Assessing the Need for Shielding at Secure Data Processing Facilities (Vulnerability Assessments) and Possible Problem Solutions

Bruce C. Gabrielson, PhD
Security Engineering Services
PO Box 550
Chesapeake Beach, MD 20714

Introduction

TEMPEST vulnerability assessments have not received the attention they deserve in recent years. Although there has been a redirection in the impact of TEMPEST countermeasures and requirements, neither the requirements nor the demonstrated need have ever disappeared. Even with secure processing equipment normally located inside a controlled area, there usually exists a requirement to provide some form of assessment concerning just how secure emissions from equipment operating in the controlled area really are. The question that should first be asked is "Do we really need to worry about protecting secure data processing equipment with some kind of expensive shielded room?" This question is asked time and time again, and the answer is nearly always determined by how much money is available, the level of classification assigned to the data being processed, and the threat presented by hostile intelligence agencies.

> ***TEMPEST IMPACT***
>
> ***Although there has been a redirection in the impact of TEMPEST countermeasures and requirements, neither the requirements nor the demonstrated need have ever disappeared.***
>
> ***There usually exists a requirement to provide some form of assessment concerning just how secure emissions from equipment operating in the controlled area really are.***

Although the exercise is necessary, seldom is a good hard assessment of genuine shielding needs performed prior to determining that a shielded room, screen room, or conductive painted room will be assembled at a specific sensitive location. While various documents, such as MIL Handbook 232, NACSEM 5109, NACSEM 5111, and NACSEM 5203, and DIAM 50-3 provide guidance and verification criteria for various secure facilities applications, it still falls upon the engineer responsible to determine the unique techniques and application of principles to be employed at each individual location.

This paper provides a sequential method of determining both the vulnerability, and, if necessary, the grounding and shielding needs for protecting the various types and combinations of secure equipment assembled at any specific location within a secure (RED/BLACK) facility. In addition, it describes the test techniques used to verify the shielding effectiveness of rooms, and the sequence of events that occur related to security during a typical building procurement process. The vulnerability assessed refers to the common TEMPEST radiated and conducted vulnerabilities associated with facilities that process classified information and does not address physical security.

Determining the Vulnerability

The Equipment TEMPEST Radiation Zone (ETRZ) is a zone established as a result of determined or known TEMPEST equipment radiation characteristics. The control zone includes all space within which a successful hostile intercept of TEMPEST Compromising Emanations is considered possible. Notice that this zone refers to radiated characteristics, primarily the E field characteristics. TEMPEST signals can take the form of E field or H field radiated emissions, conducted emissions, or emissions from fortuitous paths. However, for even a medium size installation, identifiable conducted emissions from a specific signal source become very difficult to identify as the distance from the source increases. Therefore, for typical installations with a large controlled access area (exclusion area), the primary security concern is for radiated signals.

Fortuitous source emissions are an unusual combination of signals which can appear on any conductor, and which provide an unintended path for intelligible signals. These paths could be water pipes for cooling a mainframe computer; building, fence or wall metal structural members; air conditioning ducts; cable shields for local area network equipment; overhead powerlines between buildings with different ground potentials; and telephone cables. In all cases, the objective is to prevent sensitive signals inside the control zone from appearing to a covert collector outside the zone. A typical control zone for a super computer is shown in Figure 1.

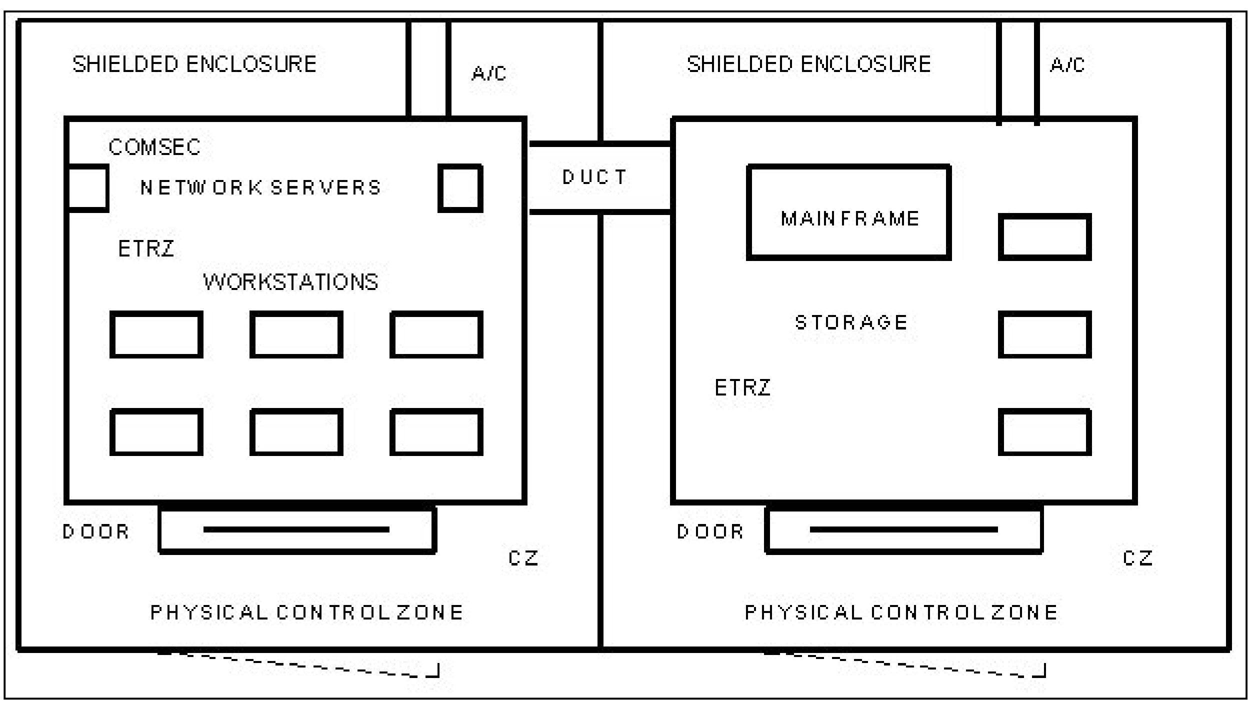

Figure 1 - Super Computer Control Zone

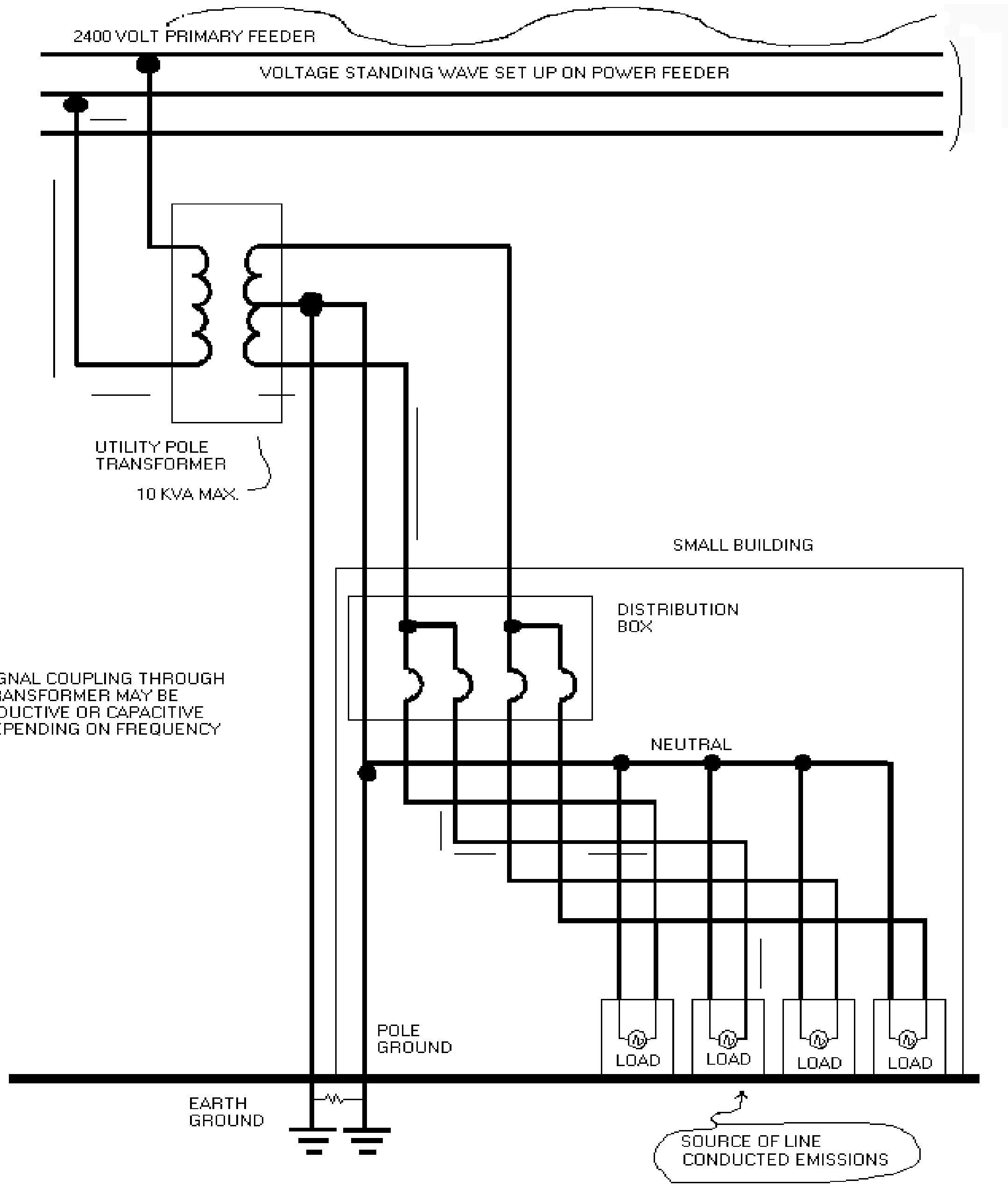

Figure 2 - Extended Antenna System on Powerlines

Sometimes the physical path signals take to reach outside the control zone are extremely difficult to identify. One unusual antenna path often overlooked is the power feeder system for the facility. Not only are conducted emissions a problem on power lines, but the entire building power structure can represent an extended wire transmission system, with compromising signals actually being re-radiated based on the antenna characteristics of the powerline wiring system of the building. These antennas are very much longer than those on circuit boards or wiring harnesses.

The rf conducted emissions on the power line can get back to the power primary feeder line through the utility pole transformer.

Figure 2 shows the power distribution extended antenna. The powerline ground has inductance that will keep the equipment side of the ground wire at a rf potential above ground.

A number six wire has an inductance of 0.301µH per foot. A twenty-foot ground wire has an inductive reactance of 37.8 ohms at 1000 KHz. At higher frequencies the reactance is proportionally higher. Therefore, the ground side of the power leads will be at rf potential above ground for any power line conducted rf emissions. These emissions will couple through the utility pole transformer to the primary feeder. The coupling will be inductive at low frequencies and capacitive at high frequencies. The latter is due to the capacitance between the windings. Thus there is an entire "antenna farm" of radiators for the conducted emissions. The emissions can be radiated great distances from the powerline, and also can be conducted for a fairly long distance unless they are suppressed at the source.

Another emission problem often overlooked is the antenna farm effect due to interconnecting cables. In a system with well designed enclosures, a field induced problem can be created by the shielded or non-shielded cable between enclosures. Unshielded wires carrying differential mode signals will radiate due to either an offset voltage on one wire, or due to common mode noise on both wires. For a shielded cable carrying either common mode or differential mode signals, unwanted energy coupling will be the result of current flow on the cable shield itself.

