What is TEMPEST
Chapter 1

Introduction

This text presents an overall introduction to classical information theory, basic communications theory, as well as TEMPEST design. Related issues in modulation, telecommunications, telemetry, shielding, and propagation are covered as they apply to TEMPEST control. The theoretical relationships presented form the basis of all TEMPEST testing and test requirements, as well as describing the means of escape for controlled signals from within the TEMPEST protected container.

The information in this book is presented in general terms. To specifically address the exact TEMPEST relationship would be outside the classification level of this text. However, by presenting the necessary information in classical form, the subject matter can be effectively covered in a non-classified environment.

Students more interested in practical applications rather than theory should consider this text as an overview, treating each area with respect to the potential for more in-depth review as needs dictate. Theoreticians and signal analysis experts will find the mathematical relationships and definitions extremely useful in a single source reference. Figure 1-1 below depicts the book organization.

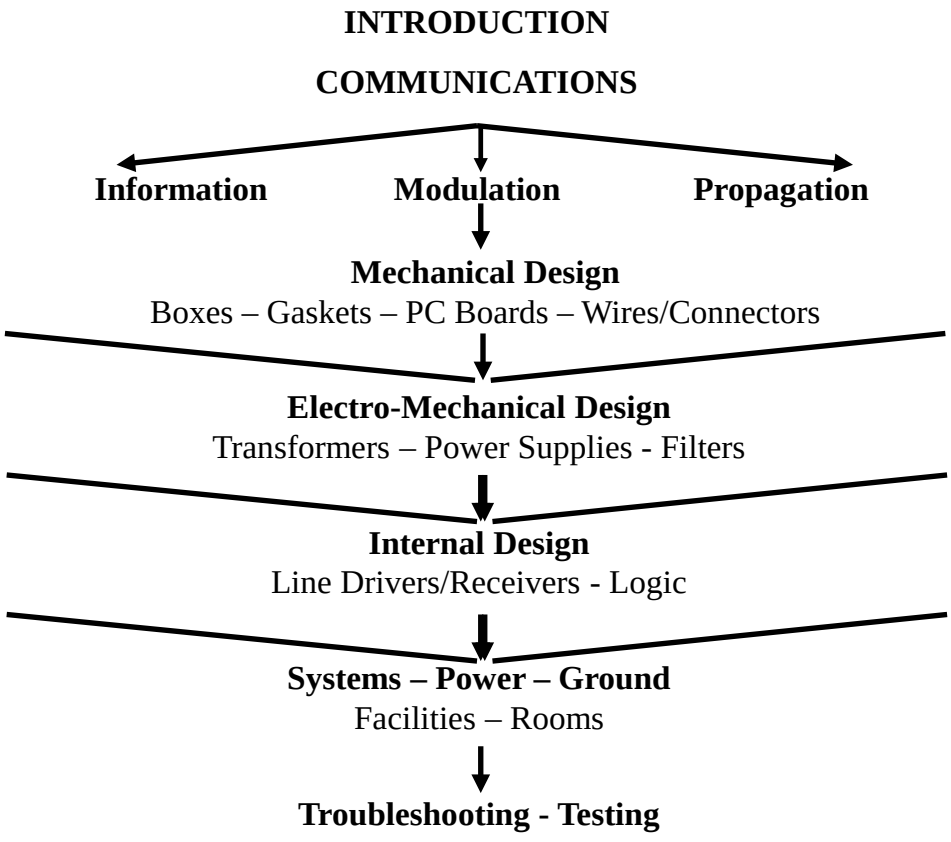

Figure 1-1 Book Organization

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.

Typical Misconceptions

TEMPEST is a black art only understood by very few technical individuals.

TEMPEST can always be added in once the electronic design is finished.

TEMPEST emissions can always be controlled with shielding and filtering.

No one can see a signal in "all that noise"

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.

The Tempest Industry

Prior to the 1980s, the TEMPEST industry experienced tremendous growth. However, due to equipment emission controls, regulation changes, and how emissions can be detected, the industry suffered significant losses. The current focus is more on facility and zone protection; with TEMPEST still a factor in the COMSEC and tactical environment. From the commercial equipment perspective, basically manufacturers of various data processing or telecommunications related products want to sell these products within the defense industry. The commercial need for TEMPEST support is therefore primarily in the realm on design and accreditation work.

