# INDUSTRIAL TEMPEST PROGRAM

All electronic equipment emits extraneous electromagnetic energy. When this energy causes operational problems in other equipment, a condition of electromagnetic interference (EMI) is said to exist. In the case of equipment that processes information, it is possible to extract extraneous energy related to the data being processed. If that data is classified, a security compromise is a distinct possibility. This problem is referred to by the unclassified short name (not an acronym) "TEMPEST". Although many of the basic engineering techniques used to prevent a TEMPEST problem are similar to those used to avoid EMI, the evaluation techniques and criteria for acceptability are substantially different. A piece of equipment can be electromagnetically compatible with surrounding systems (and, in fact, fully compliant with MIL-STD-461A, the military standard for electromagnetic interference), and still be a TEMPEST hazard. The converse is also true. That is, equipment can fully comply with TEMPEST requirements while, at the same time, emit high levels of non-information-bearing electromagnetic energy. The engineer who deals with both EMI and TEMPEST must be able to wear two very different hats.

Whenever a government contract requires equipment to comply with a TEMPEST specification, there is a reasonable chance that it will be processing classified information. To provide an unauthorized interested observer with information regarding the TEMPEST characteristics of that equipment, and how such characteristics are evaluated, would be tantamount to leaving the combination to your security file written on your office blackboard. Therefore, there has been, and will continue to be, a very real requirement to safeguard technical information regarding TEMPEST test procedures, analysis techniques, acceptability criteria, suppression methods, and especially the emission characteristics of any equipment which the government might use to process classified information.

Because of the classification of the information, the government TEMPEST community has not divulged much more than the simple definition of "TEMPEST" except under strict conditions of need-to-know. This lack of technical communication existing between industry and the government resulted in a situation which had two basic problems: First, contractors were not knowledgeable about TEMPEST, its implications, or its solutions. Therefore, any RFQ for equipment which included TEMPEST requirements could expect a cost response with a large built-in contingency factor to cover the unknown TEMPEST quantity. Second, for TEMPEST engineering to keep pace with the state-of-the-art in the important areas of signal detection and analysis, detection system development, and communication system design, the experts in these fields needed to be aware of the TEMPEST problem. Much of the expertise resided, of course, in industry, the very community which was being "kept in the dark".

To help alleviate these problems, The National Security Agency, acting for the government, instituted the *"Industrial TEMPEST Program."* This has done much to improve the situation by providing a vehicle by which technical TEMPEST information can flow between contractors and government, and between contractors themselves. This is not to say that NSA has relaxed its controls over such information. If anything, they are more closely defined. For example, articles dealing with TEMPEST, such as this one, must be submitted to the National Security Agency for classification review prior to publication. However, within the context of those controls, new channels of communication are now available for those companies who become voluntary participants in the Industrial TEMPEST Program.

The Industrial TEMPEST Program is not intended to provide an alternate means of obtaining classified information when a means already exists. For example, if classified TEMPEST documents are required in conjunction with the contract or RFQ, the contractor must obtain them from the contracting officer. The Industrial TEMPEST Program is intended to provide a means of obtaining classified TEMPEST information when no contractual requirement exists.

The principal objective of the Industrial TEMPEST Program is to encourage the voluntary development, by industry, of information-processing equipment which complies with the TEMPEST specifications. In the past, the greatest single stumbling block to many companies who needed to learn about TEMPEST, or who had something to contribute to the TEMPEST state-of-the-art, was the fact that without an on-going government contract whose DD-254 (the DoD Contract Security Classification Specification) specifically provided for the possession of TEMPEST documents, such a company was definitely "on the outside looking in," from the standpoint of the TEMPEST community. Now, however, if a company can satisfy various requirements for facility security clearance and classified document storage capability, and can establish to a reasonable degree that it is in the government's interest that the company participate in the Industrial TEMPEST Program, the National Security Agency will assume the responsibilities that the Industrial Security Manual assigns to a contracting officer, and will issue a DD-254 security form. This means that such a company, even though it has no active contracts involving TEMPEST, can receive necessary classified TEMPEST documents. This is of significant benefit to contractors in that it permits them to establish TEMPEST capabilities, both in manpower and capital equipment.

Another significant benefit to participants in the Industrial TEMPEST Program is that it provides for crossfertilization between participants. For example, if Company A manufactures a printer which meets TEMPEST requirements, and if Company B has a need for such a printer, Company B may obtain a copy of the classified TEMPEST Test Report for the printer, *provided* that both companies are participants in the Program, and that Company A provides written permission for Company B to obtain a copy of its Report. Such information exchange within industry will do much to ensure that the government is offered the best available TEMPEST equipment and systems.

Finally, to become a voluntary participant in the Industrial TEMPEST Program, interested companies need only express their interest by writing to

Director, National Security Agency
Fort George G. Meade, Maryland 20755
Attention: S643

NSA will then provide additional information about the Industrial TEMPEST Program.

---

*The above article was written by Daniel J. Norton, Manager, TEMPEST Engineering Section, Sanders Associates, Nashua, N.H.*

# RFI/TEMPEST ISOLATION

The need for an isolation device arises from the requirement to remove from a communications signal all other signals, both transverse (across pair) and longitudinal (between the pair and ground) (common-mode), which should not pass between the signal source and its load or pass beyond a specified point in the signal route. This general requirement would be typical of radio frequency interference (RFI) and TEMPEST problems.

Since the unwanted signals and noise may fall within the band-pass of the desired signal, it is not desirable to employ passive filters. The patented technique employed by Versitron, Inc. consists of interposing an isolation device in the signal line to propagate the signal by optical means, thus breaking the electrical conductor path. Almost complete isolation against longitudinal (common-mode) unwanted signal coupling is obtained.

