TEMPEST Low Emission Controlled Design

Dr. Bruce C. Gabrielson, NCE

Brucegabrielson@yahoo.com

Last Updated: 2002

Based on the Texts:

TEMPEST, A Description and Approach
Hardwire and Cable Design in Secure Communications
TEMPEST Hardware Design
TEMPEST Systems Engineering & Program Management
INFOSEC Engineering

Design Course Outline

This course is divided into four parts: Program Management, Theory, Mechanical/Electrical Design, and Facilities.

The H/W Design section is divided as:

1. Mechanical Design
2. Wires/Connectors
3. Transformers
4. Power Supplies
5. Filters
6. Line Drivers/Receivers
7. Facilities/Platforms
8. Trouble Shooting

H/W DESIGN COURSE OVERVIEW

COMMUNICATIONS

Information | **Modulation** | **Propagation**

Mechanical Design

Boxes – Gaskets – Boards – Wires/Connectors

Electro-Mechanical Design

Transformers – Power Supplies - Filters

Internal Design

Line Drivers/Receivers - Logic

Systems – Power – Ground

Facilities – Rooms - Ships

Examples

Definitions

- 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.

Four Components of COMSEC

- 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.

Electronic Emissions

- All electrical devices generate emissions.
- Emissions can reveal the information being processed.
- Emissions couple to grounds, signal lines, power lines and other metallic items.
- Emission vulnerabilities of a device can only be determined through testing.

Emission Protection

- The intent of a secure environment is to reduce or prevent sensitive emissions from escaping the controlled area either through coupling paths or by radiating to the outside world.

Compromising Emanation

- Unintentional Data-Related Emanation (USDE) or intelligence bearing signals which, if properly intercepted and analyzed, disclose the classified information transmitted, received, or otherwise processed by any information processing equipment.

TEMPEST Definition

- TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations, conducted or radiated, on complete equipment.
- TEMPEST looks within the system noise in order to uncover meaningful information.

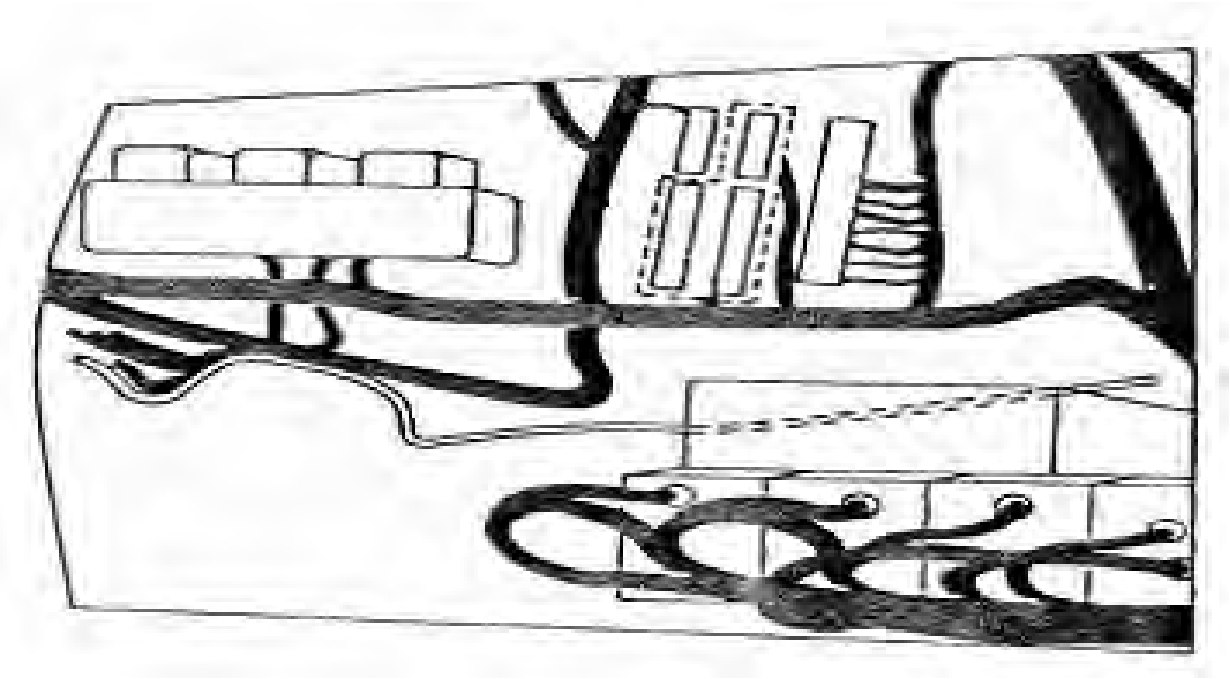
What is TEMPEST

- TEMPEST is the application of reverse communications theory to the design and test of complete equipment or systems which process and/or transmit secure information.

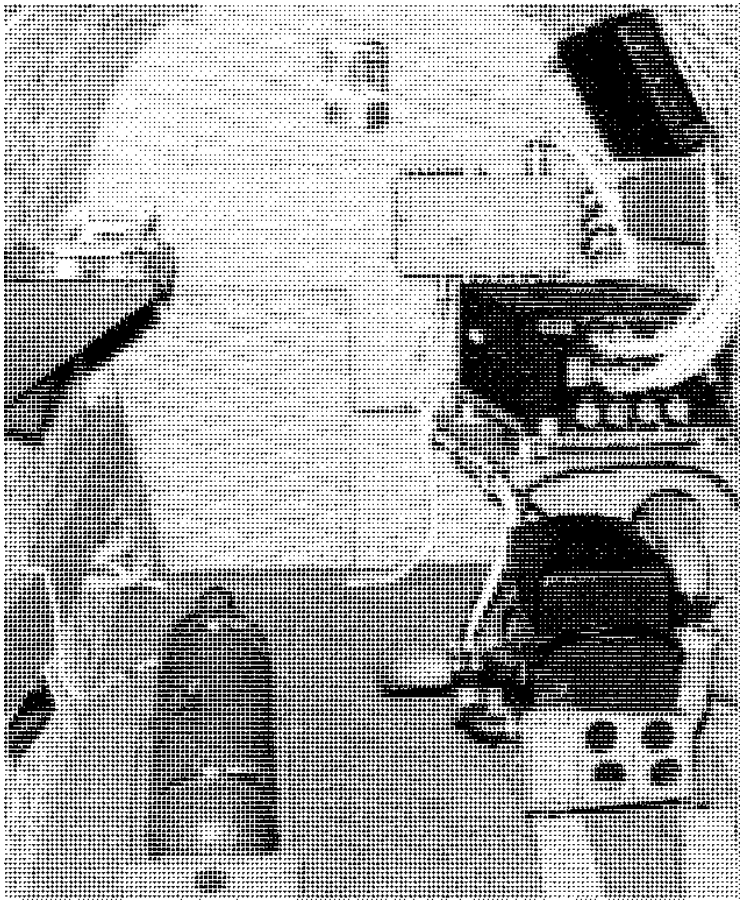
RED/BLACK Concept

- Electronic circuits/components/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.

Emission Protection Is Complicated

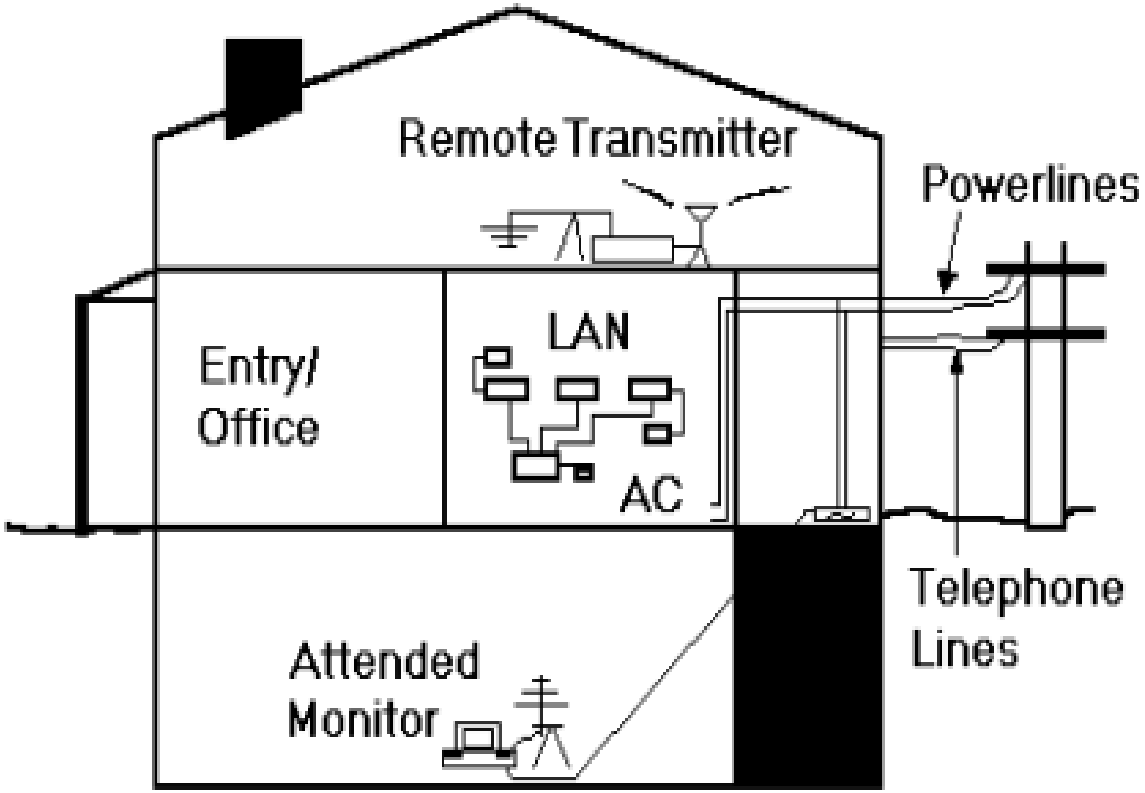


Aircraft Platforms



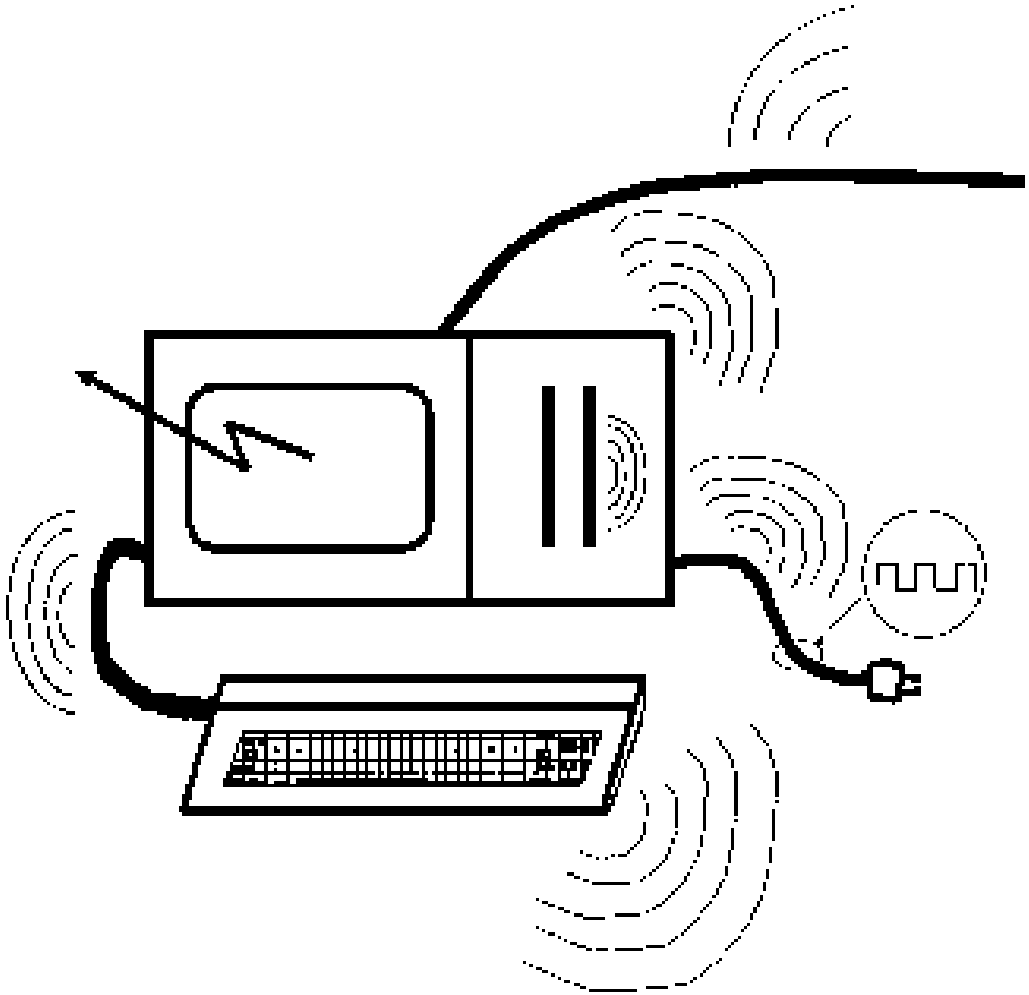
- Real platforms require significant emission controls be installed to protect against inadvertent loss of information.