Needs and Costs

Defense companies face TEMPEST needs from two directions: direct and indirect. Many contracts involve TEMPEST design identified directly in the statement of work for a product. Labor costs involved in hiring and supporting full time employees for single contract TEMPEST requirements are high.

The second TEMPEST need faced by defense contractors is not as specific. In this case, the contractors have security requirements imposed on their programs which define the need to physically perform the engineering and documentation work on processing equipment that has been TEMPEST emission secured. To satisfy this requirement, contractors can purchase TEMPEST secure equipment directly, or they can meet the TEMPEST requirement through a facility zoning approach. The zoning approach again requires either in-house employee technical support, or the use of outside consultants.

If the purchase of TEMPEST secure equipment is necessary, this need provides an additional support requirement from the equipment manufacturer. In this case, the manufacturers of commercial versions of the secure equipment must either redesign and test the

equipment in-house, or seek out a firm specializing in TEMPEST work to perform the necessary engineering and/or testing activities. Many companies choose a combination of training supported by some outside consulting.

Who Does Tempest Work?

With significant technical requirements driving the need for outside TEMPEST support, two types of organizations have evolved to serve marketplace. In the commercial equipment industry, since engineering costs generally amount to 70% of a TEMPEST design and certification program, the real governing factor in awarding a program is actual costs.

The least expensive support comes from design and documentation type organizations which perform all non-testing related activities for an organization, then farm out the actual certification and accreditation test to a local test house. Overhead costs for the consulting only type firms are substantially lower than test organizations due to differences in test equipment expenses and maintenance. While consultants with substantial direct experience are rare, these organizations have become extremely popular in recent years.

The primary drawback to engineering service only commercial support organizations is that they are not recognized directly by NSA currently under the Endorsed TEMPEST Services Program. However, since the NSA directly evaluates all documentation submitted by both the Company Appointed TEMPEST Authority and by the Certified TEMPEST Engineer, so long as experienced and recognized individuals submit the necessary documents and the resulting designs successfully pass the test requirements at an approved laboratory; the equipment is approved regardless of who did the work. This approach is similar to what is taking place in the FCC equipment certification industry currently, with consultants charging considerably less then approved test organizations to redesign equipment for emission control.

Large defense industry organizations with direct TEMPEST support requirements are very limited in the methods they can use to satisfy contractual requirements. Major consulting firms have high overheads, and subcontracting costs, while short term in nature, will be higher than hiring in-house personnel directly. Small business consultants are also normally expensive. In addition, few are willing to take on major projects that require full time support for extended periods of time. Probably the best approach for a defense contractor with a small or medium technical requirement is to hire the lower cost less experienced employee, and then arrange for an established consultant to support the program on a part-time basis.

Where is The Technical Support Available?

The majority of TEMPEST test work is performed along the East Coast from Washington D.C. north to New England. Since NSA and the Department of Defense are headquartered near Washington D.C., most industry support and talent has developed in this region. Design engineering organizations are scattered throughout the country. Many of these organizations offer both EMC and TEMPEST support. However, EMC and TEMPEST are not the same. TEMPEST and EMC conducted test approaches are different and the documentation cannot be combined. TEMPEST in not closely related to EMI except for some applications in the use of shielding, grounding, and passive filtering. EMI is concerned with overall noise while TEMPEST does not consider noise levels, but analyzes communication signal related voltage measurements on power and data lines. Measurement bandwidths, sensitivity levels and frequency requirements are incompatible

The problem with many TEMPEST oriented commercial and consulting organizations is their major reliance on these few key technical staff members. Many TEMPEST support organizations are owned by either engineers or businessman with non-technical TEMPEST backgrounds. Without someone at the top who can technically run the entire program, these organizations are continually forced to take shortcuts or negotiate with available talent to keep their business operations active. The cost and resultant problems in years past with companies who took shortcuts forced the National Security Agency eventually change their existing procedures regarding commercial equipment accreditation requirements. Costs were also a factor driving the zone protection requirements that eventually evolved.

