailed examination of communications theory. TEMPEST emissions are basically the result of inadvertent telemetry systems formed naturally by electronic devices and propagated via natural physical elements (antennas or wires) to the outside world. The efficiency of this inadvertent TEMPEST telemetry system to transmit signals through natural means is in reality the weakness of the equipment to protect its secure information.

Where Theory and Test Investigations Meet

since the communications channel in a TEMPEST system is not intended to convey information, the signals (compromising emanations) are not optimized for best reception. Therefore, a TEMPEST engineer must be familiar with other engineering disciplines such as information theory, complex modulation theory, and transmission line theory if he is to fully understand the scope and depth of the emanation problem.

Being able to unscramble a complex signal is simply a matter of understanding the probabilities of what each signal might represent for a particular type of data stream. In other words, a signal developed from an ASCII data source looks different than one originating from a CCITT data source. Also, signals transmitted in return to zero format look different then those sent non return to zero.

Modulation also is a problem. Signals can modulate on a carrier or appear as a baseband source. Amplitude modulated signals are the easiest to identify, and also the simplest to demodulate. Even with a trained eye however, since background noise sources are usually high, and since Gaussian noise distributions can sometimes look like signals, simply assuming that a detected signal is a compromising emanation can lead to massive overkill in a redesign effort. Also, since in TEMPEST systems, signals often modulate a harmonic of a noise source, these emanations can appear at nearly any frequency in the spectrum. The bottom line is that in the majority of cases, an engineering approach that disregards communication theory, and simply addresses redesign through trial and error test techniques, is both expensive and difficult to achieve in a reasonable time period.

Where Theory and Design Meet

Far too many modern TEMPEST engineers use "run and gun" type redesign approaches to fix emanation problems they find. This is the typical "add a capacitor on the line and see what happens" syndrome. The approach usually results in long redesign efforts, and often simply shifts the problem to another frequency or location, which is then found at a later date resulting in additional problems. What they don't understand is that signals radiate because transmission line theory tells us that if the signal channel's source and load impedance don't match, which they never do at all harmonics of a signal, then standing waves are created and some energy escapes to the outside world. Re-tuning the transmission line simply changes its characteristic impedance, and the signal will still be present, just at some other frequency.

As most TEMPEST design engineers will agree, fixing a problem before it appears is by far the most desirable approach. However, TEMPEST redesigns normally are intended to fix someone else's problems "after the fact". Here is where design and theory really merge. If the TEMPEST engineer understands the theory, plus if he is familiar with the limitations and capabilities of rf design techniques, he can usually provide a problem solution consistent with overall program needs. He can first find the problem, then generate a fix specific to the problem that won't simply move it to some other location, and finally, insure the problem stays fixed by maintaining constant quality control over the fix implemented.

A New Definition

Probably the best approach to explaining what TEMPEST is all about is to re-define the term as follows:

> *TEMPEST is the application of reverse communication theory to the design and test of complete equipment or systems which process and/or transmits secure information.*

While this definition isn't formatted in the normal jargon of the defense industry, it does cover the critical concerns that face the TEMPEST engineer during his daily activities.