The term differential mode (balanced or transverse mode) describes signals that are sent out over and return back over another wire. Neither wire is grounded, such as the case of the transformer coupled MIL-STD-1553 data buss. For differential mode transmissions, when the signal on one wire goes up by +V, the signal on the opposite wire goes down by -V with respect to ground. Figure 3 describes common and differential mode voltage potentials.

The term common mode (or longitudinal mode) describes signals that are sent over one wire and return via a common ground. The voltages on the sending wire vary with respect to ground, and can be especially troublesome if the ground at each end of the cable has a different potential.

In general, it is very difficult to accurately predict the antenna effects of interconnect cabling. Where this becomes an issue is if the building's average power consumption is 100 KVA or higher. Current regulations state that TEMPEST countermeasures are not a CONUS (Continental US) concern for facilities with power consumption above this level, regardless of what a vulnerability assessment indicates. Determining the <u>AVERAGE</u> power consumed is not as simple as it seems, so the following information will address the vulnerability assessment problem as it really exists.

A TEMPEST site survey test would produce a more accurate evaluation of the potential problem. However, two criteria can be evaluated which will identify the potential for a TEMPEST problems existence. If interconnecting cables are more then 10% the length of the wavelength of the signals carried (or any coupled signals which might also be present), the potential for a problem exists. The wavelength of a 100 KHz signal is 3000 meters in air. Therefore, problems should exist primarily at very large facilities.

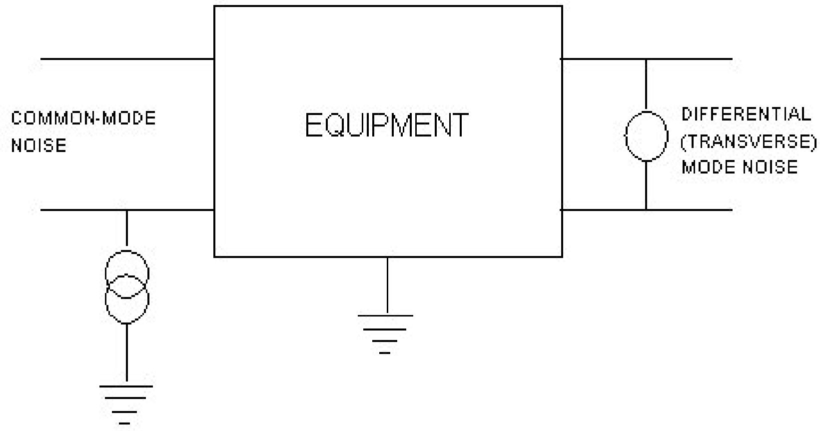

Figure 3 – Common and Differential Mode Noise

One issue to look at is whether or not cable shields are greater than skin depth thick compared to the signals being carried. Skin depth indicates how far an electromagnetic field can penetrate a conductor before its amplitude is reduced to 37 percent of what it was at one surface. Since most cable shields are less then a skin depth thick. substantial leakage can occur directly through the shield. The formula for skin depth is provided below.

$$\sigma = 5\sqrt{\varepsilon / \mu_r f}$$

where $\in$ is the resistivity of the metal in ohm-cm
μ_r is the permeability of the metal relative to air
f is the frequency in MHz

The final issue to examine which could lead to common mode or differential mode TEMPEST problems is the facility ground system. It is seldom the case that the grounds in two parts of a building are at exactly the same potential. Very low ground potentials can occur if the building has welded rebar embedded in the foundation, but this is generally not the case in most buildings. If a difference in the ground potential is suspected, a cable shield connecting two locations in the facility should be isolated at one end to prevent current flow in the shield.

As shown in Figure 4, hostile threats can be attended or unattended, and can be located above, below, or to the side of the room where secure processing equipment is located. High quality receivers are sensitive to signals within 6 dB of theoretical Johnson noise floor, so sensitivity is not a problem. In addition, techniques have been developed that defeat the need for highly sensitive receivers. Also, real time recorders can be used when analysis is not performed on site, eliminating the need for continuously active interception. For most processing equipment, unless very high resolution monitors are in use, threat frequencies are usually considered to exist primarily between 1 MHz and 300 MHz. The point is that if reasonable access can be achieved to an unsecured site near the processing equipment, the task of intercepting compromising information is not an impossibility.

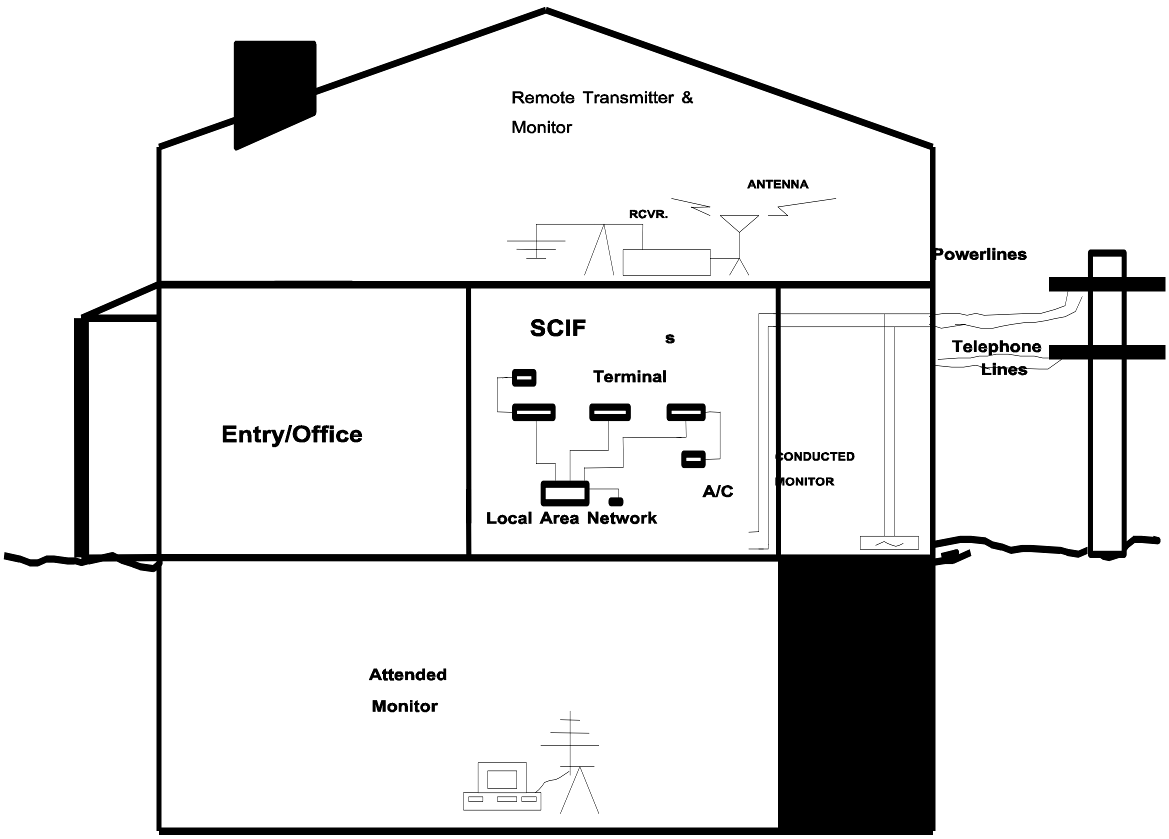

Figure 4 - Threat Locations

Equipment Emission Properties

There is currently significant interest in using off the shelf FCC approved equipment in the secure processing environment, while assuring limited additional protection through TEMPEST equipment profiling (zoning) or building walls. In order to evaluate what FCC approval means in perspective, the FCC limits must be compared directly against the specified TEMPEST or security related limits applied to the equipment to be installed. Look at the FCC limits shown in Figure 5 below.

The fact that a package of equipment processing secure information meets the FCC radiated limits shown above is insufficient to provide any rational relating to how much environmental attenuation is necessary for full TEMPEST radiated protection. However, if we know a little information about the equipment being considered, if the FCC report is available, and if we assume all radiated emanations from the equipment carry meaningful TEMPEST information, the problem of environmental attenuation becomes more bounded.

Using the voltage form for bandwidth conversions, take a sampling of the highest level signals between 10 MHz and 1 GHz from the FCC report and convert the levels to levels that can be applied towards TEMPEST limits. Notice also that the FCC measurements are taken at a distance of 10 meters. This conversion calculation is a little more difficult since transmission is directly effected by the physical proximity of the conductive ground to the receiving antenna.

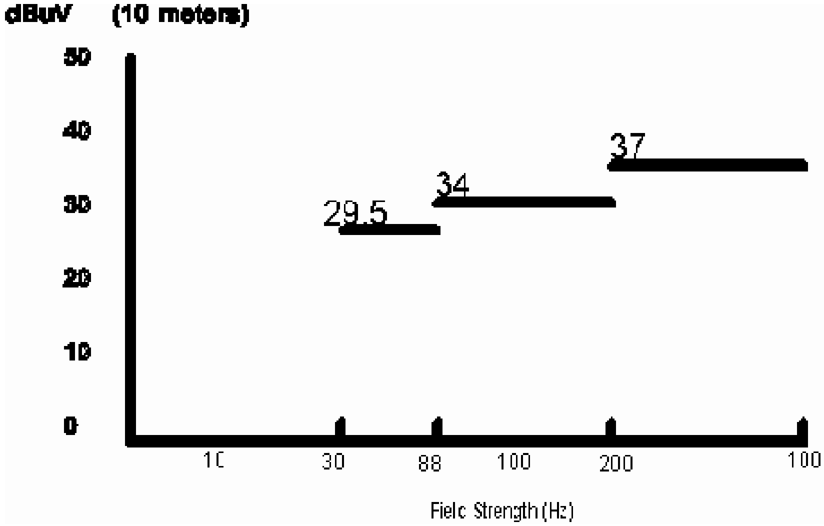

Figure 5 - FCC Limits

In general, for free space, optimum transmission is achieved when two doublets are parallel to each other and perpendicular to the line connecting their centers. If their distance apart, d, is large compared to the wavelength of the propagating signal, the ratio of power transmitted to maximum useful power received is easily determined from the following equation:

$$\frac{P_2}{P_1} = (3\lambda/8\pi d)^2$$

"P_2 is the power delivered to a matched load at the output terminal of the receiver and P_1 is the power fed to the transmitting antenna. d and λ are measured in the same units. If transmission takes place over a conductive ground or in a refracting atmosphere, the power ratio changes slightly to include the antenna gains G_1 and G_2 of the transmitting and receiving systems, and a new factor Ap is added representing the "path factor". If the electric field at the position of the receiver is desired, it is found by solving the following for power in watts and E in volts per meter."

$$E = 3\sqrt{5}\,\frac{\sqrt{P_1 G_1 A_p}}{d}$$

ROUGH TEMPEST VULNERABILITY ASSESSMENT

By subtracting the allowable TEMPEST level from the FCC emission level at various frequencies selected, a fairly accurate estimate can be made of the level of attenuation required to meet TEMPEST security, through either space loss or by shielding.

Notice that d appears in the denominator, and the path factor appears in the numerator. It is obvious that the most important and difficult part of determining field strength is the quantitative determination of the path factor as a function of the geometry of the transmission path, electromagnetic properties of the conductors or grounds associated with the path, the refractive properties of the atmosphere, and so forth. We could go on and examine the electromagnetic properties of grounds as described by their complex dielectric constants, etc., but our purpose is a bounded and simplistic solution to the radiation problem. Therefore, we will assume simple free space transmission as a worse case, and can use the chart provided in Figure 6 to determine relative field strength loss for various frequencies and distances. From the chart, the field strength loss in dB will be added to determine the appropriate level for the FCC emission to be compared against the TEMPEST limit. Next, by subtracting the TEMPEST emission level from the FCC emission level at various frequencies selected, a fairly accurate estimate can be made of the level of attenuation required to meet TEMPEST security, through either space loss or by shielding.