Buildings



- Real threats exist in facilities as well as platforms.

Typical Threat Locations



TEMPEST 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”.

TEMPEST/EMI Comparisons

- 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 is concerned with communications.
- Measurement bandwidths, sensitivity levels and frequency requirements are incompatible.

Conducted Test Approaches

- TEMPEST and EMC conducted test approaches are different and the documentation cannot be combined.
  - EMC conducted testing deals with bulk current noise.
  - TEMPEST does not consider noise levels, but analyzes signal related voltage measurements on power and data lines.

Radiated Test Approaches

- Modulation has little meaning in EMI.
- EMI radiated measurements relate to bulk emitted energy.
- TEMPEST measurements look within the radiated emission noise for meaningful signals.

Classification Differences

- EMI/EMC design techniques and rational for their incorporation are unclassified.
- TEMPEST design techniques when combined with rational for their incorporation in a specific component are SECRET.
  - Schematics with no specific reason for a particular design are not classified.
  - Schematics are normally classified for COMSEC equipment.

Emphasis

- It is very difficult to design TEMPEST protection into a circuit after it id functioning.
- It is much easier to apply source suppression into the initial design
  - Design the circuit to meet TEMPEST
- TEMPEST protection is very difficult to implement at the Black Box level.

Industrial TEMPEST Program

- Voluntary program to encourage U.S. industry to offer COTS equipment to U.S. Government in a competitive marketplace.
- Established in 1975.
- Exposes the U.S. TEMPEST Program to wide audiences (public, media, foreign nations).

Countermeasures

- Action applied to inhibit the generation of compromising emanations.
  - Electronic Approaches
    - Source suppression
    - Shielded enclosure or building (containment)
    - Facility radiation zone
  - Cost Trade-off Considerations
    - Initial cost of protection (in-house or outside)
    - Cost of certification
    - Periodic re-evaluations

Part 1: Program Management

Dr. Bruce C. Gabrielson, NCE

Brucegabrielson@yahoo.com

Last Updated: 2002

Based on the Texts:

TEMPEST, A Description and Approach
Hardwire and Cable Design in Secure Communications
TEMPEST Hardware Design
TEMPEST Systems Engineering & Program Management
INFOSEC Engineering

TEMPEST & Low Emission History

- In 1831, Johann Gauss and Wilhelm Weber, invented a representation for the unit of magnetism in terms of mass, length and time.
  - This eventually led to the discovery of Kirchhoff's circuit laws: two equalities that deal with the conservation of charge and energy in electrical circuits.
  - Gauss' Law for relating the distribution of electric charge to the resulting electric field was published in 1867.

Electromagnetic Radiation

- Electromagnetic Radiation (ER) is produced by moving charges.
  - ER is associated with Electromagnetic (EM) fields that are far enough away from the moving charges that produced them, that absorption of the EM radiation no longer affects the behavior of these moving charges.

Emissions Contain Information

- Discovered in 1918 by Herbert Yardley while developing methods of exploiting telephones and transmitters for the U.S. Army.
- First requirements document (NAG-1A/TSEC was released in 1960.
  - Radiation Requirements for Cryptographic Equipment

The First 25 Years

- TEMPEST existence closely held.
- Priority to not loose classified information by TEMPEST techniques.
- Program based on vulnerability existence
  - Threat data scarce.
- Protection achieved by equipment suppression and facility countermeasures.
- Problem limited to crypto and telecommunications equipment.

Need for Change - 1983

- Cost of TEMPEST program escalates.
- TEMPEST “atrocities” begin to occur.
- More real threat data emerges.
- General Stilwell, DUSD(P), asks TEMPEST community to review national TEMPEST policy in light of apparent minimal threat in the United States.

Extension of National Policy

- In January 1984, two documents were released that basically changed the scope and direction of TEMPEST.
  - NACSI 5004
    - TEMPEST Countermeasures for Facilities Within the United States
  - NACSI 5005
    - TEMPEST Countermeasures for Facilities Outside the United States

High Level Attention To TEMPEST Program

- In 1986, Stilwell Commission Report States:
  - “TEMPEST costs are estimated to run into the hundreds of millions of dollars annually.”
- President’s report to Congress indicates TEMPEST costs are excessive.
- Senate Select Committee on Intelligence reports on threat.
- GAO audit of DoD TEMPEST Program negative.

GAO Audit Conclusions June 1986

- NACSI'S 5004/5005 not being implemented.
- Evaluations not being performed before countermeasures applied.
- Lack of central control of TEMPEST program.
- Training for TEMPEST Countermeasures application needed.
- Conclusion - Issue a new policy.

New National Policy October 1988

- NTISSP 300
  - National Policy on Control of Compromising Emanations
- NTISSI 7000
  - TEMPEST Countermeasures for Facilities

Instructions/Advisories

- National Telecommunications and Automated Information Systems Security (NTISS).
- NTISSI
  - Replaced old NACSI instructions (must be implemented).
- NTISSAM
  - Replaced old NACSEM/SIM (advisory memo).

Policy Impacts - Industry

- Implements TEMPEST program evolution based on threats.
- Industry has voluntary support by the U.S. Government through the Industrial TEMPEST Program.
- Industry suffered through significant drop in sales.
- Per unit cost of equipment increased due to lower volume.

Policy Impacts - Government

- Certified TEMPEST Technical Authorities help eliminate atrocities.
- Many U.S. facilities need no or minimal TEMPEST countermeasures.
- TEMPEST protection outside U.S. have more emphasis.
- Cost of TEMPEST in U.S decreased significantly.

Highlights of NACSI'S

- Differentiated between threat in U.S. and overseas.
- Range of countermeasures offered.
- Allowed use of algorithm for TEMPEST countermeasure selection.
- Estimated threat is an integral part of the algorithm.

Highlights of NTISSI 7000

- Combines NACSI 5004 and NACSI 5505.
- Simplifies algorithms for TEMPEST countermeasure selection.
- Establishes six alternative TEMPEST countermeasures.
- Encourages Dept/Agency IG review of TEMPEST programs.

Highlights of NTISSP 300

- Countermeasures commensurate with threat.
- TEMPEST experts required to approve countermeasures by testing (Certified TEMPEST Technical Authority)
- NSA to provide threat data and training.
- NTISSC approves countermeasure recommendations and training guidelines.

TEMPEST Approved Devices

- TEMPEST limits apply to both commercial equipment used in classified applications and to COMSEC equipment that encrypt classified information.
- There are three layers of TEMPEST approved cryptographic devices.
  - Type I contains a controlled classified algorithm.
  - Type II contains an unclassified algorithm for use with unclassified but sensitive information.
  - Type III contains an unclassified algorithm registered with NIST for protecting unclassified sensitive or commercial information.

Important Documents

- NACSIM 5004, Tempest Countermeasures for Facilities Within the United States, January 1984 (S)
- NACSIM 5005, Tempest Countermeasures for Facilities Outside the United States, January 1985 (S)
- NSA 65-6, R.F. Shielded Enclosures for Communications Equipment, National Security Agency, October 30, 1964 (U)
- NSTISSAM 1-92, Compromising Emanations Laboratory Test Requirements, Electromagnetics, December 15, 1992 (C)

TEMPEST Industry, Program Management

Design Control, Testing, QA, and Corporate Security Needs.

Bruce Gabrielson, PhD

brucegabrielson@yahoo.com

Last Updated: 2002

Military TEMPEST

- Box accreditation not necessarily associated with the Endorsed TEMPEST Products Program (ETPP).
- COMSEC and other related requirements imposed due to overseas applications.
- Test requirements based on NSTISSAM requirements and may include KAG 30A/TSEC.
- Design control plans required.
- COTS often used with TEMPEST Zone Analysis.

Commercial COMSEC

- Accreditation of encryption type through the Commercial COMSEC Endorsement Program (CCEP).
- Requires specific NSA/Gov. sponsor.
- Intended for developing off-the-shelf Type I or Type II COMSEC equipment.
- Test requirements based on NACSIM 5100A and may include KAG 30A/TSEC.

CCEP Participation Criteria

- Potential vendor must not be under disqualifying foreign ownership or influence.
- Proposed product must provide a direct and obvious benefit to the cause of improving the communications security of the nation.
- Potential vendor must have a cleared facility and must demonstrate the ability to produce the product.

TEMPEST Advisory Group

- TAG was established to support the US Government's TEMPEST security objectives.
- TAG recommends threat-based TEMPEST countermeasures for approval, develops and recommends policies, instructions and guidelines for the control of CE, and provides a forum for the exchange of ideas.

TEMPEST Accreditation

- TEMPEST accreditation is the process by which a Certified TEMPEST Technical Authority (CTTA) authorizes a facility to process National Security Information.
- Accreditation follows a TEMPEST Countermeasures Review of the facility and the implementation of recommended countermeasures.

TEMPEST Endorsement Program Components

- Programs intended to authorize and accredit commercial evaluation facilities to conduct independent third party validations of security-enabled COTS product against accepted national and international criteria.
- Made up of:
  - Endorsed TEMPEST Products Program (ETPP)
  - Endorsed TEMPEST Test Services Program (ETTSP)
  - Zoned Equipment Program

Commercial TEMPEST Products

- Accreditation procedure through the ETPP.
- A no cost contract between Government and industry.
  - Used for units intended for Government sale through the ETPL and also for the development of new test equipment.
  - No guarantee of sale to Govt. purchasers.
- Test limits based on NSTISSAM 1-92.

Endorsed TEMPEST Products Program Steps

- Sequential steps required:
  - Pre-proposal MOU
  - Submit product specific proposal
  - Agency evaluation
  - Product management plan development
  - MOA issuance
  - Product development
  - Agency evaluation and endorsement on ETPL

ETPP Product Specific Proposal

- Product Specific Proposal consists of Product Assurance Survey, written Product Proposal, and a Company Profile.
  - Product Assurance Survey reviews the company's ability to develop and produce the intended product.
  - Written Product Proposal describes:
    - details of the proposed product
    - intended market
    - target development and production schedule
    - subcontractor involvement
    - general and applicable company information

Security Requirements for Access Control

- All TEMPEST product specific design and test information is considered COMSEC classified.
- Company must comply with:
  - DOD 5520.22, Industrial Security Manual for Safeguarding Classified Information
  - DOD 5220.22-S-1, COMSEC Supplement
  - DOD Form 254, Contract Security Classification Specification

Endorsed TEMPEST Test Service Program

- Intended to provide TEMPEST test services and product configuration services
- Test services include preparation and execution of test plans
- Product configuration services include:
  - TEMPEST Control Plan review
  - TEMPEST Test Plan review
  - Critical Features List preparation
  - Engineering change reviews and assessments

TEMPEST Program Management

- Managing a program with TEMPEST requirements is significantly different then traditional program management.
  - Significant security issues drive the design objectives.
  - The perspective of design engineers must shift to view technical issues differently.
  - Cost drivers and traditional scheduling are impacted significantly by these requirements.

Program Manager

- The key to effectively managing a successful program rests with the program manager.
- There are major differences between the functions of a commercial TEMPEST program manager and a defense contract program manager with TEMPEST requirements.
  - TEMPEST programs and schedules must not be considered “success” based.
  - Very few “if any” products meet TEMPEST on their first try.

Managing People Resources

- The lack of QUALIFIED (not necessarily certified) people within an organization is the major reason for the failure of equipment to meet TEMPEST.
  - A common management failure is to consider TEMEST as just another “ility” function and to staff accordingly.
  - It is a serious mistake to consider TEMPEST a design first and then fix where it fails issue.

Proposals and Programs

- Proposals and programs must consider TEMPEST as a design driver and plan accordingly.
- Good design engineers, including good EMC engineers, are NOT necessarily good TEMPEST engineers.
- Independent TEMPEST consultants are very difficult to find without a long lead time and sufficient funding.

TEMPEST Unique Knowledge

- To prevent significant cost impacts and delivery delays, managing programs with TEMPEST needs require:
  - A knowledge of the terminology including the difference between source suppression and containment.
  - A knowledge of the general capabilities of and rational for TEMPEST equipment requirements.
  - An understanding of security requirements related to TEMPEST information and programs.
  - An understanding of the limitations of and rational for outside TEMPEST consultants as well as internal staff.

System/Platform Level Node Approach

- The node approach is considered the most effective means of meeting TEMPEST requirements in large systems.
  - Node approach is containment on a large scale.
  - Groups of non-TEMPEST Red or Black equipment are placed in a shielded rack and then interconnected using shielded cables and connectors.
    - Rack doors must remain closed.

Box Level Approaches

- Source Suppression
  - Designing such that emissions from every internal circuit handling sensitive data are contained within the circuit loop.
- Containment
  - Totally enclosing the existing electronics package inside a metal housing with filters, waveguides, and cable shielding added for signal egress

Development Costs Source Suppression

- Source Suppression
  - Longer engineering development time/costs.
  - No guarantee that all problems can be solved without a mechanical redesign.
  - Resulting design can usually be manufactured in-house with minimal extra assembly time.
  - Detailed QA and configuration management required.

Development Costs Containment

- Shorter engineering development time/costs.
- Higher probability of early success.
- New housing design may change multiple times.
- Remanufacturing often costly.
- Higher risk if problems detected later.