Definitions and Concepts

The primary definitions used in this text include:

- Security
    - A state that exists when all measures have been taken to provide a level of protection considered free from danger.
- COMPUSEC
    - Protective measures to prevent the unauthorized access to or use of computer based information.
- COMSEC
    - Communications security is that measure taken to deny unauthorized persons access to telecommunications information.

The four components of COMSEC include:

- Cryptographic
    - Conversion of intelligent information to a form unintelligent to the unintended recipient.
- Transmission
    - Methods of minimizing unintended interceptions
- Physical
    - Physical methods of access
- Emissions
    - Methods taken to prevent unauthorized derivation of information from emanations.

In TEMPEST, you're dealing with a difficult problem that's hard to find; wires, power systems, and haphazard grounds can provide many paths for signals to get out. A typical real aircraft platform is shown in Figure 1-2. Real platforms require significant emission controls be installed to protect

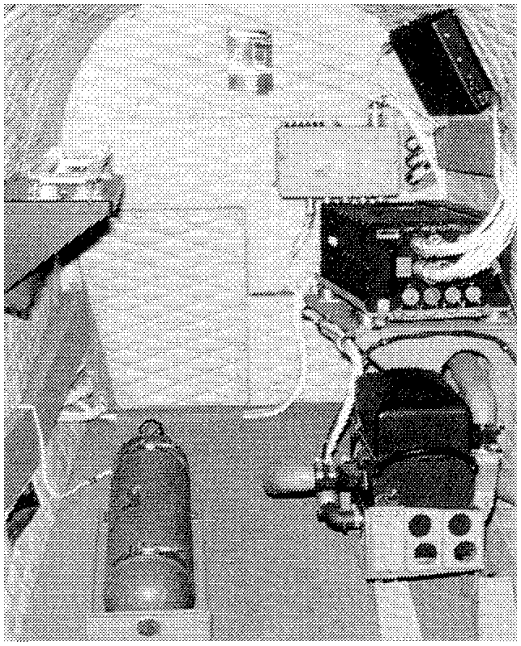

Figure 1-2 Typical Aircraft Platform

against inadvertent loss of information. Remember there is no earth ground in the air so significant attention to detail is necessary to design a secure, TEMPEST emission free environment.