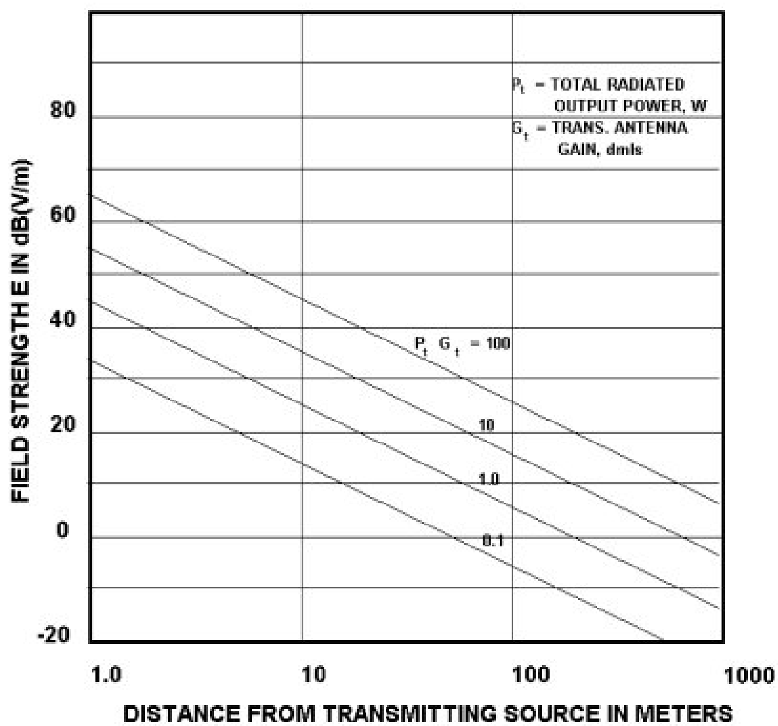

Figure 6 - Free Space Transmission Loss With Distance

Environmental Shielding

All structures provide a certain level of environmental shielding at some frequency. According to Ferraris[1], research has shown that the attenuation provided by dry, single layer brick is negligible below 300 MHz. Above 300 MHz, some attenuation may occur, but usually less then 5 dB. Block wall and brick construction, and also non-reinforced concrete, have nearly identical characteristics.

[1] *Ferraris, L., **The Screening of Existing Rooms and Buildings**, RFI Shielding, Braintree, CM7 7YW, Enigma Variations, 1988.*

I-beam girder construction, typical of that used both on external walls, and some internal office walls with aluminum or conductive replacements for wood 2 x 4 construction, provide shielding dependent on the spacing of the girders. Anodized aluminum, however, looses between 30 and 50 dB of shielding effectiveness between 100 KHz and 100 MHz, and will provide little in the way of environmental attenuation if used in wall construction. For maximum shielding, the metal must be well bonded to the building ground, not simply attached with a bolt at one or two points. This means that if bolts attaching the beams and girder assembly, plus the surfaces attached themselves, were not cleaned prior to assembly, some additional degradation (20 to 30 dB) of shielding effectiveness occurs.

The calculation of environmental shielding for I-beam girder construction is straight forward. The cut-off frequency for the wall being considered is the frequency below which attenuation is virtually non-existent. This frequency directly relates to girder spacing, and is approximately the frequency at which the girder spacing is approximately one tenth of the wavelength. The cut-off frequency is calculated from:

$$f_c = \frac{C}{2d}$$

Where c is the speed of light and d is the distance between the girders. From this equation the shielding effectiveness at some frequency of interest f can be found from:

$$SE(dB) = 20 \log \frac{f_c}{f}$$

Reinforced concrete provides the greatest environmental attenuation to radiated signals. Iron reinforcement rods used in floors and ceilings are connected in a grid pattern, and can provide significant shielding, especially if the cross-members are welded or otherwise conductively attached. In addition, The ends of each rod must also be bonded if maximum attenuation is desired. The requirement for welded rebar in new structures is often a construction requirement.

In this case the cutoff frequency is again the frequency where the maximum spacing of the grid is about one tenth of the wavelength. However, in this case also we have multiple grid openings in the form of squares surrounded by conductors.

The final building construction method is the use of hollow steel ribs with layered concrete. For this case there is usually no solid electrical contact between adjacent ribs. Therefore, as in the case with brick or block wall construction, environmental attenuation is found from the previous equation.

One important point to clarify is that although some attenuation is available at about 3 MHz, there is virtually no attenuation provided above 30 MHz. Therefore, since the radiated threat from most data processing equipment exists above this frequency, additional shielding will still be required in most instances, either from room to room or from room to outside wall.

Only an in depth review of the facility, equipment, and security requirements, plus a detailed review of the building construction characteristics will allow the incorporation of security engineering features into the design. To accomplish this objective, and to determine the amount of increased structural shielding required, an understanding of the shielding effectiveness of the various shielding options is required.

Shielding Effectiveness Theory and Facility Construction

Figure 7 is the standard representation of incident wave, reflected wave, absorbed wave, and re-reflected wave. Shielding effectiveness for the so called "infinite plane" is expressed mathematically as:

$$SE = 20 \log |e^{lv}| + 20 \log |\frac{1}{\tau}| + 20 \log |1 - re^{2vl}| = A + B + C$$

where l thickness of the shield

- v propagation constant of the shield
- τ the transmission coefficient
- r reflection coefficient

It is not the intent of this section to go into a detailed analysis of shielding theory, especially for realistic shields, but instead to evaluate the reflected component of the above equation. Reflection loss depends upon the distance from the source to the shield rather than upon the shield thickness for both low and high impedance fields. In these cases, the reflection loss decreases as the frequency increases, and is better when the ratio of g/μ is higher. g is the conductivity of the shield material relative to copper, and μ is the relative permeability of the shield material.

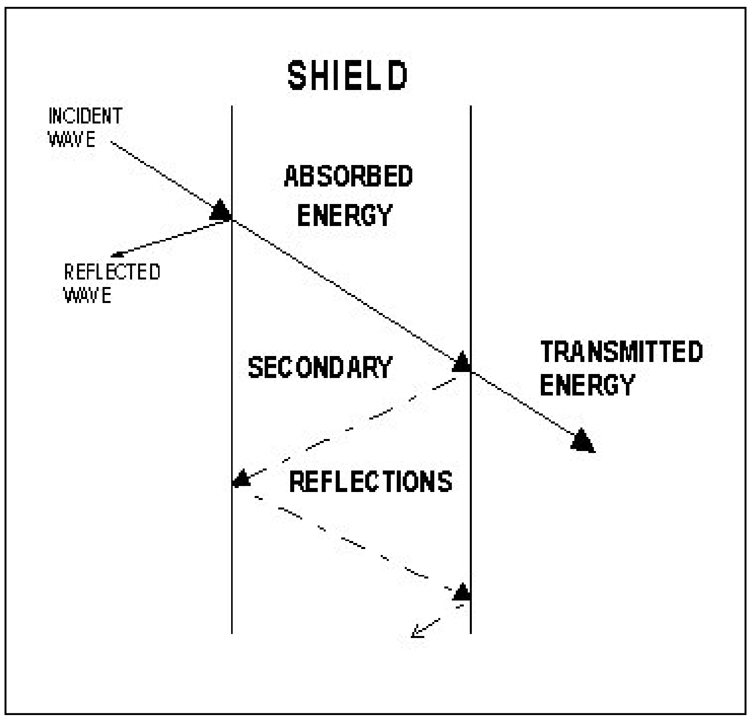

Figure 7 - Waves at a Shield

The EM field at a distance of more then a few wavelengths from its source is essentially a plane wave usually with a wave impedance equal to the intrinsic impedance of the propagation media (377 ohms for air). Unlike the low and high impedance fields associated with the near-fields of magnetic dipole and electric dipole sources, the plane wave field reflection loss is independent of the distance between source and shield. The plane wave reflection loss decreases as the wave frequency increases, and is better for shielding materials with lower μ/g ratios.

THIN SHIELDS

It is possible in some instances to provide significant shielding effectiveness to an existing structure through the use of multiple thin layer shields located at successive locations within the structure.

The bottom line with all the above theory is that it is possible in some instances to provide significant shielding effectiveness to an existing structure through the use of multiple thin layer shields located at successive locations within the structure as shown in Figure 8. If walls are being built, a layer of conductive environmental material both outside and inside each panel side, and on both sides of a wall, will greatly enhance the attenuation characteristics of the wall. The ideal situation is to provide one multiple shield layer on both sides of the wall near the processing equipment, and then provide a second multiple layer on a wall located at a distance based on the calculated threat in the far field from the processing equipment. Using steel doors and metal plates on outlets will reduce potential shield degradations due to discontinuities.

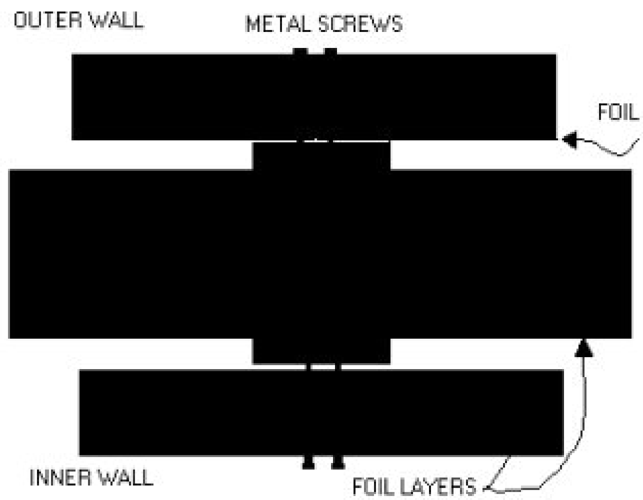

Figure 8 - Multiple Thin Shields

Ceilings and floors, especially false floors, are protected in the same manner as walls, but in these cases, additional consideration must be placed on the shield degradation effects based on continuous stresses and discontinuities in the shield.

Windows can be protected using either a mesh laminated between glass panels, or a conductive coating sprayed on the outside of the glass. Figure 9 and 10 show shielding characteristics of conductive-coated glass. Below 1 MHz mesh attenuation is slightly better then glass coatings, and averages about twice as much attenuation from around 10 MHz up. It is important to note that either technique is expensive, and should not be considered unless absolutely necessary, or when other interior shielding is ineffective.