TEMPEST Design Control Plans

- In addition to providing a “living” design plan of the product from beginning to end, the Control Plan insures a well thought out program of emanation control.
- Time and again accurate predictions of emanation problems have been identified and resolved through the plan before major delays are incurred.
  - It is a serious mistake to treat a TEMPEST Design Control Plan as “one more document to be submitted.”

Control Plan Specifics - Management

- Management Controls
  - Organizational capabilities, lines of authority, milestones, QA controls, background on TEMPEST design personnel.
    - TEMPEST engineer certification only applies to formal testing and has little to do with designing a box.
    - Good RF engineers can also be good TEMPEST engineers.
    - Many organizations use consultants for this section of the CP.

Certified Personnel Requirements

- Certified TEMPEST Engineer required for:
  - Accreditation testing at an endorsed service facility
  - Test plan writing
  - Maintaining service facility certification
- A minimum of 1 CTE is required to maintain NSA certified facility endorsement.

TEMPEST Professional Certification

- Program intended to certify test lab personnel who perform TEMPEST accreditation testing for products to be listed on the Government's Endorsed TEMPEST Products List.
  - Examination required for certification
  - Certification lasts for three years

Product Development Personnel

- A CTE is not required for:
  - TEMPEST design or redesign of equipment.
  - TEMPEST Design Control Plans or QA Plans.
  - DOD COMSEC testing or certification unless specifically stated in government contract.
  - Commercial COMSEC Endorsement Program TEMPEST certification unless specifically stated in MOA.

Product Verification Plan

- The PVP (QA Program Plan) is intended to assure production of ETPL products using reasonable commercial standards that can be verified as to integrity and consistency at each stage of manufacturing.
  - Details incoming inspection procedures, critical features checklist, in-process inspections, life-cycle support requirements, and final inspection procedures.

Quality Assurance Program

- Mandatory program for all ETPP manufacturers.
- QA plan specifically tailored for the product must be submitted along with a QA Test Report.
- No engineering change can be made without written approval by sponsor.
- Mandatory re-testing required for all changes.

Typical QA Concerns

- Torque on screws.
- Pre-cleaning of mechanical parts.
- Galvanic corrosion on dissimilar metals or gaskets.
- Wire breaks on shielded cables.
- Compression set in gaskets.
- Residue removal when gaskets replaces.
- Low tolerance electronic parts.

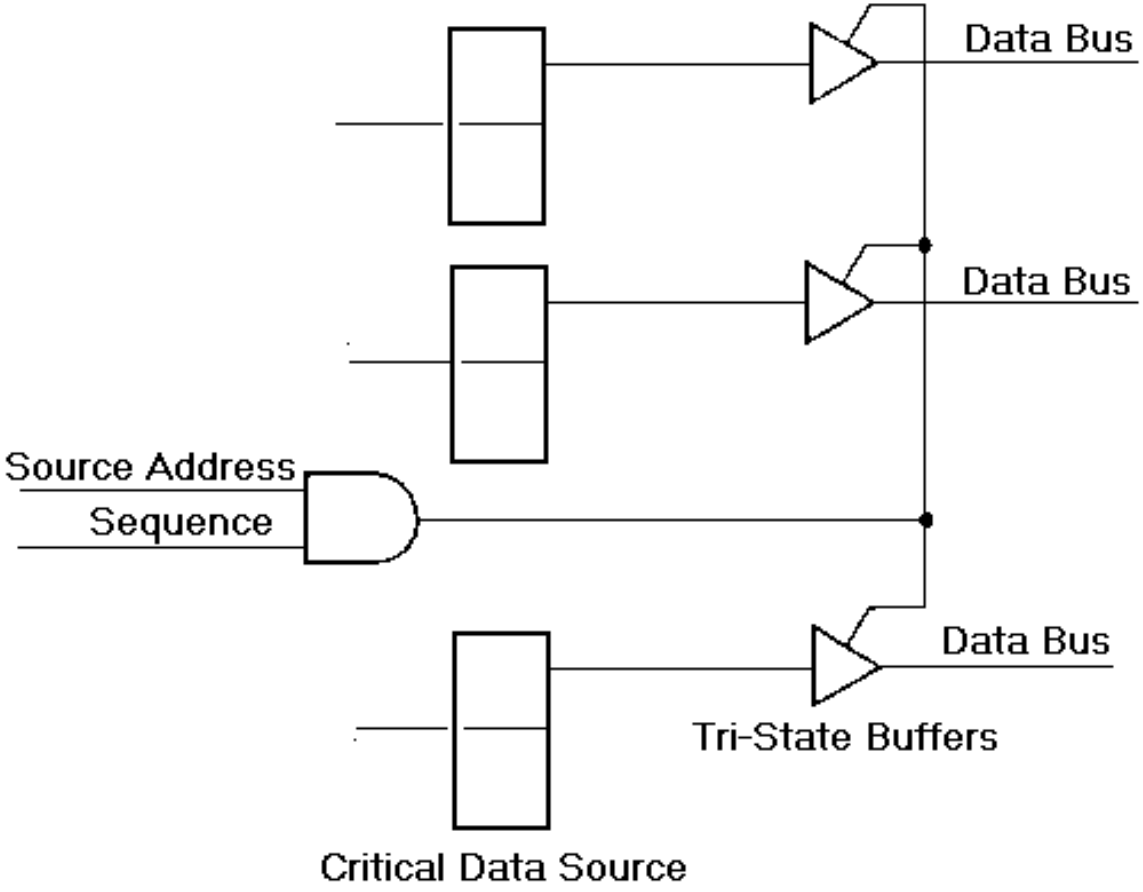
QA Provisions After ETPL Listing

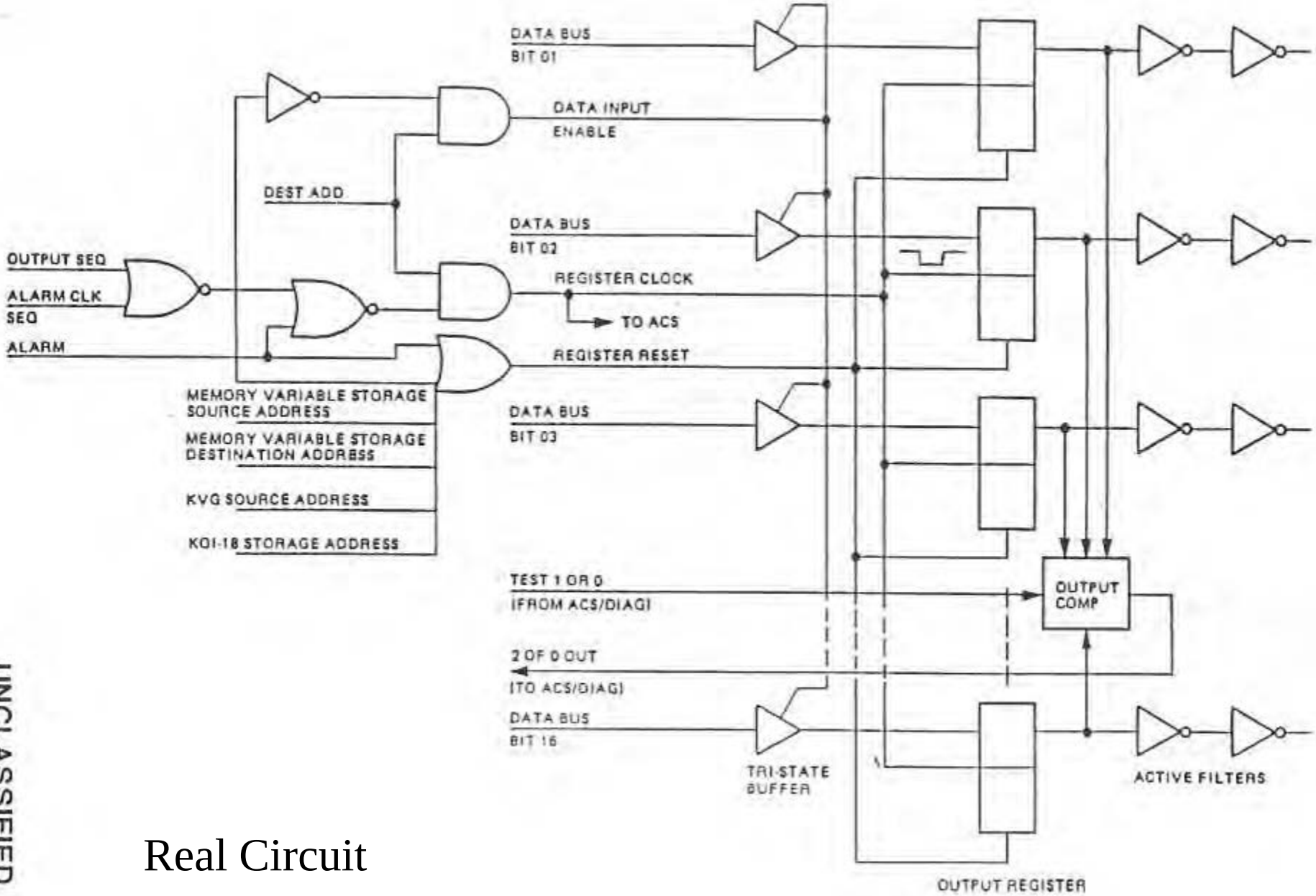
- The Government maintains an aggressive lab evaluation program to detect deficiencies in TEMPEST equipment
  - If a problem is discovered, the company is informed and given 3 months to fix it
  - If the problem isn’t fixed, the product is withdrawn
  - The ETPL should not be used as the final authority for further TEMPEST evaluations

Control Plan Specifics - Spectrum

- Spectrum Control
  - Description of how signals will be limited including good engineering design practices and interface considerations.
    - Function, purpose, and location of signals
    - Waveform characteristics
    - Spectral content
    - Proposed signal constraints