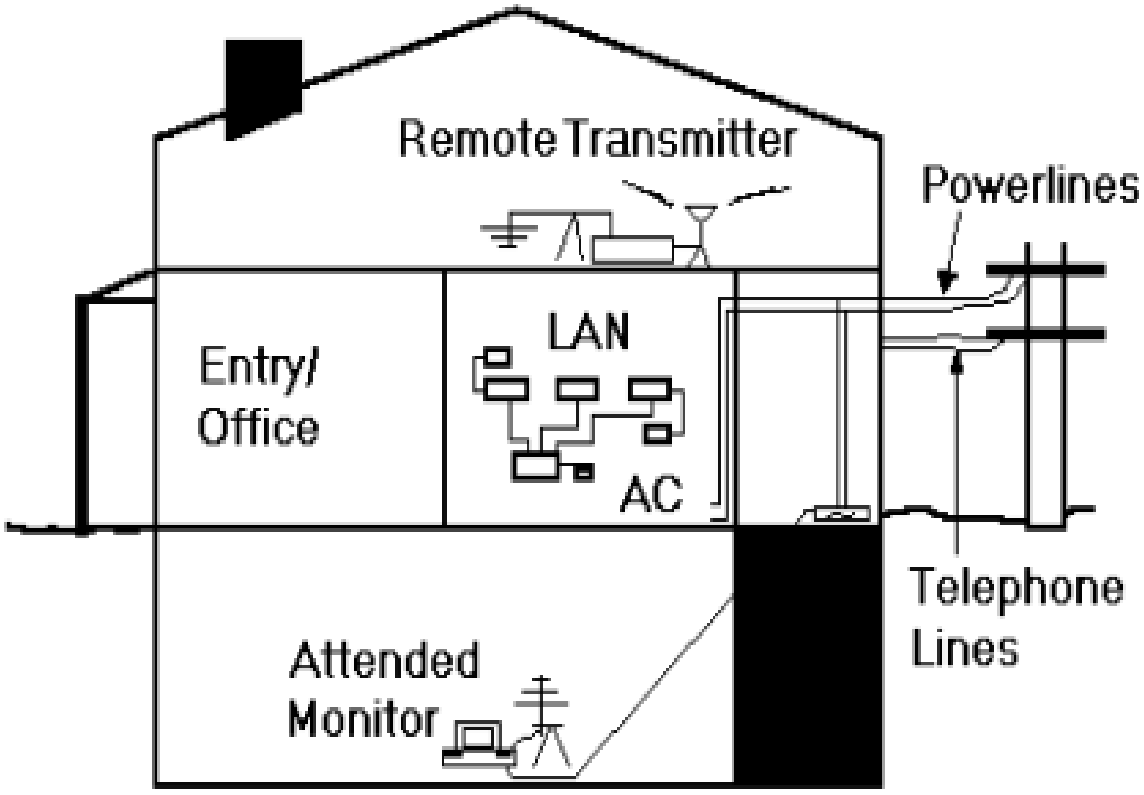

Figure 1-3 Threat Locations in a Facility

Real threats exist in facilities as well. Figure 1-3 shows possible facility threats due to radiated, conducted or fortuitous emission paths. In this case, a covert observer could be located virtually anywhere, including in a parking lot or under a telephone line.

Another concept used herein is the RED/BLACK concept. Electronic circuits, components, and systems that handle classified (plain text) in electric signal form (RED) must be separated from those that handle encrypted or non-classified (BLACK). Circuits that handle Crypto-variables are often considered as RED-RED.

What is the Best Approach?

Since threats are potentially widespread, since emissions can show up anywhere, and since subject matter experts in TEMPEST design are difficult to find, what is the best approach if you have a real compromising emanation problem to solve? Basically, it resolves around cost trade-offs between:

- Electronic Approaches
- Source suppression
- Shielded enclosure or building (containment)

- Facility radiation zone

Remember that it's very difficult to design TEMPEST protection into a circuit after it's built and functioning. Many designs used the "BLACK BOX" approach whereby a conductive box was put around equipment in an effort to contain the emanations. These approaches often failed or were too difficult to use or maintain. It's much easier to apply source suppression into the initial design. Figure 1-4 shows the many locations where an emanation can escape an equipment enclosure.

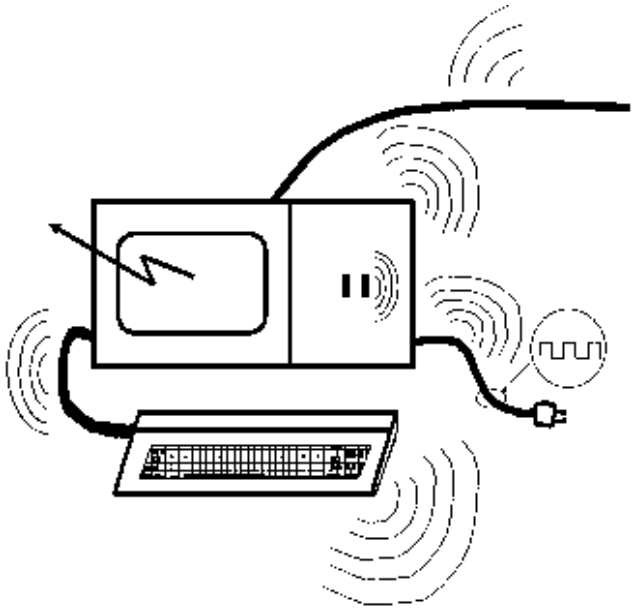

Figure 1-4 Multiple Leakage Points

Classification Differences

A final note on classification is needed before we continue. All EMI/EMC design techniques, and rational for their incorporation, are unclassified. On the other hand, TEMPEST design techniques are unclassified, or, when combined with rational for their incorporation in a specific component, are classified SECRET. Schematics with no specific reason for a particular design are not classified. Schematics are normally classified for COMSEC equipment.