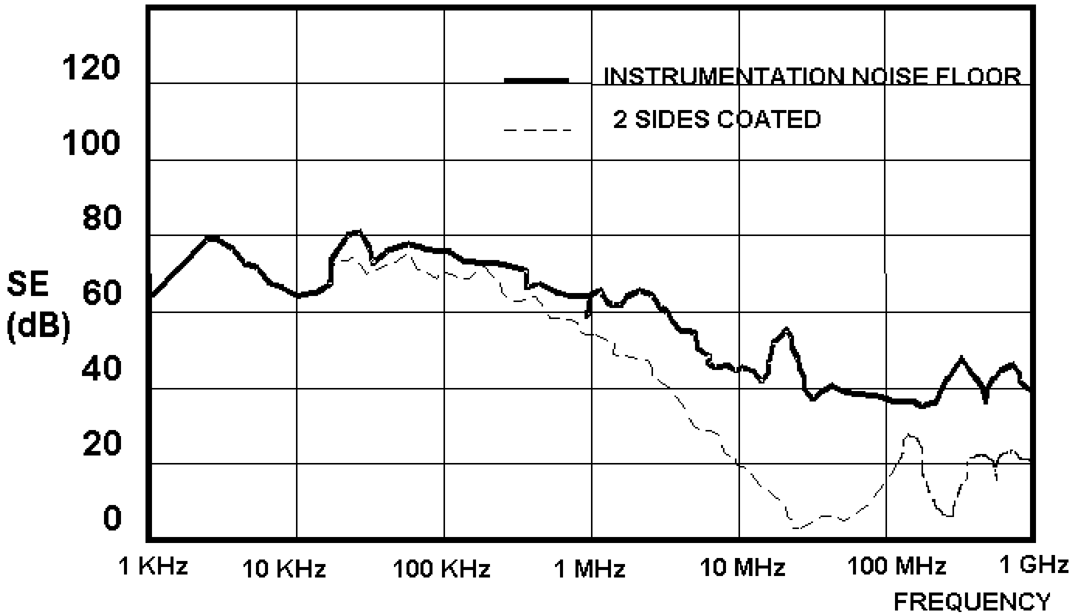

Figure 9 - Aperture Attenuation

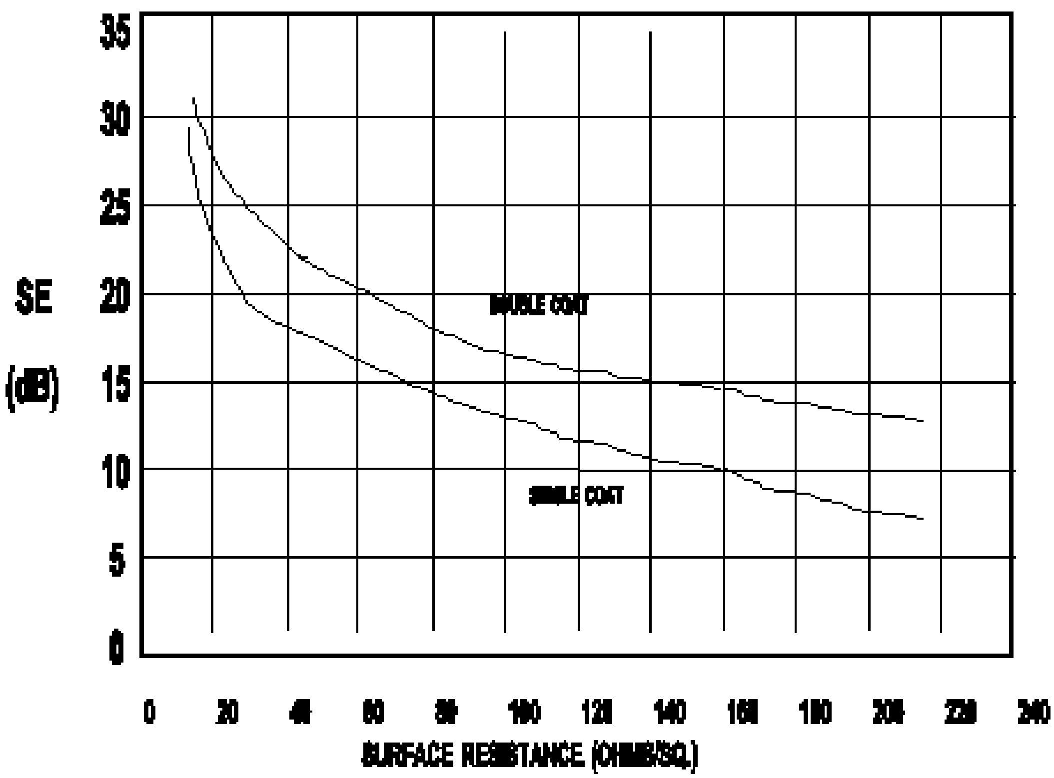

Figure 10 - Shielding Effectiveness of Conductive Glass to High Z Waves

Apertures

Theoretical shielding effectiveness and attenuation calculations are based on an infinite conductive plane with a finite thickness. When this plane is penetrated by a discontinuity, the shielding effectiveness is degraded by leakage of the electromagnetic energy. The amount of energy able to penetrate through an aperture is related to the longest physical dimension (d) of the hole, and the wavelength of the radiating field. For wavelengths equal to twice the hole dimension or larger, the energy will pass through the opening with no attenuation. The frequency where the energy passes without attenuation is the cut-off frequency described earlier f = c/2d. Below this frequency, the aperture attenuation can be found from:

$$R(dB) = 20 \log \frac{\lambda}{2d}$$

$$t \text{ is the wall thickness} \quad \frac{\lambda}{2} > d > t$$

Apertures reduce both the reflection and absorption characteristics of a shield. The reflection term is lowered as a result of an increase in the barrier impedance relative to the wave impedance. This increase in barrier impedance is caused by leakage inductance, and is related to the dimensions of the aperture and the spacing of the radiating circuits from the aperture. Normally, an aperture provides 0 dB shielding at the cut-off frequency, and increases linearly at 20 dB per decade as frequency decreases. Figure 10 shows aperture attenuation for various values of thickness d. These values are accurate for noise sources located at a distance at least as far or farther away from the hole than the value d.

At distances closer than d, the approximate cut-off frequency is reduced proportionally to the ratio of the distance (r) from the aperture to the dimension d. The approximate cut-off frequency and attenuation are changed to:

$$f_c = \frac{C}{2d}\left(\frac{r}{d}\right)$$

$$R_{dB} = 20 \log \frac{f_c}{f} = 20 \log \frac{\lambda}{2d}\left(\frac{r}{d}\right)$$

$$\text{where} \quad \frac{\lambda}{2} > d$$

For a wall hole such as non-metal electrical switch holder and cover, the hole resembles a rectangular waveguide. The cut-off frequency for a rectangular waveguide is:

$$f_c = \frac{1.5 \times 10^{10}}{w_{cm}} = \frac{5.9 \times 10^{9}}{w_{inch}}$$

where w is the largest dimension of the waveguide cross section.

For frequencies much below the cut-off frequency (f/f_c) much less then 1, the absorption loss A becomes:

$$A\ dB = 27.3\ t/w$$

where t = depth of the waveguide

Available Facility Shielding Techniques

When available facility attenuation and inherent emission characteristics are such that increased attenuation from the facility becomes necessary, a variety of techniques can be used to upgrade facility emission protection.

Four primary methods are used to enhance interior shielding in buildings; conductive coated walls, foil linings, copper mesh screens, and metal enclosures. Each technique has advantages and disadvantages depending on logistical and life cycle factors such as permanence, location, physical proximity to potential threat, level of threat, physical proximity of processing equipment, looks, budget, environment, and size requirements. However, conductive spray coatings and metal foils lend themselves to outer decorations and paint coverage better then metal or mesh walls.

Conductive paints are available that use silver, nickel, graphite, or copper as their base. Paints are easy to apply on multiple surfaces between the data processing equipment and the outer edge of the protective zone for existing buildings. Table 1 describes the advantages and disadvantages of each type. Note that overlap seams are not required for paint applications.

AVAILABLE SHIELDING METHODS

conductive coated walls
foil linings
copper mesh screens
metal enclosures.

The conductivity, and hence the shielding performance of metal filled coatings are effected by factors such as pre-coat, coating thickness, coating formulation, viscosity, and drying rate. The surface treating prior to metal coating in important to insure the metal coating does not flake off. The substrate should be coated with materials compatible with the resin used for the metal filler. The formulation of the paint is important and can effect the conductivity by as much as a factor of 3[2] for coatings of identical thickness. In a very low-viscosity coating layer, the metal filler tends to settle, creating a layer primarily of resin on top and primarily metal next to the substrate. To minimize settling, coatings should be sprayed at as high a viscosity as reasonably possible, and usually with a 1:1 dilution with thinner.

The temperature during application, and the temperature extremes the coatings are exposed to, also effect conductivity. Walls should be painted when warm dry conditions exist. Forced drying during application is not recommended since it tends to decrease conduction. As a rule, if forced drying is absolutely necessary, it should not be used until the solvent has flashed off. Normally, slower evaporating thinner is used. Coating to a thickness of .05 mm or thicker will reduce the effects of temperature cycling if the facility is subjected to this type of condition. The attenuation properties at 10 MHz of each type of paint are described in Table 2.

Table I - Advantages and Disadvantages of Paint Types

Base	Advantages (single coat)	Disadvantages
Silver	Good conductivity Conventional equipment Resistant to flaking Conductive oxide Ease of application 60 - 90 dB Shielding	Expensive
Nickel	Conventional equipment Good conductivity Oxidation resistant 30 - 60 dB Shielding	Need proper dry film thickness for maximum shielding effectiveness Moderately Expensive
Graphite (carbon)	Conventional equipment Good corrosion resistance Inexpensive 5 - 20 dB Shielding	Not very effective shield
Copper	Conventional equipment Ease of application Questionable corrosion resistance 30 - 60 dB Shielding	Copper oxidation reduces conductivity Moderately Expensive

COATING MATERIALS

RFI Shielding
Zinc-Tin Spray
Nickle Filled Acrylic
Nickle Filled Aqueous Polymer
Graphite Filled Acrylic
Two-part Copper/Epoxy Polymer
One-Part Silver Acrylic

Conductive Adhesives
Two-Part Silver Epoxy
Two-Part Copper/Epoxy Copolymer
One-Part Copper/Epoxy Copolymer

[2]*Amato, J.R., et al.,* ***Shielding Effectiveness****, IEEE Transactions on Electromagnetic Compatibility, Vol. 30, No. 3, August, 1988.*

Table 2 - Attenuation Properties of Paint

Base	Thickness (ml)	Resistivity (ohm/sq ft)	Attenuation (dB)
Silver	1	0.04 - 0.1	60 - 70
Nickel	2	0.5 - 2.0	30 - 75
Graphite	1	7.5 - 20	20 - 40
Copper	1	0.5	60 - 70

Wall linings usually take the form of conductive foils or textiles. Wall linings are often preferred when higher attenuation is required and they facility already exists. Textiles have almost identical characteristics to foils at higher frequencies, and they are much easier to work with. They have high transparency to visible light close permeability to air. Their primary disadvantage is cost since they are considerably more expensive then foil. The Table 3 below lists typical attenuation values for a high attenuation metalized textile:

Table 3 - Metalized Textile

Frequency	Attenuation
10 MHz	65 dB
100 MHz	75 dB
1 GHz	85 dB
10 GHz	90 dB

PROBLEMS WITH COATINGS

The biggest single problem with conductive coatings is their shielding effectiveness after extended high temperature and humidity exposure.

Significantly, if cost can be justified, only zinc-arc type coatings provide extended shielding after long-term environmental exposure.

The usual material used in foil-lined walls is aluminum about 0.1 ml thick. Again, as is the case with spray paints, holes or discontinuities in wall coverage are to be avoided. Specifically, holes or slots larger the 10 to 15 mm are to be avoided. Non-bonded overlapped joints about 100 mm thick provide sufficient capacitive coupling to prevent radiated leakages at seams. Also, foil and other metal rooms require a safety ground attached between the shield and the building ground structure. Table 4 lists attenuation values for conductive foil rooms.

PROBLEMS TO CONSIDER DURING COATING

Paint formulation can effect conductivity by a factor of 3.

Temperature during curing and drying:
Paint in warm dry conditions
No forced drying

Sealing with paint will prevent pealing and flaking, but cannot currently protect against aging.