Each isolation unit is housed in two separate modules marked "Input" and "Output". A non-metallic light guide is then placed between the two modules, thus propagating signals without a metallic path. Circuit techniques are employed for digital units in order to suppress transverse noise levels. In addition, time regeneration is available on digital units, while the bandwidth can be restricted as required in analog units. Therefore, with proper installation and choice of model, the isolation device becomes a unidirectional signal repeater covering practically all communications frequencies and isolation requirements.

Common-Mode Isolation:

Common-mode signal isolation, for the purposes of the isolation devices discussed here, is defined as the signal attenuation between the shorted input and the shorted output of an isolation device when the generating source is between the shorted input and a ground reference, and the detecting instrument is between the shorted output and the same ground reference. (See figure 1).

Isolation devices accomplish this common-mode isolation by the use of seperate input and output module chassis. The input module converts the input electrical signal to a modulated light beam and the output module converts the light signal to an output electrical signal. Therefore, no electrical conductor exists by which to conduct the undesired common-mode signal. To complete the isolator installation, a grounded shield most be interposed between the input and output modules in order to eliminate space radiated coupling. This ground plane is normally a chassis wall or shielded room wall. The light beam is passed through the ground plane by means of a waveguide penetration. The dimensions of the waveguide are chosen so that its cut-off frequency is above the highest frequency of interest. This waveguide penetration must be chosen with two factors in mind. First, the wavelength of the highest frequency of interest must be large compared to the diameter of the waveguide. Second, the ratio of the length of the waveguide to the diameter determines the amount of attenuation below the cut-off frequency.

A formula containing these factors but excluding the low frequency "H" wave would take the following form:

$$A = 32 \frac{L}{d} \left[1 - \frac{f^2}{f_c^2}\right]^{1/2}$$

Where:
- A — Attenuation (dB) of waveguide
- L — Length of waveguide in meters
- d — Diameter of waveguide in meters
- $f_c$ — $\frac{3 \times 10^8 \text{ (cut-off frequency)}}{2d}$
- f — Any frequency below $f_c$ for which A is computed

The above formula assumes worst-case criteria such as: Diameter = ½ cut-off wavelength: dielectric constant = 1.

For frequencies significantly below cut-off, A = 32 L/D.

In view of the above and the fact that the light guide is a non-conductor, it is obvious that the common-mode isolation is independent of the electronic circuitry of the isolator. This, assumes, of course, that the power sources for the isolator modules are properly isolated or filtered. Photon couplers that do not use the above technique do not provide the highest degree of EMI or TEMPEST protection. They provide only DC and low-frequency isolation.

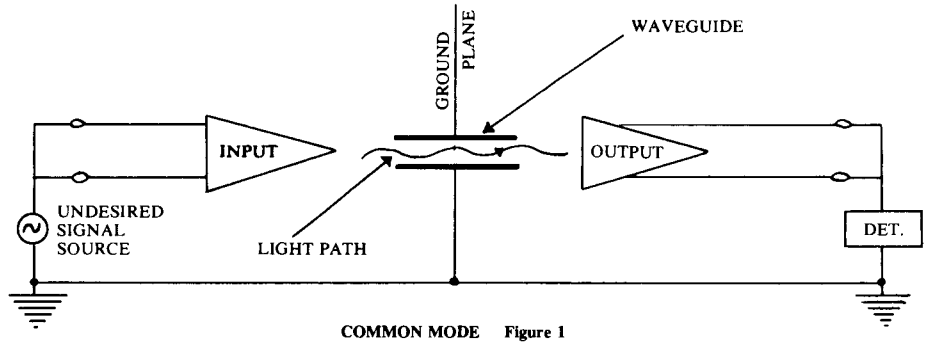
Transverse-Mode Isolation:

Since the common-mode rejection (balance) of practical circuits and wiring are never perfect and since cross-talk is a danger in multicircuit situations, it is often necessary to provide suppression of unwanted signals and noise in the transverse-mode. This mode is defined as the signal across the input or output terminals of the isolator, minus the desired signal. In the case of digital isolators, the input module light source circuitry is electrically saturated in the ON or OFF state and therefore, does not respond to superimposed undesired signals as long as the total instantaneous value does not exceed the threshold point for the opposite transition. (See figure 2).

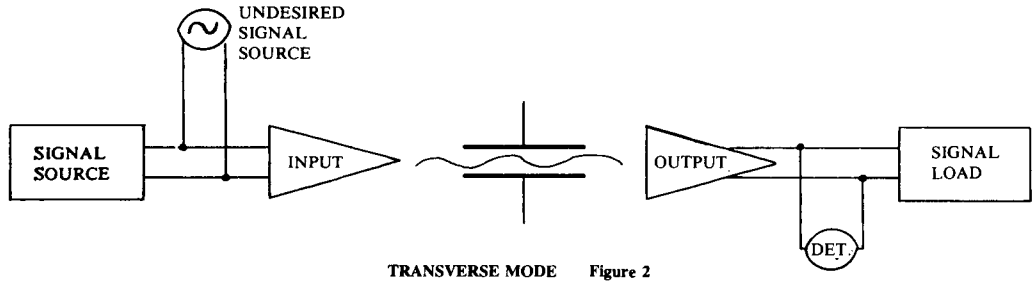
Where the undesired signal takes the form of phase or frequency modulation, time regeneration of the desired signal is used.

---

*This article was written by David C. Sherrick, Vice President, Versitron, Inc., Washington, D.C.*




**COMMON MODE Figure 1**




**TRANSVERSE MODE Figure 2**