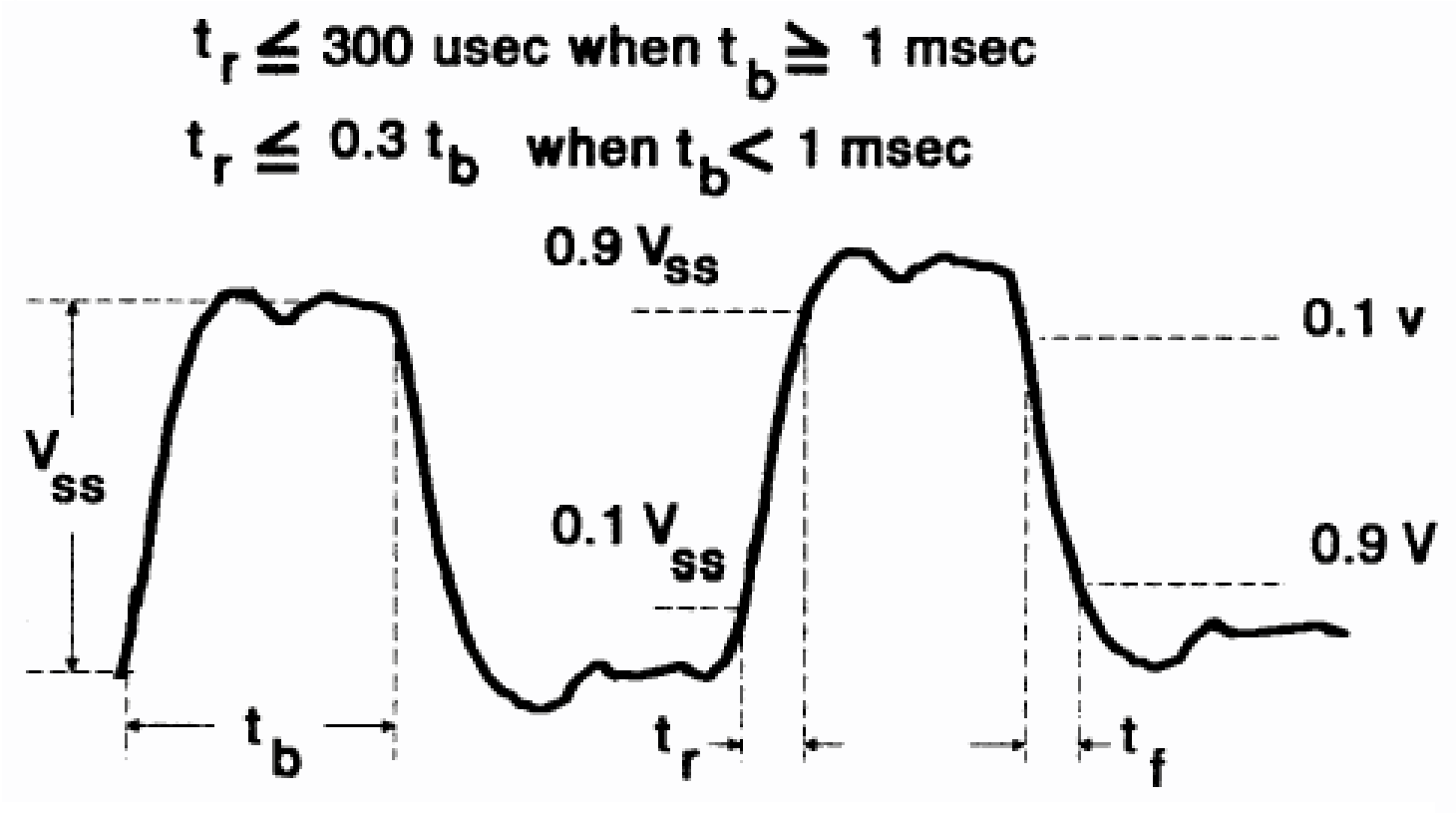
Circuit Locations



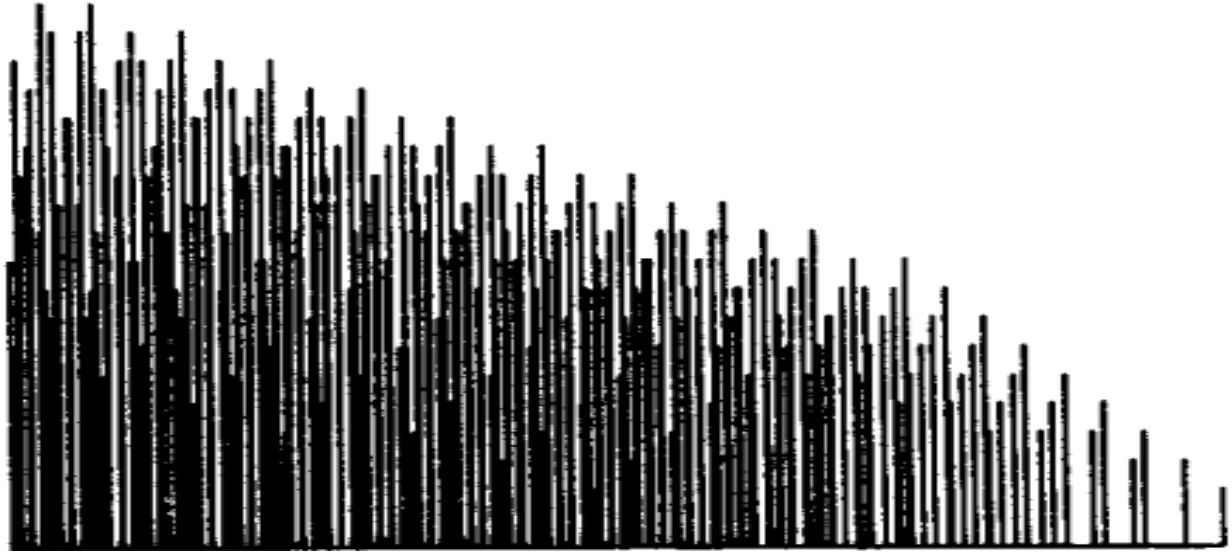


Real Circuit

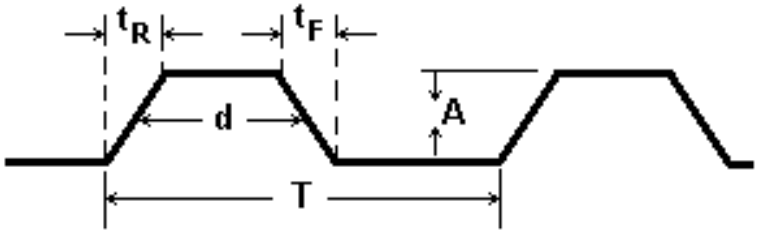
Waveform Characteristics



Calculate Spectral Content

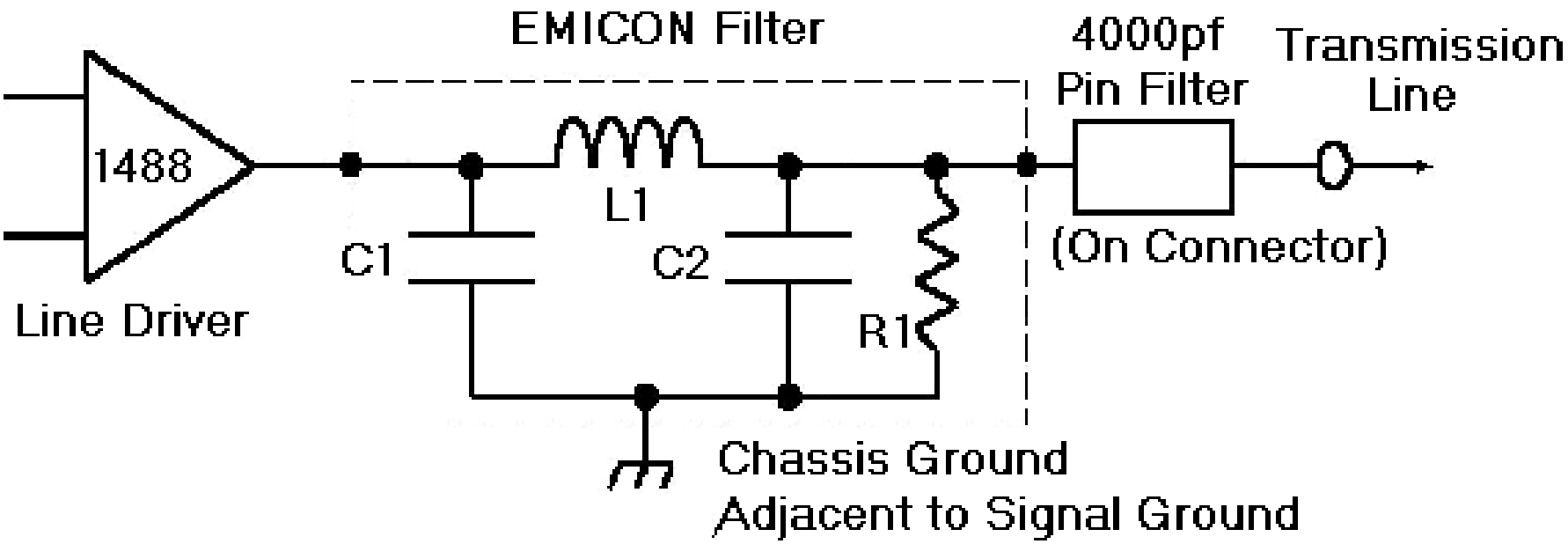


Predicted Emission Level



Lines	Amplitude		Pulse Width	No. of Spectral Lines	Spectral Spacing	Pulse Width Corner Freq.	First Null Freq.	Rise Time Corner Freq.	
	Narrowband	Broadband							
	$20\log\left(\frac{2Ad}{T}x10^{6}\right)$	$20\log\left(2Adx10^{12}\right)$	d	$\frac{T}{d}$	$\frac{1}{T}$	$\frac{1}{\pi d}$	$\frac{1}{d}$	$\frac{1}{\pi t}$	
								$t_R=$	$t_F=$
	$dB/\mu V$	$dB/\mu V/MHz$	S	Hz	Hz	Hz	Hz	Hz	Hz

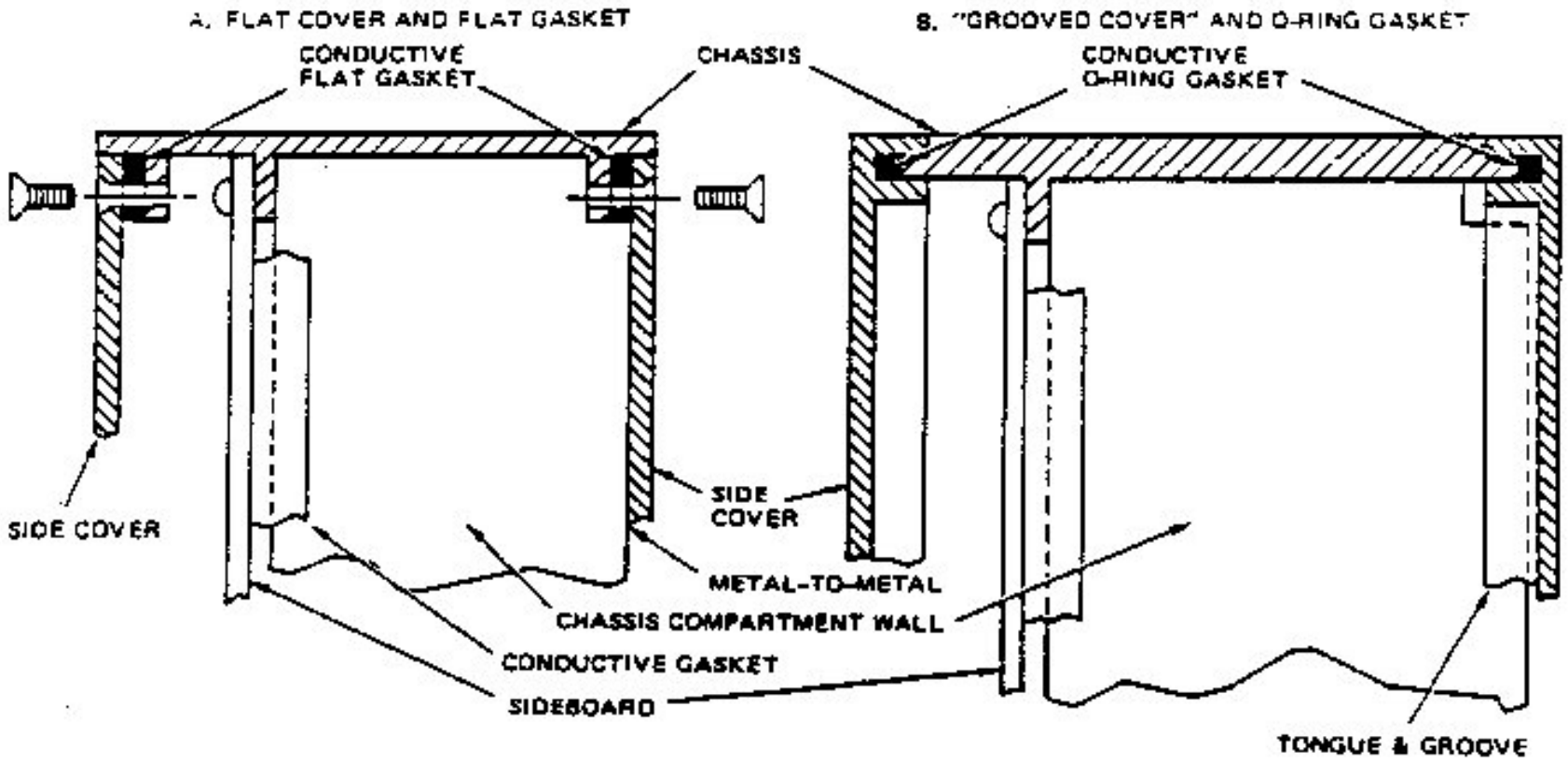
Signal Constraints



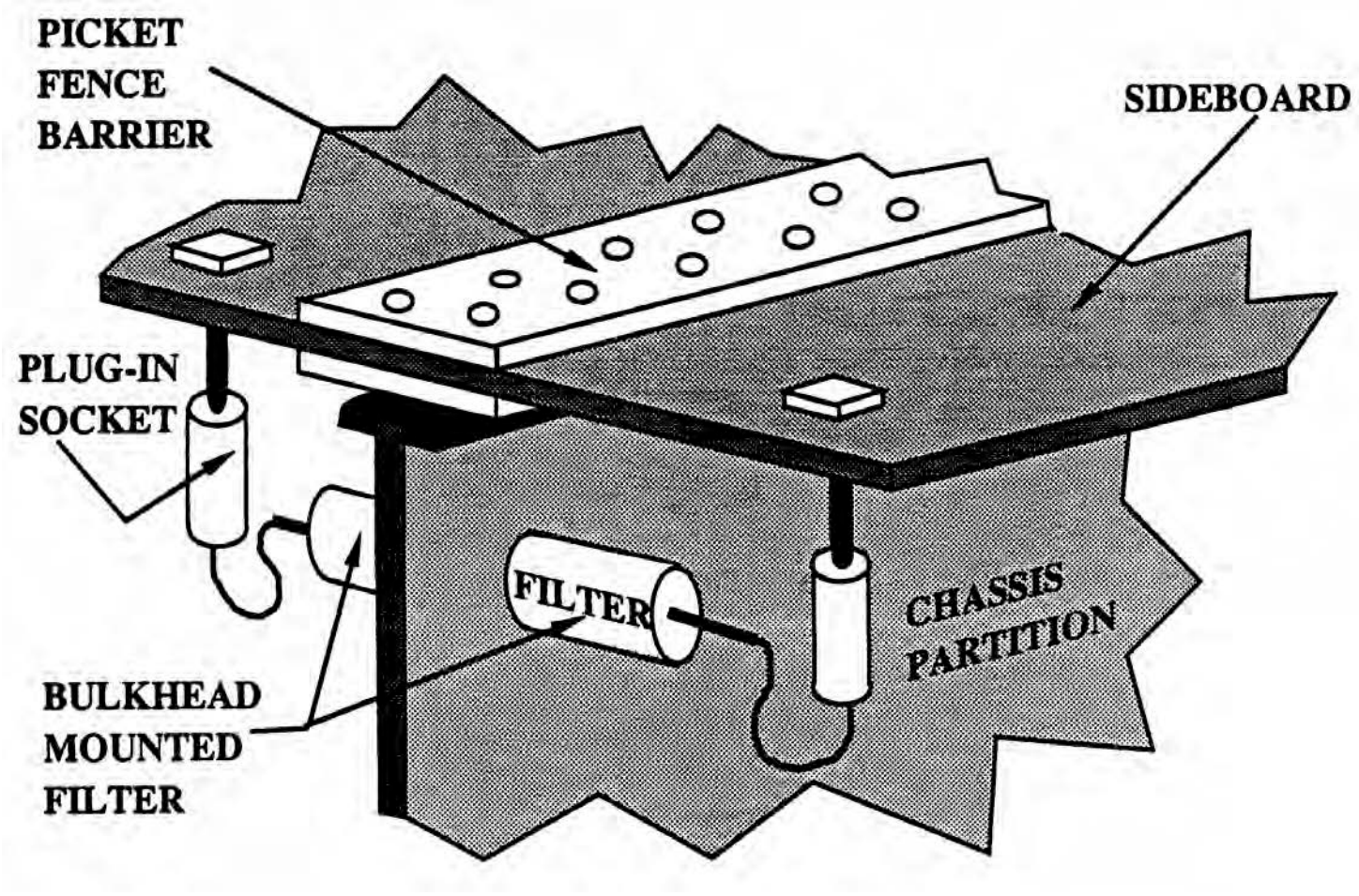
Control Plan Specifics - Mechanical

- Mechanical Design
  - Materials and construction methods
  - Access ports
  - Internal compartmentalization
  - Filter locations/applications
  - Gasketing
  - Grounding
    - Signal and chassis grounding