Stand Alone Shielded Enclosures

The three most common base materials used for stand alone shielded enclosures are copper, aluminum, and steel. Since the slight differences in each of the material's conductivity and permeability have only minimal effect on the amount of shielding provided, the primary determining factor when solid rooms are required is cost. Steel is significantly cheaper then the other materials and is most often specified.

Table 4 - Conductive Foil Rooms

Field Type	Freq. (MHz)	Atten. (dB)
H Field	0.01	28
	0.1	50
	1.0	55
E Field	1	113
	10	97
	100	105
Plane Wave	400	90
	1000	72
	10000	66

As shown in Table 5 and Figure 11, there are also three types of construction for shielded enclosures that are considered "stand alone". Stand alone means they are self supporting, usually assembled inside an existing room, and normally on a permanent basis. The three methods of construction are single shield, double shielded not electrically isolated, and double shielded electrically isolated. The figure below compares relative attenuation characteristics of each type of room at 1 GHZ for screen mesh construction.

Table 5 - Attenuation Comparison of Construction Types

E Field and Plane Wave Atten.

Type	60	90	120
Isolated	-----------------------------------		
Non-Isolated	-------------------		
Single	--------		

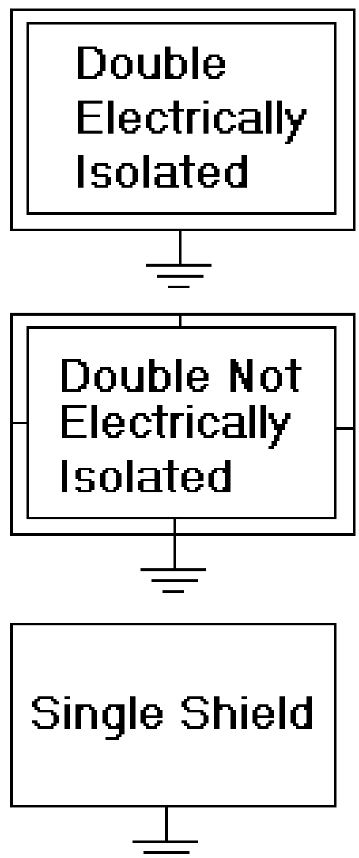

Figure 11 - Enclosure Types

Copper mesh enclosures are basically stand alone shielded enclosures that consist of wire covering a wooden frame. Unless magnetic field problems exist, or unless a vault or protected access solid wall type structure is preferred, this form of enclosure usually provides sufficient attenuation for most applications. However, if this type of structure is considered, a safe approach is to first have the facility and potential processing equipment scan tested so an accurate evaluation of needed attenuation is available.

Copper mesh rooms are easier then metal rooms to install, are considerably cheaper, and are not considered "permanent" structures in that they can be taken apart much easier then metal rooms. Table 6, from Lindgren, provides E-field and H-field attenuation characteristics for a 22 x 22 -.015 copper screen room.

For maximum shielding, the use of galvanized steel walls is recommended. Individual panels are bolted, welded, or otherwise solidly attached to each other in order to prevent or reduce RF leakage at joints and corners. In general, if the room is not well sealed at corners and joints using copper wool, copper tape, or welding, shielding effectiveness is reduced about 30 dB. Also, steel rooms have a tendency to loosen up with age and require periodic re-work. Table 7, also from the Lindgren enclosure catalog, compares each of the room types for 24 gauge galvanized steel constructed shielded enclosures.

Table 6 II - Attenuation Comparison for Copper Screen

Room Type	15 KHz H-Field	1 GHz E-Field
Isolated	.-------------- 68 dB	.------------ 120 dB
Non-Isolated	.---------- 48 dB	.--------- 90 dB
Single	.- 6 dB	.------ 60 dB

Table 7 - Attenuation Comparison for Steel

Room Type	15 KHz H-Field	1 GHz E-Field
Isolated	.---------- 84 dB	.------------ 120 dB
Non-Isolated	.------- 68 dB	.---------- 100 dB
Single	.----- 48 dB	.--------- 90 dB

Regarding steel rooms, there are several acceptable techniques to penetrate shields so shielding capabilities will not be degraded. One of the primary concerns with room penetrations, as well as with metal rooms in general, the necessity to provide good low impedance bonds at metal to metal interfaces, joints, bolts, wave guides, etc. Shown in Figures 12 and 13 are methods of electrical bonding for several connections as recommended in AFDH 1-4[3].

Methods and Requirements for Attenuation Testing

There are three primary standards in the U.S. identifying shielded enclosure attenuation requirements, equipment, and test procedures. MIL STD 285, Attenuation Measurements for Enclosures, Electromagnetic Shielding, for Electronic Test Purposes, Methods of, dated 25 June 1956 is first widely accepted test standard still in use today. This document was derived from an earlier document, MIL-S-4957A, which was written as a procurement requirement for wire mesh screen rooms use for research testing. NSA 65-6, National Security Agency Specification for R.F. Shielded Enclosures for Communications Equipment, General Specification dated 30 October 1964, and NSA 73-2A, National Security Agency for Foil RF Shielded Enclosures, dated 15 November, 1972, are both widely specified currently in procurement's for RF Shielded Enclosures. These requirements documents list high levels of attenuation, and also were originally intended primarily for test labs or highly classified equipment processing areas. Figures 14 and 15 show the attenuation limits of 65-6 and 73-2A. Note that the attenuation requirements for 65-6 extend to several frequencies in the plane wave range up to 10 GHz.

[3] *AFSC Design Handbook DH 1-4, Electromagnetic Compatibility, U.S. Airforce, 5 January 1975 with Revisions.*

The test methods called out in MIL STD 285 are intended more for screen mesh rooms rather then metal wall constructed rooms. Primarily, measurements are specified for antenna placement in the middle of the shielded wall. While perhaps acceptable for a mesh room, this type of antenna positioning would provide relatively little information for a solid wall constructed room. A mid-wall type of test is especially unacceptable is situations where multiple seams or wall joints are present in the room wall. This is the normal condition for shielded rooms.

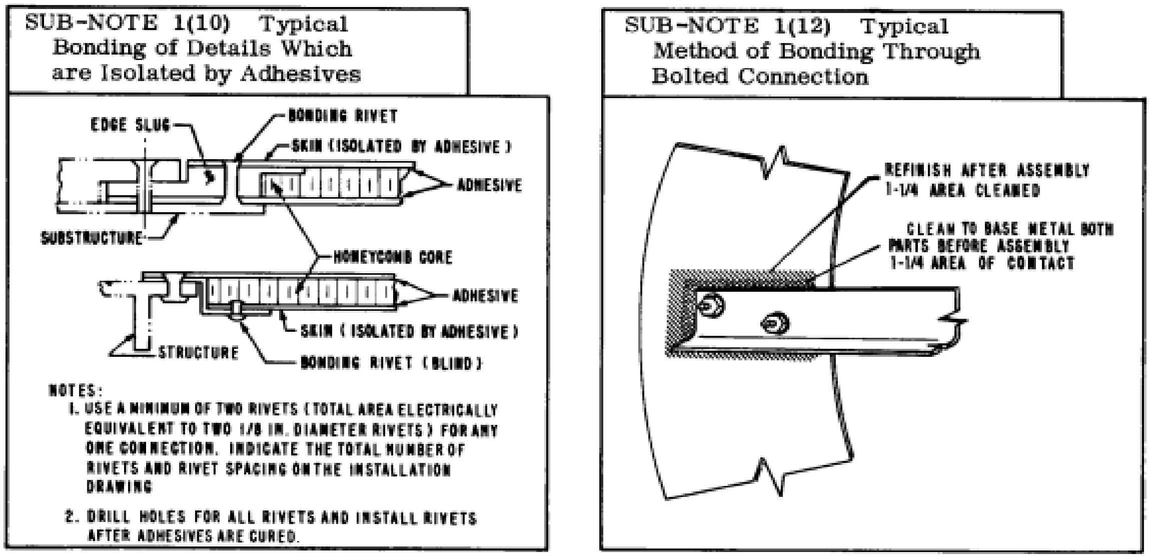

Figure 12 - Methods of Bonding (AFDH 1-4)

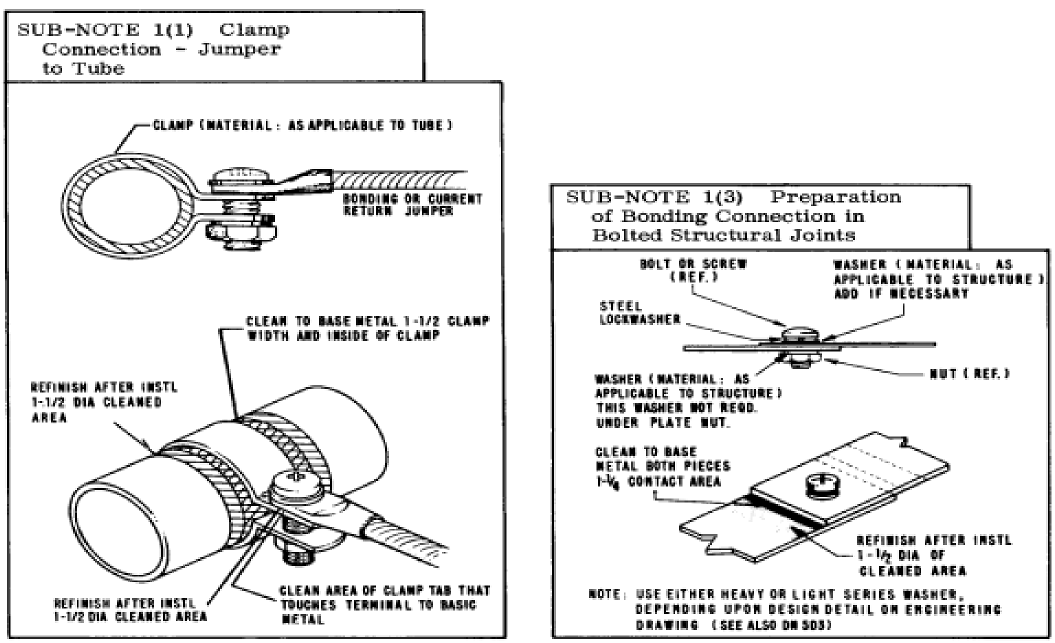

Figure 13 - Methods of Bonding (AFDH 1-4)

NSA 65-6 states that "Leakage checks must be made all around the door frame, through accessible joints, around the filters and all around the air ducts. In addition, the magnitude and location of the maximum signal level emanating from the enclosure should be found by moving the antennas to at least four locations, preferably on different walls." Depending on interpretation, the number of test points to be measured could be the total number of seams plus penetrations, or only the number of penetrations and 1 point on each wall. Room installers normally test every seam for leakage, even on large rooms, and then use a seam in the middle of the wall for their formal measurement point.

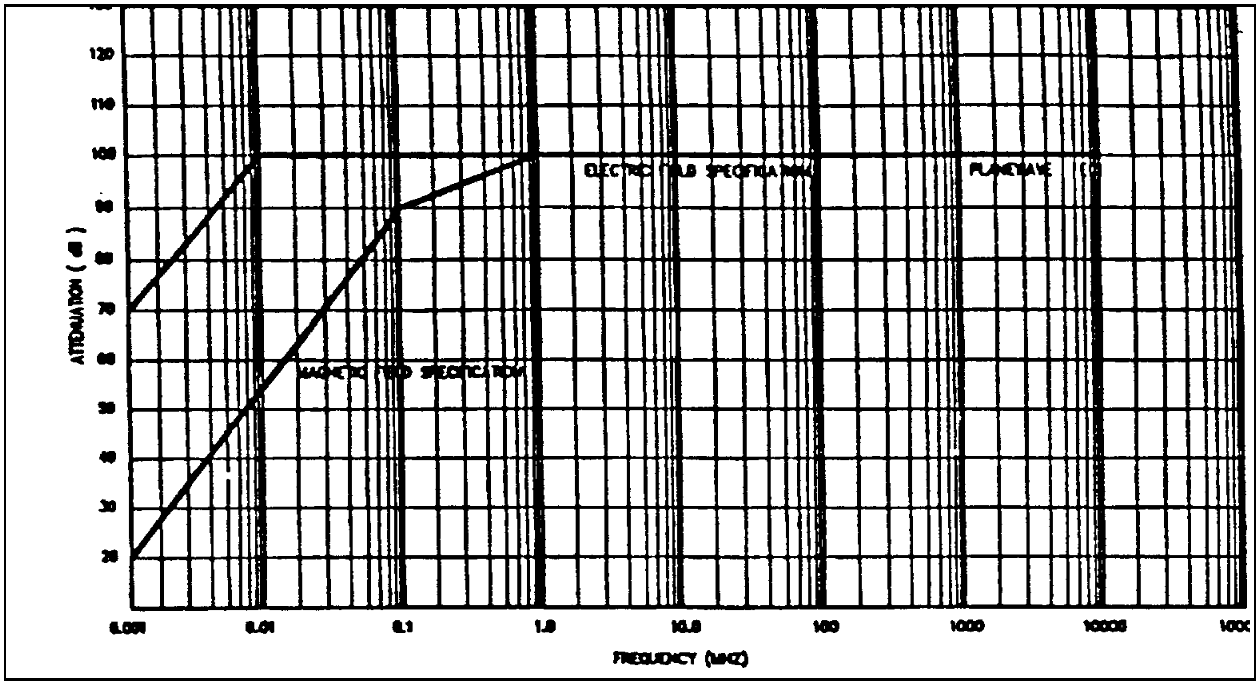

Figure 14 - NSA 73-2A Limits

Equipment test set-ups are slightly different between 285 and the two NSA documents. Equipment setups are shown in Figures 16 through Figure 19. MIL-STD 285 requires the transmitting antenna be located outside the shield and the receiving antenna inside the enclosure. NSA 65-6 and 73-2A require the transmitter be located inside the enclosure for all but planewaves. The main drawback with locating the transmitter inside room is the creation of standing waves reflecting off walls inside the room. Reflections can be reduced by incorporating absorptive material on the inside of the walls.

The methods used for shielded room testing should also be used to perform environmental attenuation testing if desired prior to specifying a shielded enclosure be installed. The NSA location for the transmitting antenna (inside) is used while the 285 method of testing in the middle of the wall is the area tested. Floor and ceiling measurements are no problem since antennas on tripods can be directed towards any position. Also, if testing a facility for environmental attenuation, it is most helpful if the two people performing the test use a pair of small transceivers to communicate with each other prior to each measurement. Since testing for E-field and H-field requires access to one meter on both sides of a wall, it is not always possible to know where the opposite antenna is or when a measurement will take place.

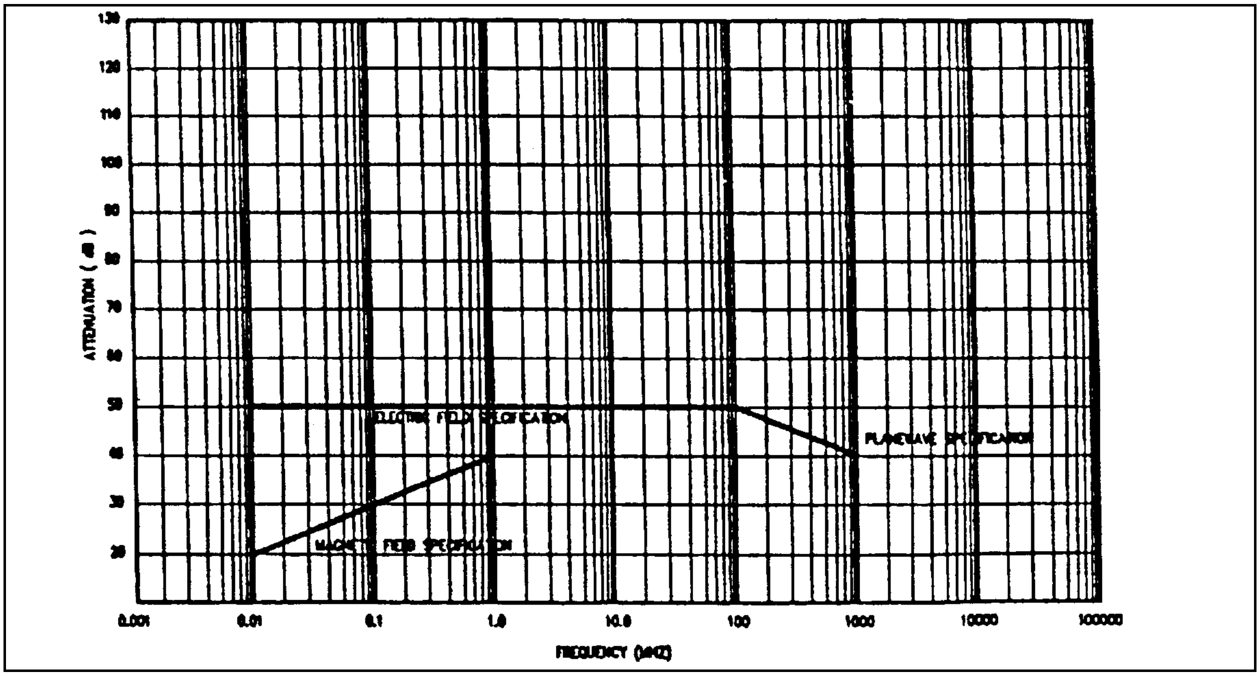

Figure 15 - NSA 65-6 Limits

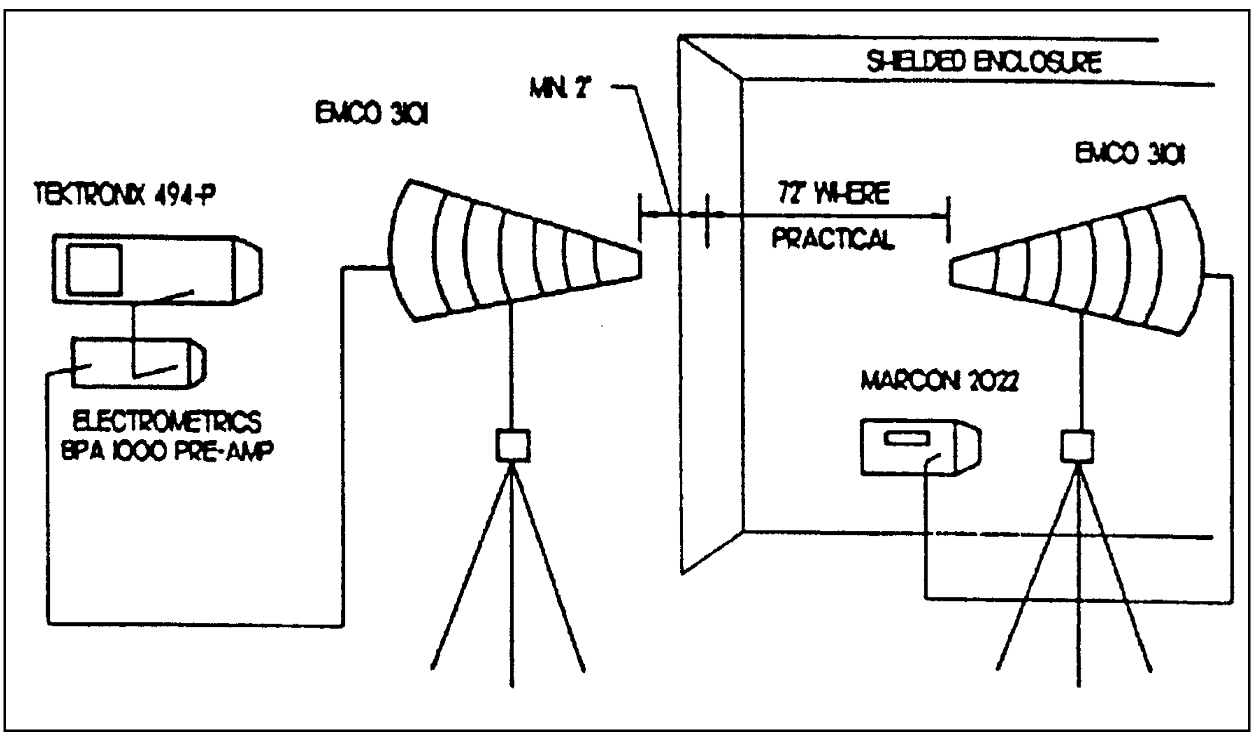

Figure 16 - NSA 65-6 Planewave Test Set-up

Planewave measurements are slightly easier for a facility using the 285 technique, but a transceiver for communicating is still helpful. Insure that transmitting occurs in short bursts so interference to other organizations is kept to a minimum. Position the transmit antenna at ground