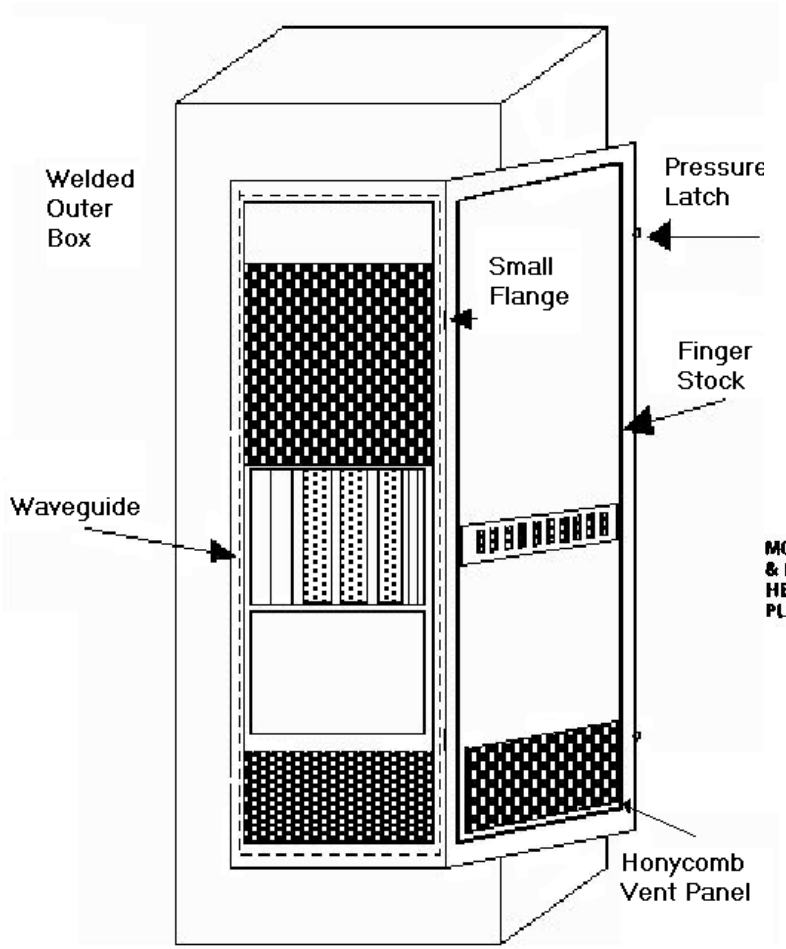
Construction Methods

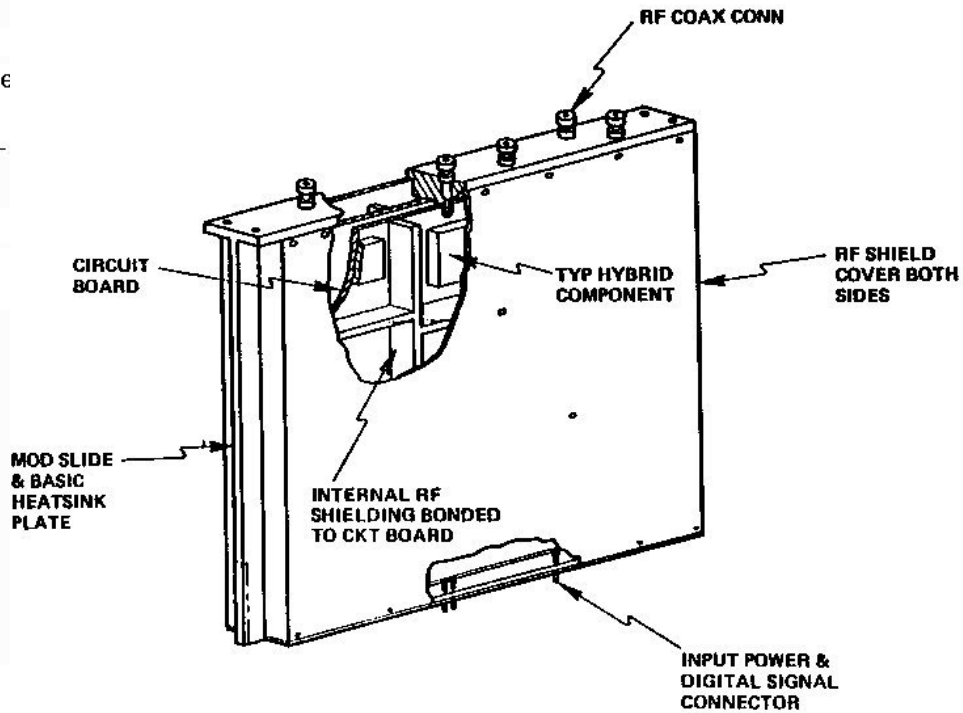


Filters Locations/Applications



Access Ports/Partitions

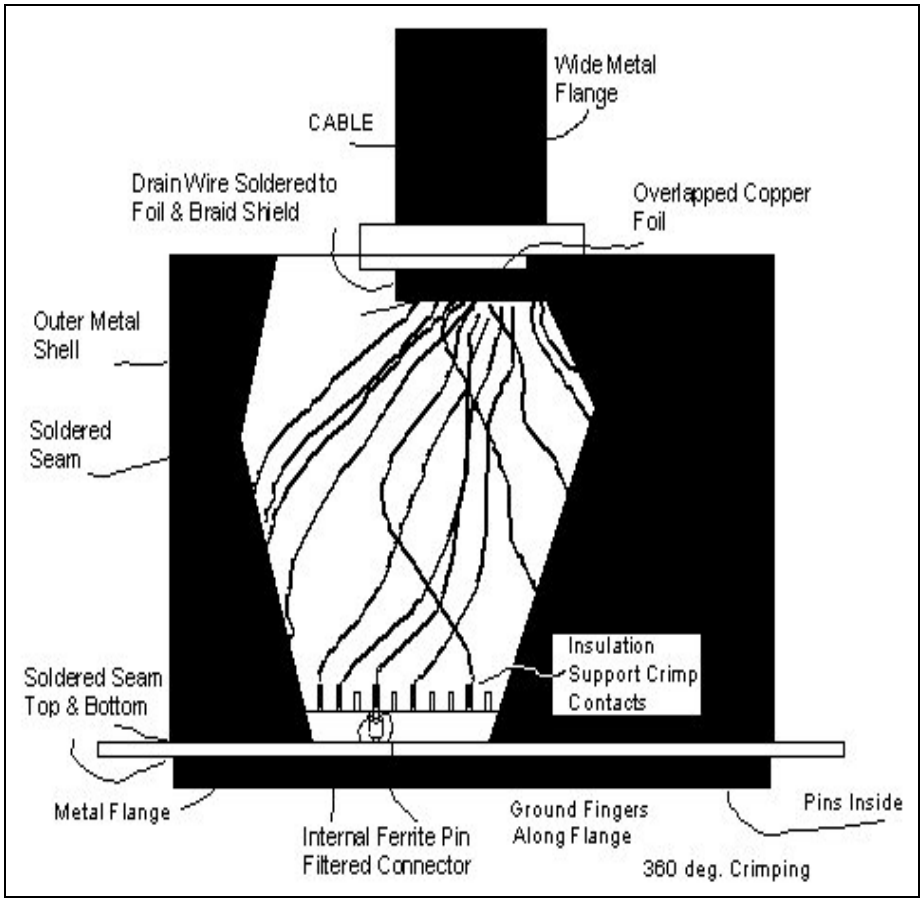


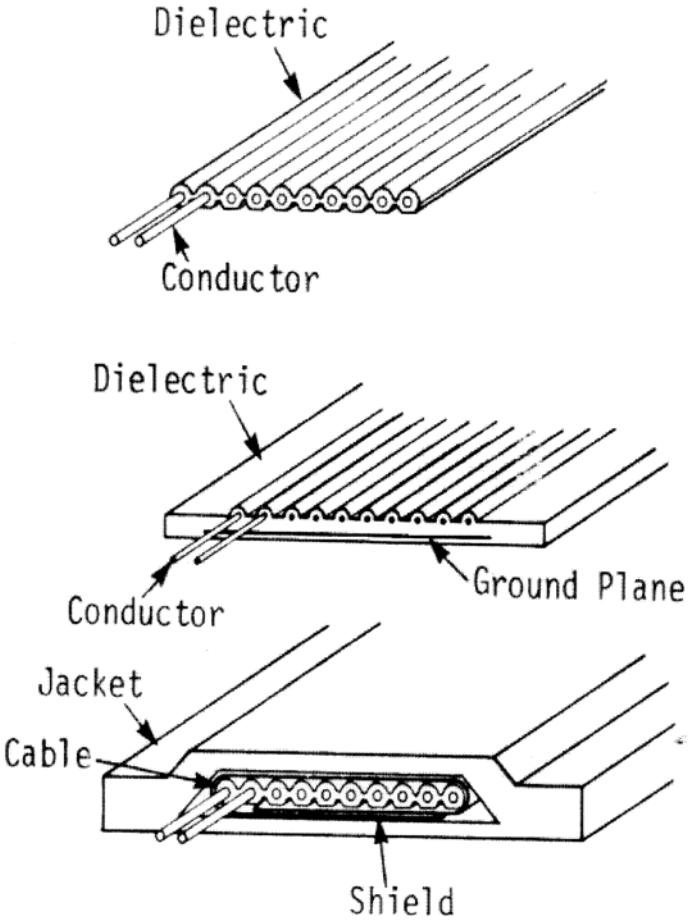


Control Plan Specifics - Connections

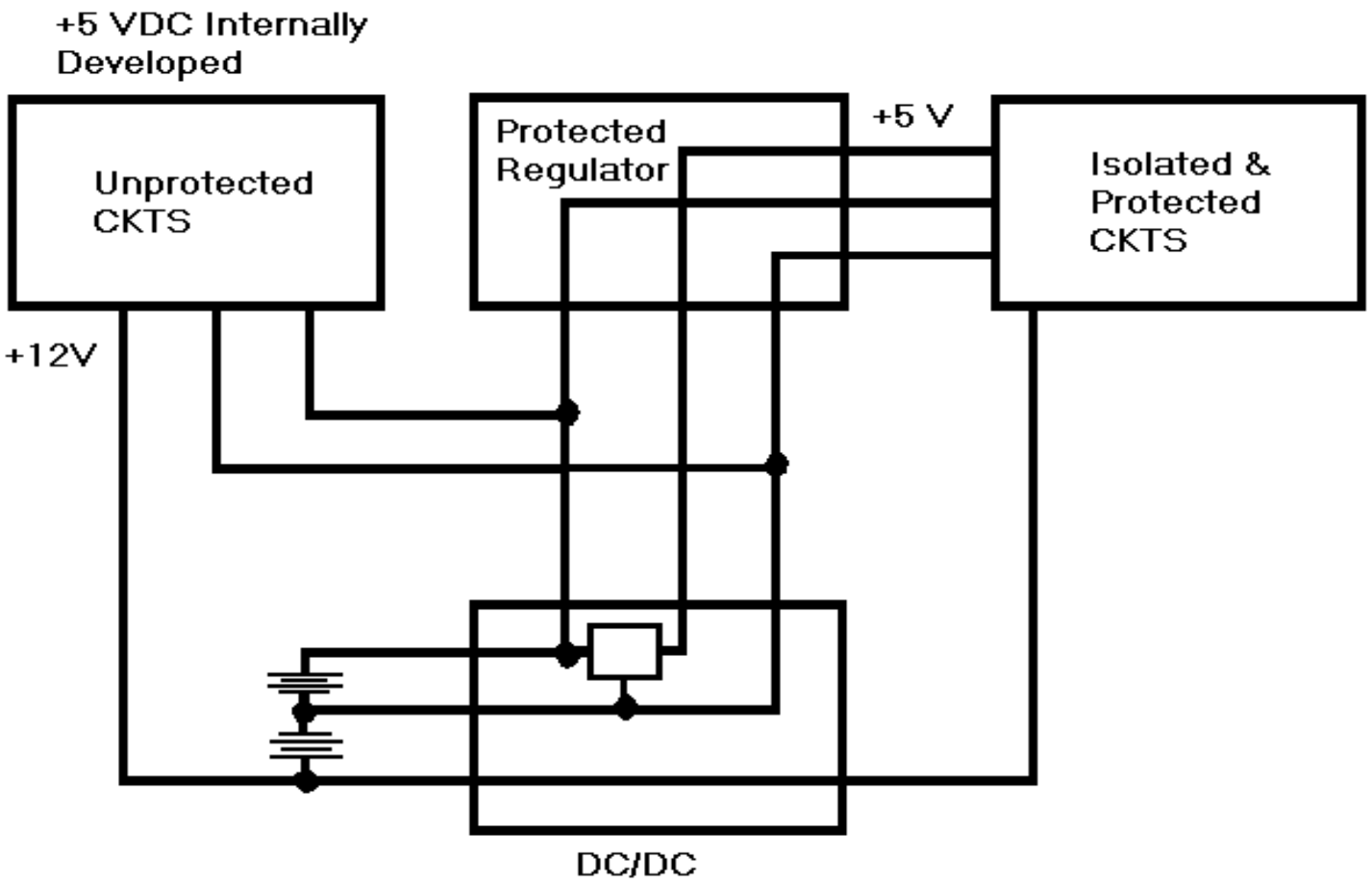
- Electronic/Electrical Wiring Design
  - Natural antenna reduction methods
    - Wave shaping
    - Backboard design
  - Coupling reduction methods including:
    - Connectors
    - Cable type/separation
    - Signal isolation
    - Power distribution system
    - Grounding