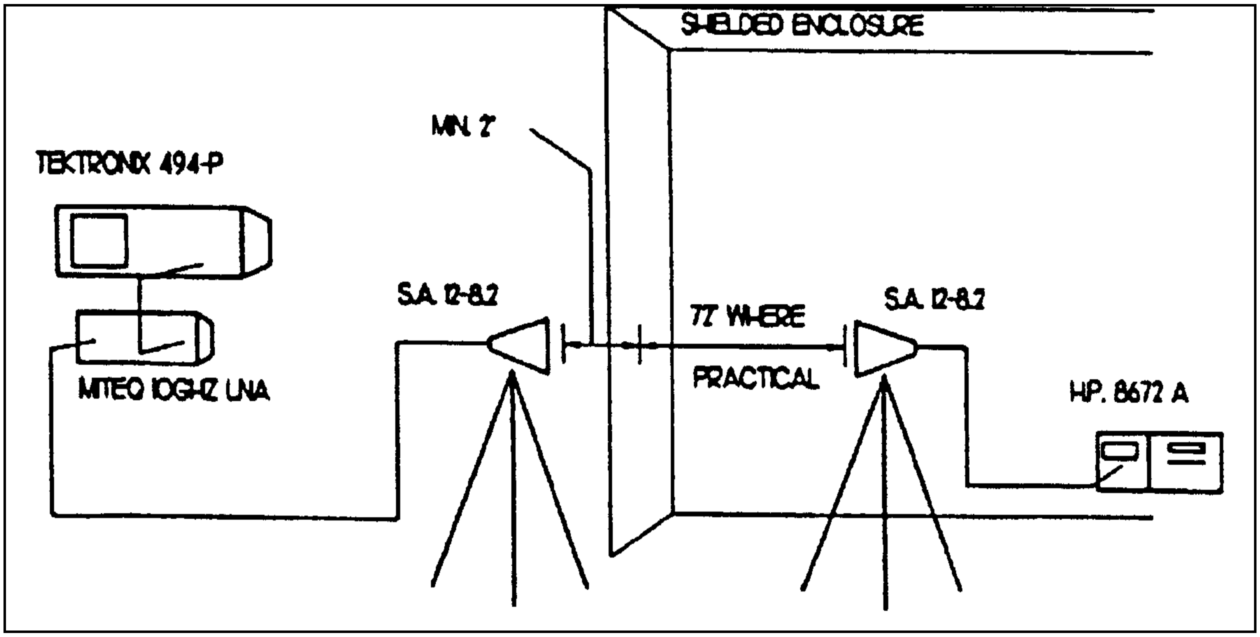

Figure 17 - MIL-STD 285 E-Field Test Set-up

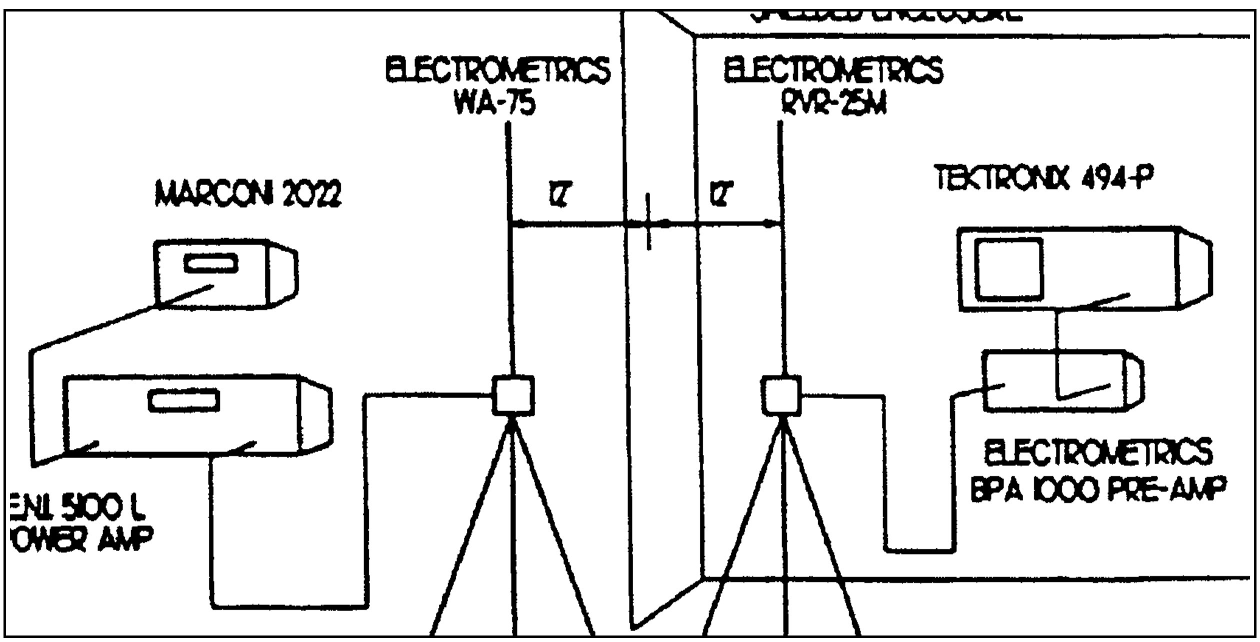

Figure 18 - MIL-STD 285 E-Field Test Set-up

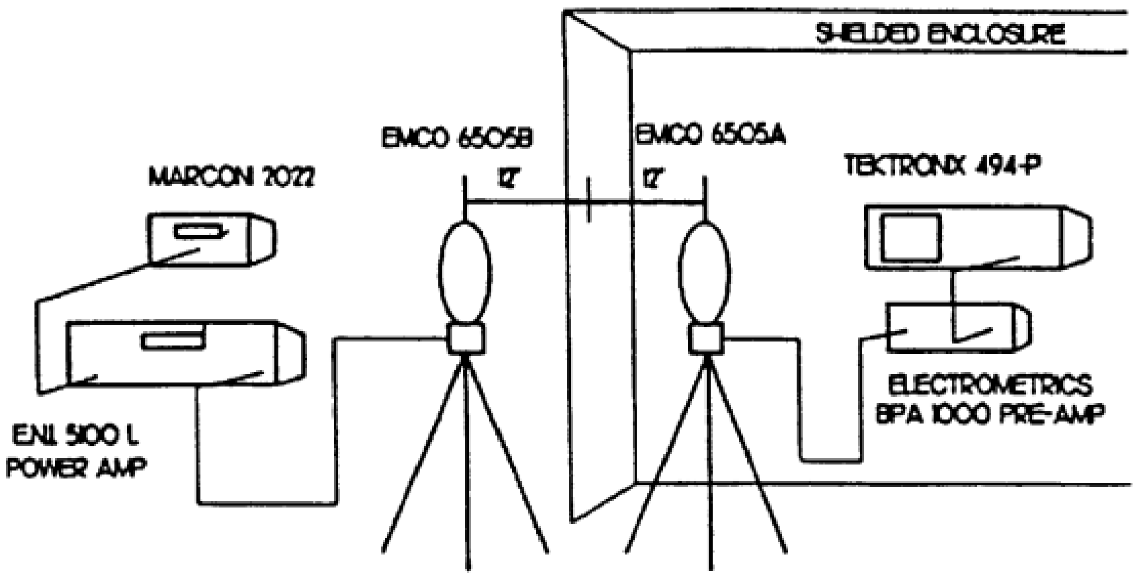

Figure 19 - MIL-STD 285 H Field Test Set-up

level at a distance from the building equal the height of the building. Direct the antenna to the center of the area to be tested. One antenna location should be adequate to cover a 40' by 40' wall. Increase the power to the transmitting antenna until the signal is detected at the receive antenna. After testing, move the transmit antenna back to a distance equal to the distance the receive antenna was located from the internal wall. Place the receive antenna outside at least 1 meter from the outside wall and perform a second dynamic range test. The resultant loss is the path factor loss over open ground at the test location will be used as the baseline for determining environmental loss or shielding loss for the facility. This method is also used for testing at microwave frequencies and on facilities that are located above ground level.

Non-Radiated Problems and Their Solutions

Thus far, this document has concentrated on TEMPEST problems related to radiated emissions and spent little effort on identifying and correcting conducted TEMPEST problems. Relating back to earlier discussions in proposal paper, uneven grounds between different building locations are a primary cause of TEMPEST problems. Using fiber optics between the various equipments is a common technique represents one way of isolating the grounds at each equipment. Another technique often overlooked is the use of isolation transformers.

Isolation Transformers

Isolation transformers are often used to protect high gain circuits, or to prevent ground paths in instrumentation. All transformers isolate circuits electrically to some degree, while simultaneously coupling circuit signals through magnetic induction. The electrical energy is transformed at the same frequency, but usually at a different voltage or current level. As frequency increases, capacitance between the inductor windings tends to shunt higher frequency components, providing a practical limit to the passband of the device.

Shielding at the instrumentation level or rack level is difficult and often ineffective when ground loops between connected equipment are present. The case or rack acts as an outer shield for internal processing, while serving as the zero signal reference for system output signals. An isolation transformer can be used to control shield currents, and to break up the mutual capacitances between internal instrumentation and the unknown power ground.

During the time power is being transferred between windings, noise potentials between the primary circuits and ground is similarly coupled to the secondary through both capacitive and resistive paths. As previously indicated, the noise appears as common mode, differential mode, and also radiated via the transformer windings. Since common mode noise is referenced to the power system ground, the most obvious method of eliminating this noise is by grounding the transformer center tap to the system ground through the lowest impedance path possible.

The key to maximum noise reduction on powerlines for differential mode applications is to differentiate between power and TEMPEST signal noise, and then reduce the signal noise. Basically, the objective is to transfer the power required by the load at the fundamental power frequency, and to eliminate all higher frequencies. Sub-harmonic frequencies of the primary powerline frequency (such as those relating to a 50 bps teletype) are attenuated or eliminated by operating the transformer at a relatively high flux density. Above the fundamental frequency of the transformer, noise is reduced by introducing as much leakage inductance as possible consistent with good power transfer to the secondary. Most well designed isolation transformers are intended as noise reduction devices, and are designed to operate in the manner described. Therefore, especially when large high current processing systems are involved, isolation transformers rather then powerline filters are sometimes all that is required to eliminate conducted noise. Isolation transformers used with a screen room is shown in Figure 20. Figure 20 also shows the application of a powerline room filter.

Filters

Filtering powerlines to secure processing areas, especially shielded enclosures, is perhaps one of the most misunderstood applications of filters that commonly takes place. Current regulations dictate that powerline filters are not required when average peak power consumption is 100 KVA. While this appears a contradiction of terms, the intent is to prevent unnecessary filtering on facilities located in the continental US (CONUS). To actually determine is power consumption inside a facility meets this criteria, a complete accounting of normal operating times, average power ratings for all equipment, plus information on facility heating and air conditioning would be necessary. The determination could cost more than the installation of filters. The current trend by GAO auditors at this writing is to blanket reject any filtering for CONUS facilities, regardless of vulnerability, so long as they are located in a controlled access area. This paper addresses the proper application and use of powerline filters, regardless of their actual need.

Two objectives are addressed by powerline filtering. For rooms used as test cells, the objective is to reduce outside noise such that signals within the chamber will be easier to detect. For secure areas, the objective is to reduce noise originating internally such that it can not be detected externally.

Since it is desirable to reduce both common mode and differential mode between the powerlines, and since, for safety reasons, the room must have a safety ground, the best practice is to isolate the entire room from facility ground using an isolation transformer and a local ground rod, and then to provide both common mode and differential mode filtering to the powerlines at the room walls. The isolation transformer can be configured to provide two separate phases of power with a center tapped neutral, or just a single secondary depending on equipment requirements within the room. The biggest problem is how the room filters are configured.

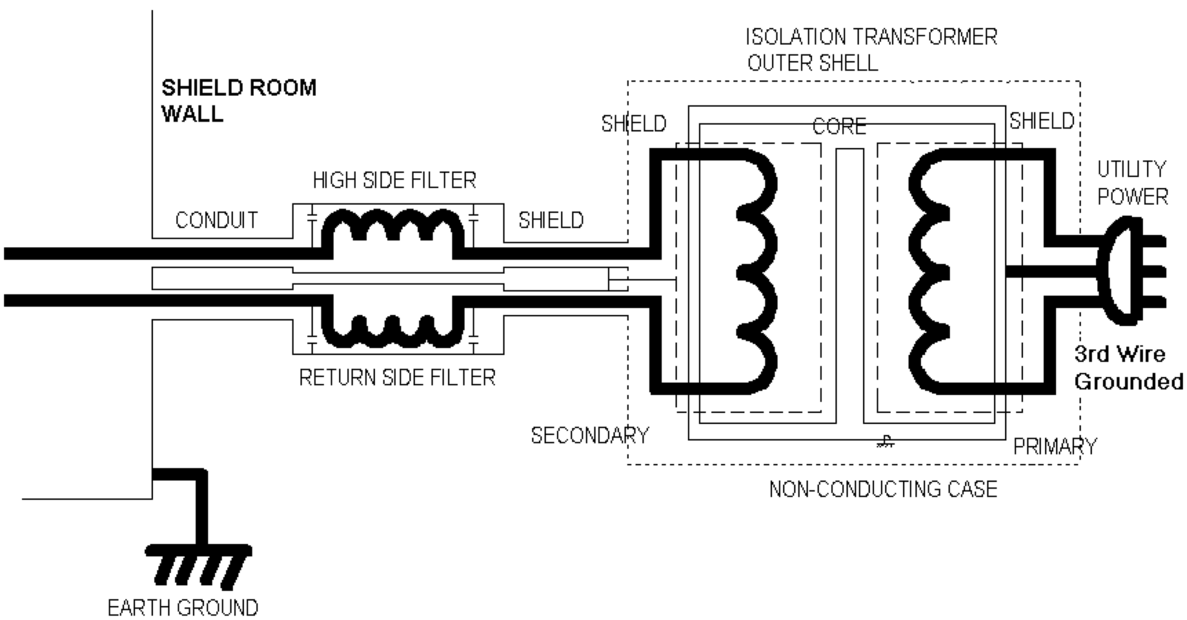

Figure 20 - Room Application of Isolation Transformer

Screen Room filters are configured as pi-type filters. Capacitors are grounded through a connection to case at the room wall. Adequate filtering normally requires both common mode and differential mode filtering, with the differential mode capacitor located prior to the inductor in each filter, inside to outside for maximum internal security attenuation applications. Therefore, achieving the proper powerline filter configuration for both common mode and differential mode protection will require control of the third wire ground return at all internal plugs by grounding at only one point near the filters, disabling of the internally facing capacitor within the room filter, and finally by placing a properly selected powerline capacitor across the internal high and return wires.

Another problem is how to specify the attenuation characteristics of the powerline filter to be used. It should be obvious by now that the manufacturers listed attenuation characteristics are not easily applied to the potential TEMPEST threat. This is especially true if the equipment being located within the secure screen room is only FCC approved and has no information related to its TEMPEST powerline conducted limits. A good rule of thumb is to calculate or measure the attenuation characteristics of the intended filter at the correct source and load impedance at a frequency of about 100 KHz. If subtracting the filter attenuation and the isolation transformer attenuation from the frequency component of the lowest data rate signal at the same frequency exceeds the proper TEMPEST limit for the frequency selected, the potential for a TEMPEST problem is realistic. In this case, additional filtering or direct TEMPEST suppression of conducted signals in the processing equipment will be necessary.

Acquisition Phases

Thus far we have discussed both the analysis process, and the available techniques used to provide security for processing and Red/Black communications facilities. While many facilities evolve into secure facilities after they have been built, many others are planned for security applications prior to their being built. Since the techniques previously discussed can be applied to existing buildings to establish relatively small secure areas, what happens when larger areas are needed and planned when the building is designed?

If a new secure processing facility is planned, the major concern is knowing at what stage of the facility acquisition and design process are various security issues and analysis most efficiently applied. Security considerations effect both major system acquisitions and facility acquisitions. From the security perspective, the contractor needs to establish and follow early in the cycle a security program for the facility in order to economically achieve the systems overall security program objectives when the building is completed. If, as is normally the case, the system to be installed consists of COMSEC equipment, Red and Black processing equipment, and interface communications equipment, certain security related issues must be evaluated during each individual phase of the program. An entire facility is much too expensive to dismantle because of a security issue once it has been completed. Therefore, specific security issues must be considered at each stage of the design and building process.

Concept Exploration Phase

The Concept Exploration Phase focuses on the exploration of a series of potential responses to a stated military threat. Its main intent is to conceptualize the most appropriate response to the threat given current or the projected availability of appropriate "hard" and "soft" technologies. In regards to a secure facility design program, the correct response relates to facility hardening, shielding and grounding control, power system design, and system design.

To accomplish the building design within the overriding security requirements, the following relevant security issues need to be addressed during the Concept Exploration Phase.

Equipment:

Equipment Requirements -TEMPEST/non-TEMPEST (including NONSTOP)
Endorsed TEMPEST Products or direct DoD control
Interface Communications Requirements
    Fiber Optic, hardwired, voice/data, computer network, COMSEC (type 1 or 2), trusted computer interface access

Facilities:

Space limitations
Level of information security at desired location
Perimeter Construction Criteria
Intrusion Detection
Zone Protection, Site Survey Requirements
Room Protection - acoustic and/or emission
SCIF/Vault
  Continuous/noncontinuous
  Class requirements
  Access Control/Physical Security
    Alarm Requirements
    SIGINT (threat environment)
  Power/Ground System
  Emission requirements and options
  Screen room necessity

Costs:

People and facilities required for development
Includes determining TEMPEST Security Index
Long term maintenance and reliability requirements

Demonstration and Validation Phase

The Demonstration and Validation Phase of the acquisition process is concerned with the initial design and testing of the equipments/facilities selected earlier in the previous phase. Related to secure facility construction, the primary emphasis in this phase is the translation of specific qualitative security requirements into quantitative specifications for the later use in the building of the desired system.

Consistent with this phase of the acquisition cycle, the following relevant security issues will be considered.

Equipment:

Specification Requirements
Hardware to be Protected
COMSEC, TEMPEST, Red/Black, LAN's, Node vs Box level security,

Facility/People:

Alarm
Access control
HUMINT
Intrusion Detection System (IDS)
Storage

Facility/Emission control - level of protection

Metal enclosure
Life cycle cost, effectiveness, and testing
Screen mesh
Life cycle cost, effectiveness, and testing
Conductive Coating
Life cycle cost, effectiveness, and testing
Power and Ground system protection
Ground plane mesh or welded rebar

Full Scale Development Phase

In this phase of the acquisition process, the facility specified earlier is built consistent with an updated analysis of the threat for which the equipment or system is to be protected against. Of major concern at this stage is the final design of a facility that can be built, and in accordance with the stated security requirements. The list below describes relevant security considerations to be considered during the full scale development phase of the acquisition program.

Hardware:

COMSEC
TSRD Documentation (security requirements of equipment spec., etc.)
TEMPEST Documentation (system test requirements)

Facility:

QA, Maintainability, Human Factors
MTTR (time between recertification)
Verification Documents (DIAM requirements or shielding effectiveness test)

Construction and Installation Phase

The Construction Phase of the acquisition process is focussed on the actual building of the facility or SCIF. From a security perspective, the production and deployment phase includes the proper preparation of the site and/or facility which will be used. Relevant security factors to be considered during the production and deployment phase of the acquisition program include the following.

Hardware:

Maintenance manuals
Special requirements for TEMPEST Facility:

TEMPEST Field/Room Attenuation Testing
Builders warranty
Methods of defeating security protection techniques

Real Facilities

Proper engineering techniques regarding equipment installation must also be applied to prevent inadvertent signal coupling, such as those suggested in NACSEM 5203 and various EMC documents. In addition, special requirements and techniques are applicable when acoustic security in specified. Dealing with the typical radiated emission issue first and referring back to Figure 1 at the beginning of this article, the figure shows a typical two room TEMPEST secure control zone with a super computer being accessed by a local area network located in the SCIF. Notice that the interface from the computer to the outside world used only a COMSEC box. Real facilities might also include access to both telephone lines and a telemetry link. However, when an antenna is associated with the secure processing area, as previously discussed, grounds and potential ground loops become extremely critical.

In many cases, an isolation transformer is used to control ground loops at either the room or the system level. An isolated shielded room was shown in Figure 20. Also, in many cases, an additional unsecured (BLACK) processing area is interfaced to the secure processing area through appropriate RED/BLACK isolation, and with a transceiver or modem to receive and transmit the Black information located entirely within the BLACK area. Regardless of the final grounding configuration, and to assure that grounding techniques include zero-volt signal reference(s), safety, and security, the facility grounding system must be considered from the beginning of the construction program, and progressively implemented along with the rest of the facility design.

Figure 21 shows a typical facility consisting of a RED and BLACK exclusion area with classified data only connected and interfaced through a KG 84 COMSEC box. Notice the important design features described on the figure. Again notice the features described for this application.

For RF/acoustic facility design, requirements apply to an assembled room, including doors, panels, joiners, and all penetrations of the secure perimeter. Sound transmission performance requires that the NIC of the complete room meets DIAM 50-3. This usually means component STC of 50 for NIC 45 (Sound Group 3) performance. Protection and acoustic attenuation to meet this requirement is usually achieved in a shielded room using internal panels and sometimes room isolation supports from the structural floor.

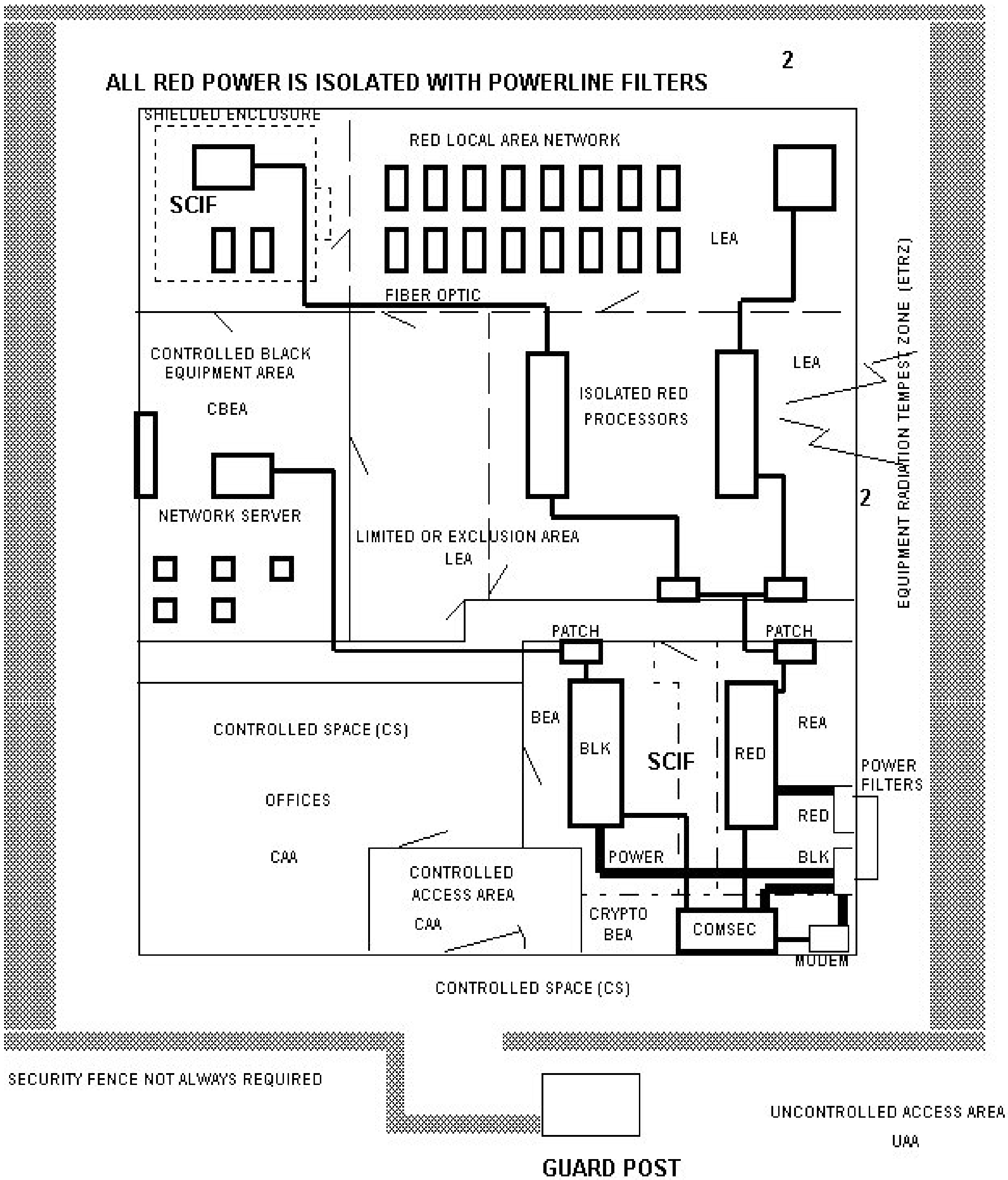

Figure 21 - Typical Large Facility

Conclusions

This paper has described suggested methods of evaluation for the needs of secure facilities. Significant misinformation currently exists related to the proper techniques for evaluations and how to assess the attenuation needs of equipment processing secure information. The primary emphasis has been placed on cost effectiveness in terms of what could be used and what it will ultimately be required to meet the desired objectives of a facility security program. The "bottom line" for determining vulnerability after construction is to test when unsure, it could save considerable grief and money for the program.