Cables/Connectors





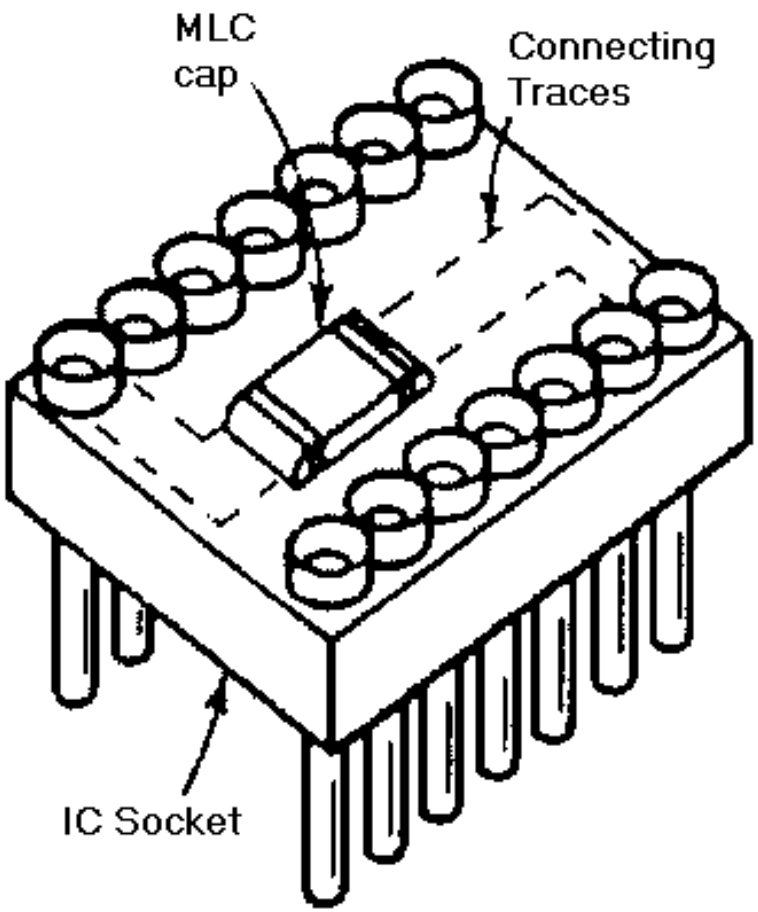
Power Distribution System/Grounding



Control Plan Specifics - Circuits

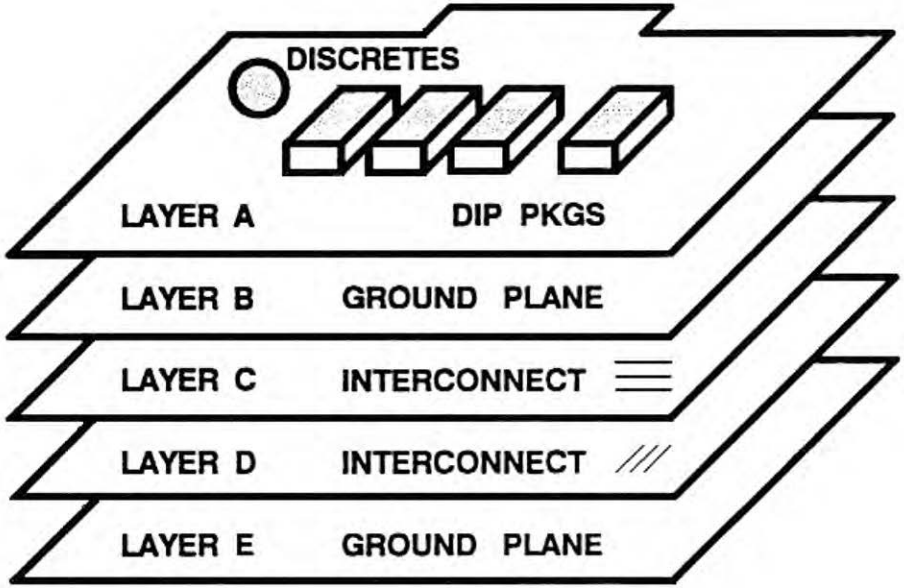
- Electrical/Electronic Circuit Design
  - Logic type
  - Rise and fall times
  - Gate grouping/fanout
  - Interface circuits
  - Filter characteristics
  - PC board design
  - Power supply isolation
  - Grounding

IC Decoupling

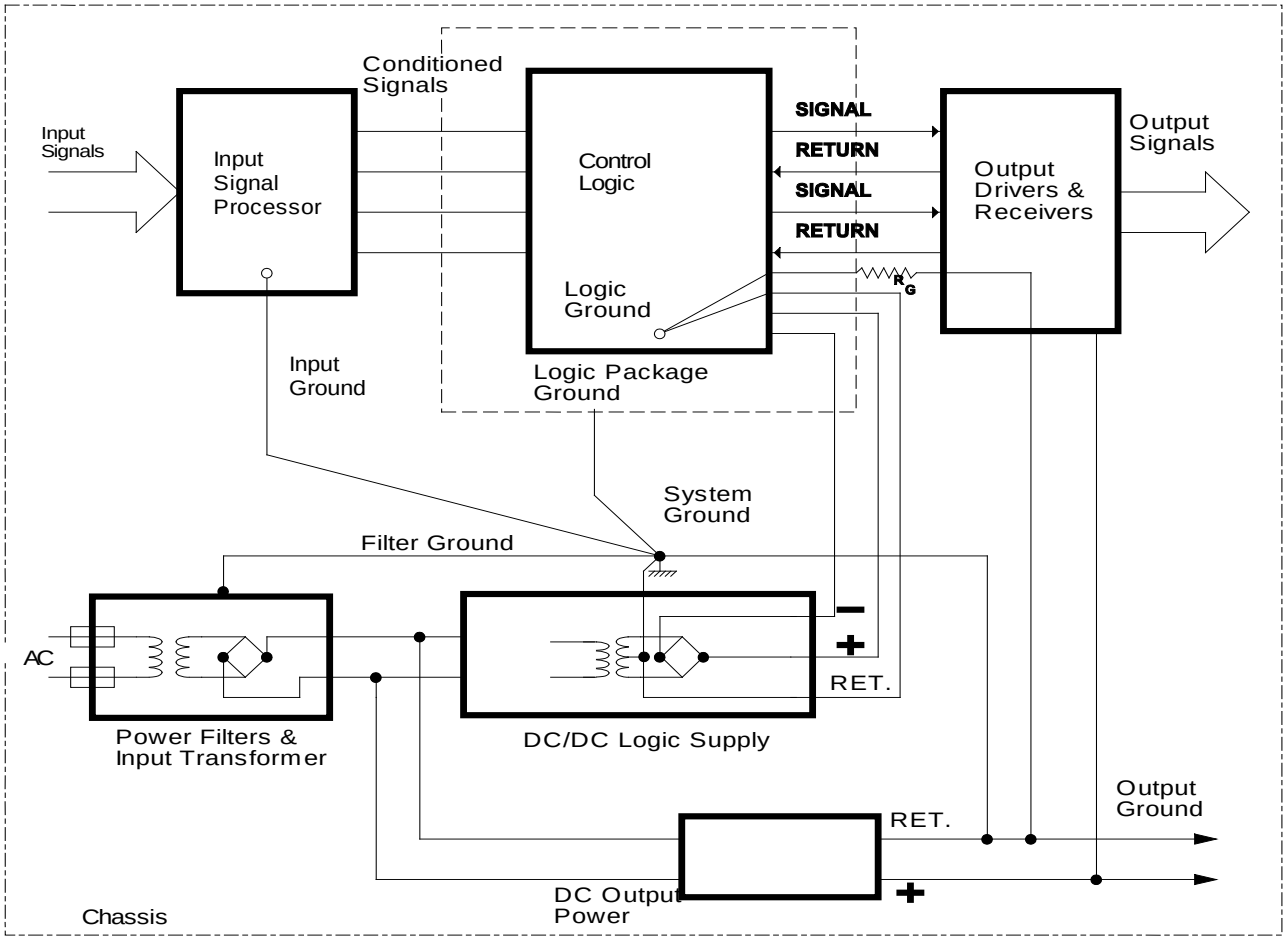


PC Board Design

Typical PC Board Sandwich Configuration



Power System/Supply Isolation



SPICE Analysis

- SPICE (or a variation such as PSPICE) is the tool used for analog circuit simulation on a PC card.
- The program will simulate difficult test measurements that would otherwise require significant equipment costs.
- By using equivalent discrete circuits in a lattice network, power supply reverse isolation can be calculated with realistic accuracy.

SPICE Noise Statement

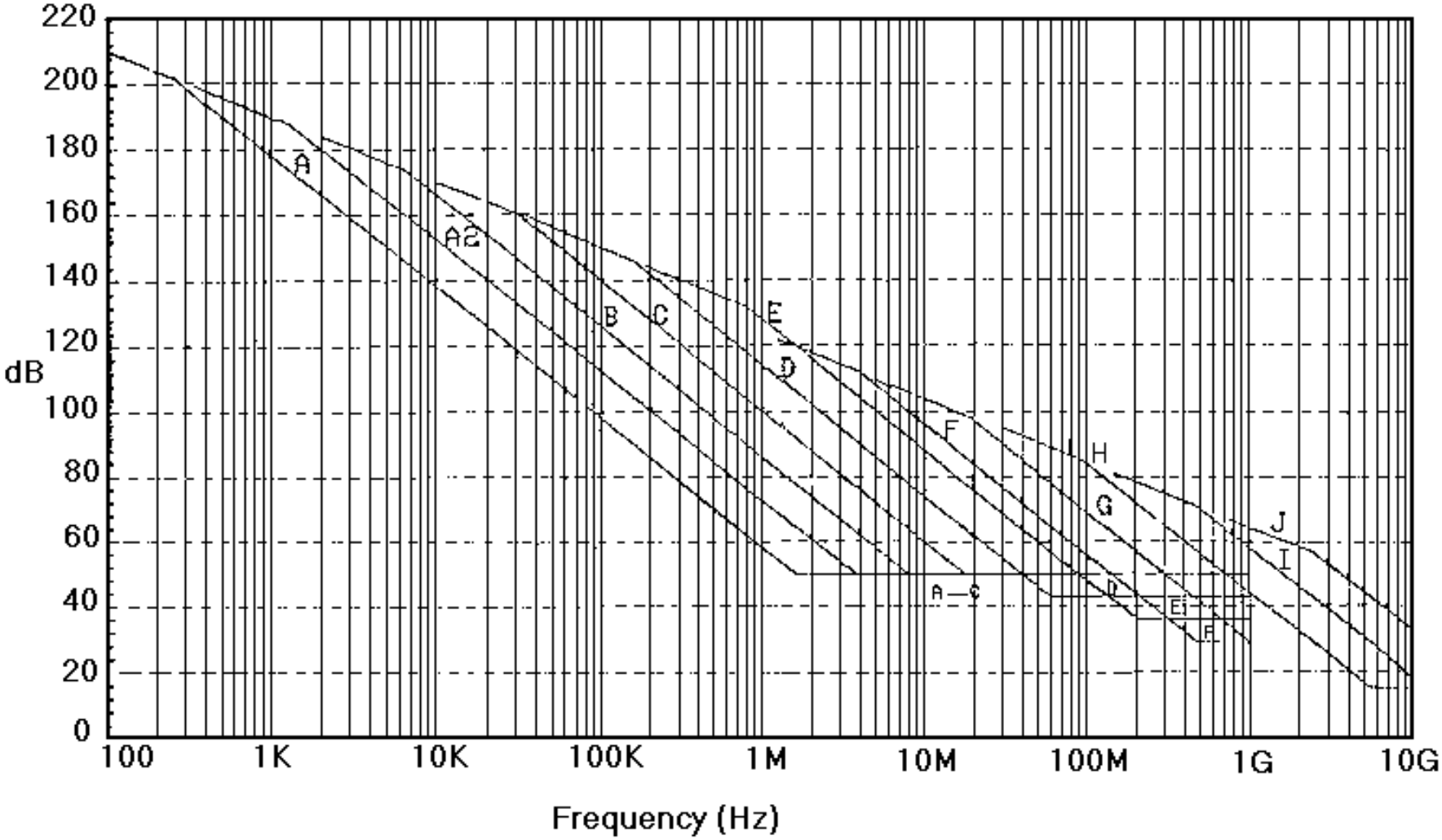
- The NOISE statement directs SPICE to perform the noise calculations and specifies which nodes are the output and where the input is.
  - Model the power supply backwards from output to input.
  - Specify the new power supply “input” as a 5 volt digital signal with the characteristics of your data pulse.
  - Calculate the frequency response.

GEMS Modeling

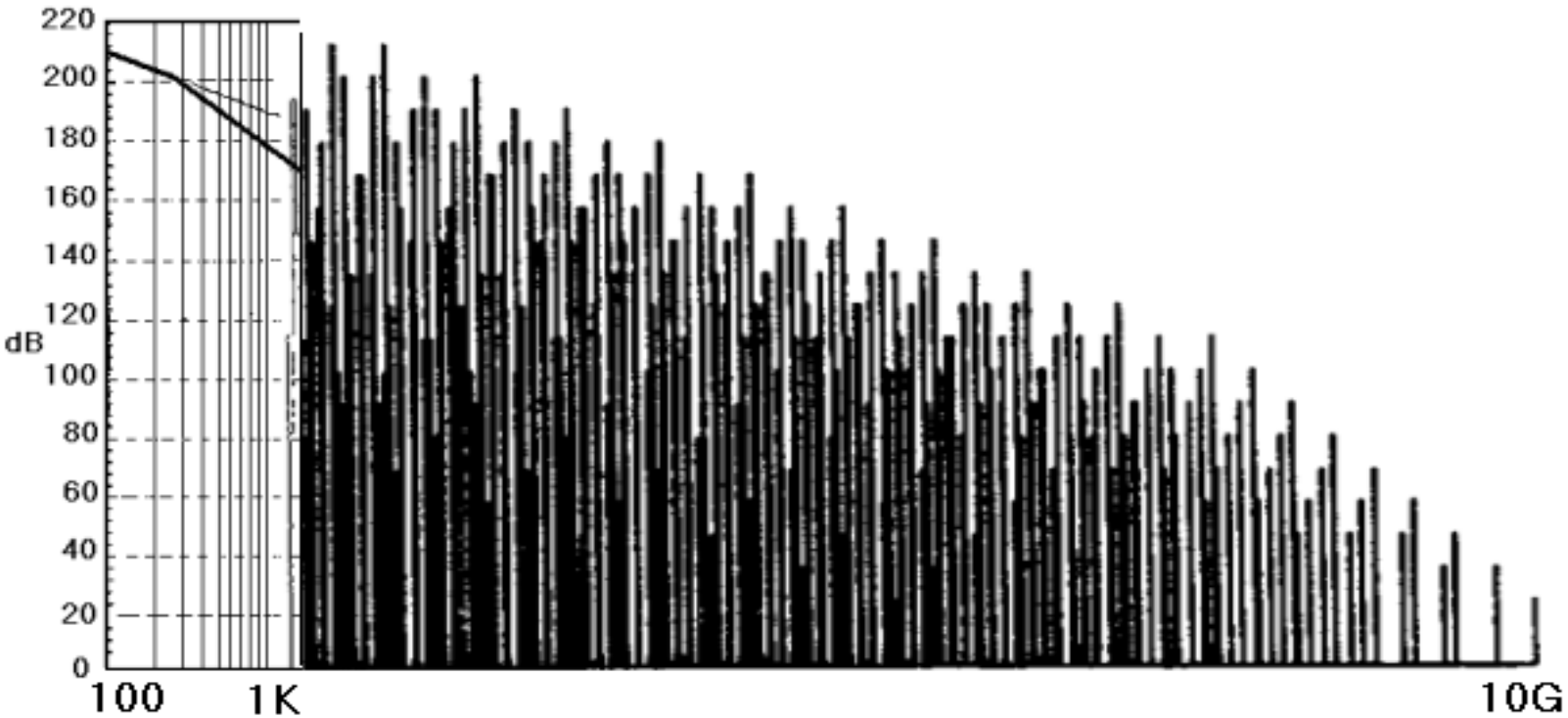
- The Graphical EMI Modeling Spreadsheet (GEMS) in a frequency domain graphical model calculation program.
- Designed for EMI predictions and fixes, it has several applications useful for TEMPEST modeling:
  - Ground loop coupling
  - Crosstalk
  - Propagation

Control Plan Specifics – R&D Testing

- R&D Testing
  - Quick look design related tests
    - Types of tests
      - Broadband & narrowband
      - Tunable & nontunable
    - Equipment set-ups
    - Emission mapping
    - Suppression approaches
      - To avoid contamination, use a battery powered fiber optic probe to monitor internal signal lines.

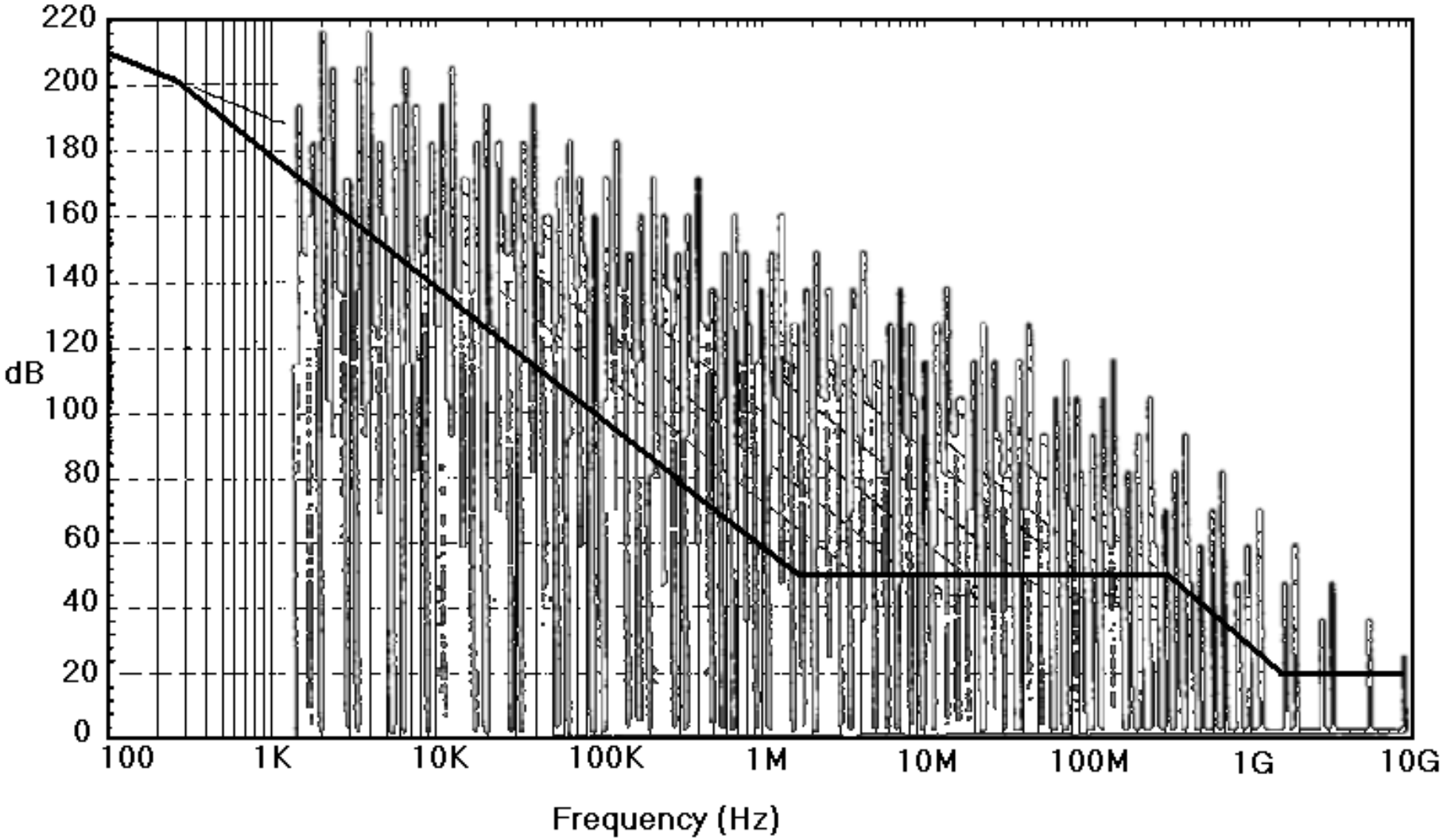


Example of Conducted Limits

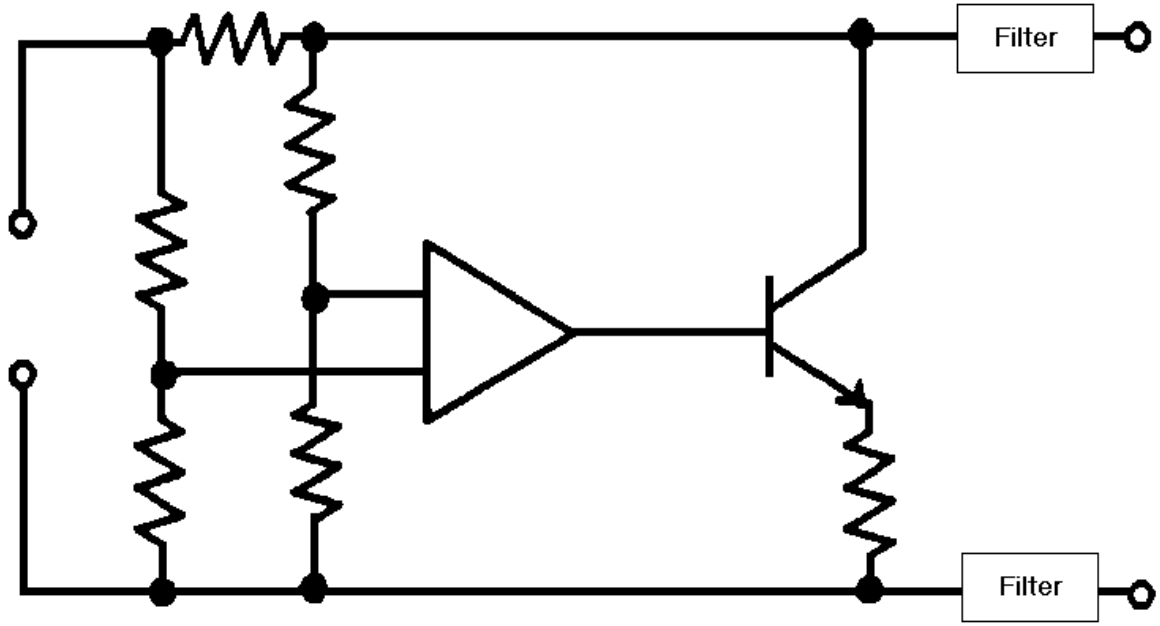


Calculate spectrum based on worst case 4.93 volt logic gate operating at a Red data rate. Note, this is a rough calculation since it doesn't account for the added energy due to many overshoots.

$$dB\mu V = 20\log\frac{V_2}{V_1} = 20\log\frac{5}{.7} \approx 128 dB\mu V$$



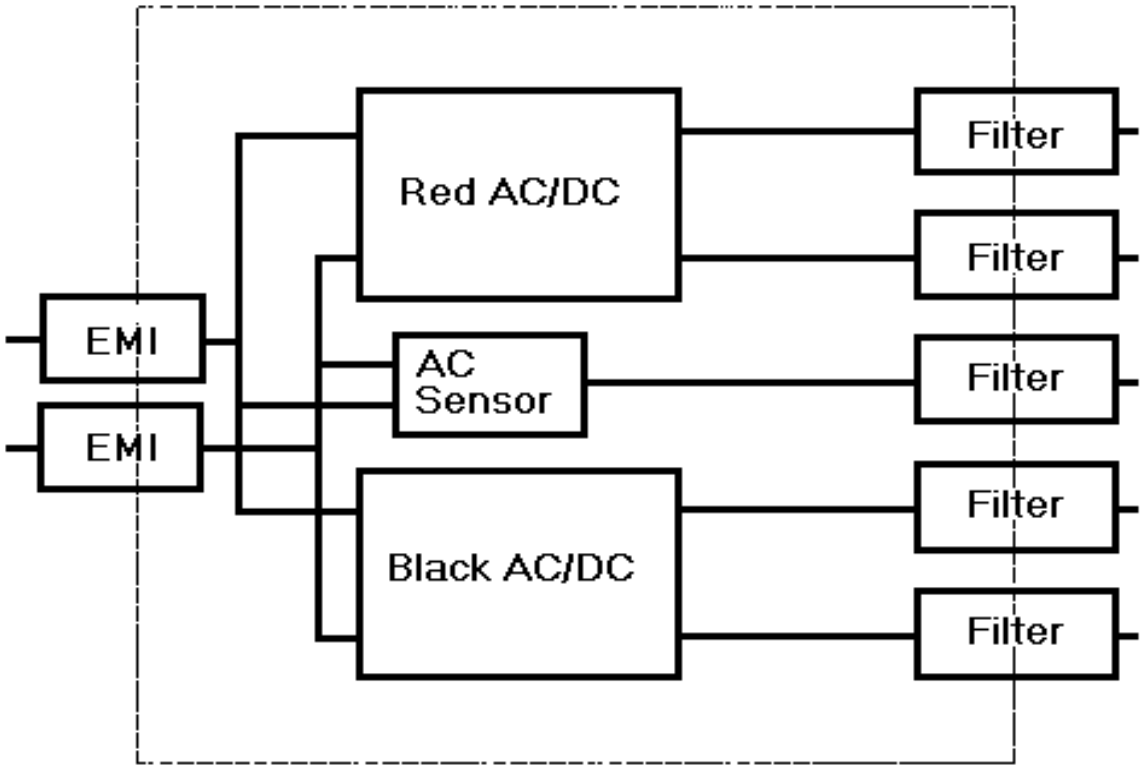
Overlay spectrum against applicable limit for conducted emissions at the redline category where it applies.



First assume all signal and power grounds have been configured correctly.

For powerline conducted emissions, start by reducing the calculated spectrum by the frequency response of the common-mode filters.

Next, reduce the spectrum by the reverse isolation of the regulator.



Calculate the voltage gain due to the input transformer.

Reduce the spectrum by the filter attenuation for the input filters.

Repeat for each Red signal.

Realistic and Predicted Levels

- A closer approximation of the generated energy can be determined by adding the combined energy (dBm) of the total number of series gates in the signal line that switch simultaneously.
- If any part of the spectrum exceeds the limits imposed, you will need to apply wave shaping or other means to reduce the emission level at its source.

Radiated Emissions

- Assume the entire calculated spectrum radiates as an E-Field emission.
- Overlay the radiated limits.
- Sequentially reduce the emission level based on:
  - PC Board ground planes
  - Isolation/shielding of adjacent wires
  - Mechanical design of housing
  - Use source suppression to reduce any predicted emissions over the required control level.

Design Control Plans Summary

- The TEMPEST Design Control Plan should be a “living” design plan of the product from beginning to end.
- Control Plan development by engineers supporting the design effort will insure a systems engineering approach is applied to the emanation control effort.
- Use the plan as justification for design activity and projected solutions before major delays are incurred.

TEMPEST Test Plans

- The test plan performs the function of tailoring general requirements found in the specifications to the specific requirements of the EUT.
- TEMPEST Test plans and the methods used to perform testing and evaluate results are classified.

Test Plan Contents

- Introduction
  - Scope of plan and objectives including references
- Provisions
  - Describes test equipment, calibrations, and breakout box or ancillary equipment requirements
- Fundamentals
  - Describes specific tests and their relationship to the EUT

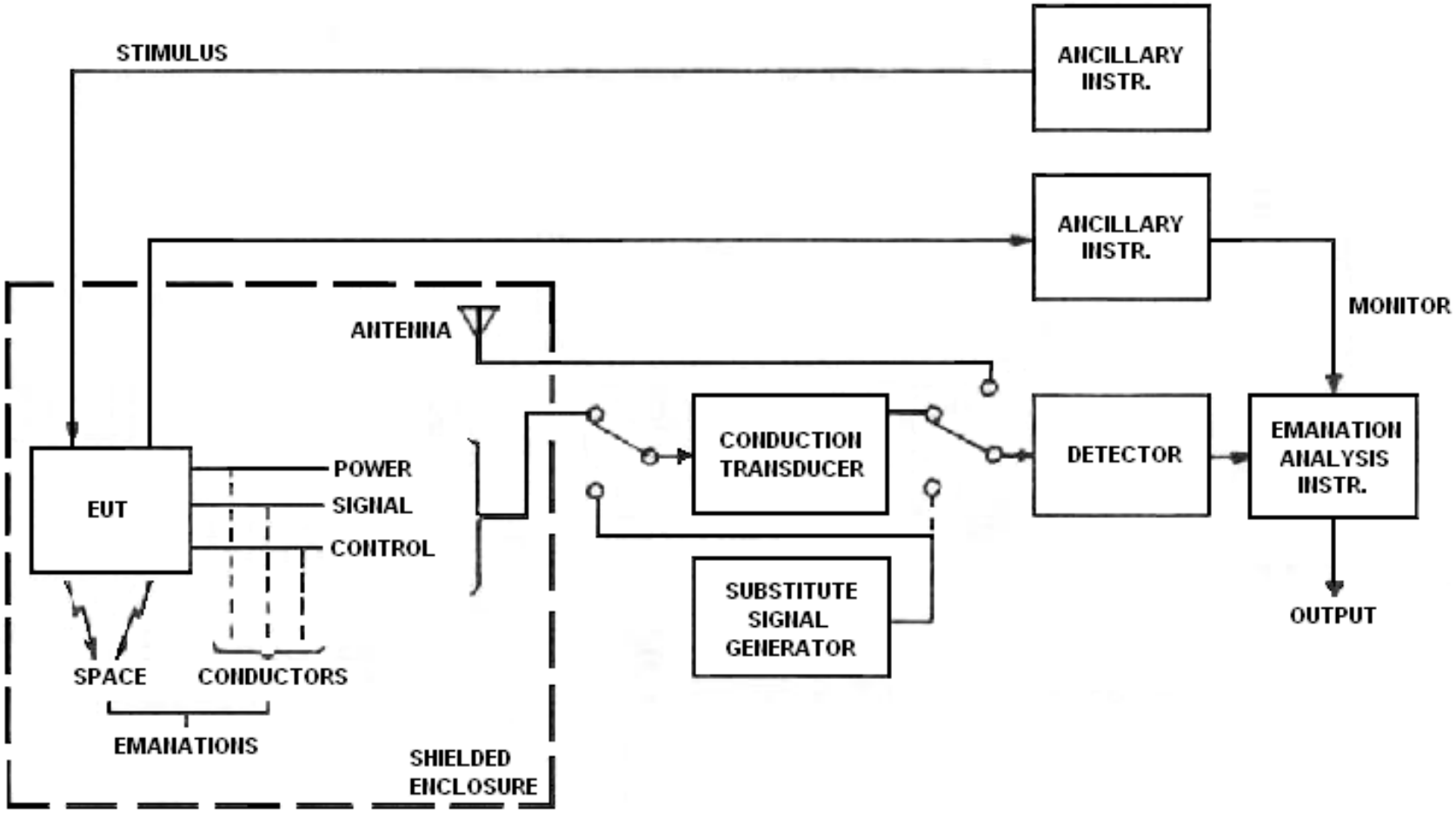
Test Plan Contents (Cont.)

- Hardware Setup
  - Includes facility and equipment interconnection requirements
    - May also include software and/or short-cycle needs
- Test Setup Verification
  - Defines pre-test requirements and procedures
- Detection System Certification Results
  - Compares measurement sensitivities to requirement limits for specific tests to be performed

Test Plan Contents (Cont.)

- Test Facility Certification Results
  - Facility description, dates of certification, plots of applicable results, list of instrumentation, background signals detected
- Ambient Signal Control Test Results
  - Dates of tests, functional description of breakout box, test environment plots

Test Plan Test Set-Up



Final TEMPEST Test Report

- The final report compares the results of testing to the test limits imposed on the equipment based on generated emission characteristics.
- Report outline contains:
  - Introduction, Summary, Conclusion and Recommendations, Provisions, Detailed Results, Limits, Deviations

Production Testing

- Random testing of production units is required
- Intended to outline the TEMPEST characteristics of the production equipment or systems that were tested as a validation of QA control.
- Discrepancies can result in fielded equipment recalls.

Production Testing Details

- A complete formal TEMPEST test is performed on the EUT (in most cases).
  - Identifies emerging deficiencies, their causes, when in production they occurred, and to provide a record available for application to future programs and technology advances.
  - Deficiencies must be corrected with a patch within 90 days.
  - Some organizations have interpreted the requirement to mean perform 1/3 the tests on each box until all tests are performed.

TEMPEST Data Item Descriptions

- Test Plan developed per NSA DI-T-5140C
- Test Facility Certification Report developed per NSA DI-T-5181B
- Detection System Certification Report developed per DI-T-5182B
- Cursory Test Report developed per NSA U-T-5604
- Test Setup Ambient Signal Control developed per NSA DI-T-5183B
- Test Evaluation Report per NSA DI-T-5180B
- Production Test Report per NSA DI-T-5149A

TEMPEST System Security Engineering Management

Based on SSEM in the Secure LAN/WAN Environment

Bruce Gabrielson, PhD

brucegabrielson@yahoo.com

Last Updated: 2002

SSEM Overview

- Policy - The ultimate goal of a system security standard is to insure a level of security, consistent with security priorities, is applied to resources throughout their deployed life-cycle.
- Scope – When dictated by system vulnerabilities, the program insures all security disciplines are integrated into the design.

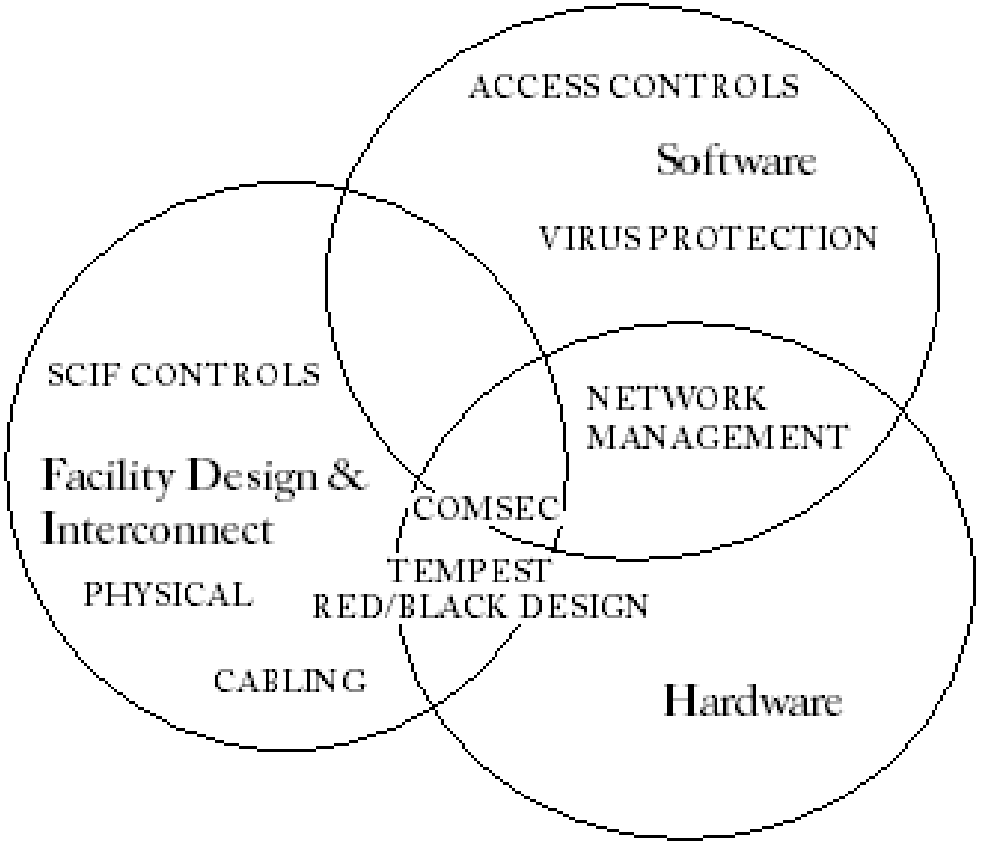
Security Engineering Management Plan

- Often used for the design of a large system or a facility containing multiple RED equipment areas.
- Initial document similar to a TEMPEST Design Control Plan
- Concentration on the potential threat and vulnerability assessments.

SSEM for Facilities

- Access control and monitored space
- Perimeter intrusion detection
- Interior intrusion detection
- TEMPEST Zone designations
- System configuration

During the Life-cycle SSEM Handles Multiple Disciplines



Acquisition Phases

- Concept Exploration Phase
- Demonstration & Validation Phase
- Full Scale Development Phase
- Construction and Installation Phase

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

Concept Exploration Phase (cont.)

- 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 (Screen room necessity)
  - SCIF/Vault
    - Continuous/non-continuous, Class requirements, Access Control/Physical Security, Alarm Requirements, SIGINT (threat environment)
  - Power/Ground System
  - Emission requirements and options

Demonstration & Validation Phase

- 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

Demonstration & Validation Phase (cont.)

- Equipment
  - Specification requirements
  - Hardware to be protected
    - COMSEC, TEMPEST, Red/Black, LAN's, node vs. box level security,
- Facility/People
  - Alarms
  - Access control
  - HUMINT
  - Storage

Full Scale Development Phase

- 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

- Hardware:
  - Maintenance manuals
  - Special requirements for TEMPEST
- Facility:
  - TEMPEST field/room attenuation testing
  - Builders warranty
  - Methods of defeating security protection techniques