NOTICE OF VALIDATION

INCH-POUND

MIL-HDBK-232A
NOTICE 2
24 October 2000

MILITARY HANDBOOK

RED/BLACK ENGINEERING-INSTALLATION GUIDELINES

MIL-HDBK-232A, dated 25 July 1988, has been reviewed and determined to be valid for use in acquistion.

Custodians:
Army - CR
Navy - EC
Air Force - 02

Preparing activity:
Army - CR

Reviewer Activities:
Navy - MC
Air Force - 11, 13
Other - DC, JT, NS

AMSC N/A **AREA TCSS**

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

MILITARY HANDBOOK

MIL-HDBK-232A
Notice 1
25 July 1988

RED/BLACK ENGINEERING-INSTALLATION

GUIDELINES

TO ALL HOLDERS OF MIL-HDBK-232A:

1. THE FOLLOWING PAGES OF MIL-HDBK-232A HAVE BEEN REVISED AND SUPERSEDE THE PAGES LISTED:

NEW PAGE	DATE	SUPERSEDED PAGE	DATE
Cover	20 March 1987	Cover	20 March 1987
ii	20 March 1987	ii	REPRINTED WITHOUT CHANGE

2. RETAIN THIS NOTICE AND INSERT BEFORE TABLE OF CONTENTS.

3. Holders of MIL-HDBK-232A will verify that page changes and additions indicated above have been entered. This notice page will be retained as a check sheet. This issuance, together with appended pages, is a separate publication. Each notice is to be retained by stocking points until the military handbook is completely revised or canceled.

Custodians:
Army - SC
Navy - EC
Air Force - 90

Preparing Activity:
Army - SC

(Project SLHC-2323)

Review Activities:
Army - CR
Navy - EC, MC
Air Force - 17, 89
DoD - DC, NS, JT

AMSC N/A

AREA SLHC

MIL-HDBK-232A
20 MARCH 1987
SUPERSEDING
MIL-HDBK-232
14 NOVEMBER 1972

MILITARY HANDBOOK

RED/BLACK ENGINEERING-INSTALLATION GUIDELINES

AMSC NO. N/A AREA SLHC/TCTS

DEPARTMENT OF DEFENSE
WASHINGTON, DC 20301

RED/BLACK ENGINEERING-INSTALLATION GUIDELINES

1. This standardization handbook was developed by the Department of Defense with the assistance of the Military Departments and Federal Agencies.

2. This handbook provides fundamental guidance to engineer and install electronic systems that process or communicate classified information. It contains guidance which will, when used in conjunction with department/agency directives, aid in the protection of such information by reducing the probability of hostile interception and exploitation.

3. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document should be submitted to Commander, U.S. Army Information Systems Engineering and Integration Center, ATTN: ASBI-SST, Fort Huachuca, AZ 85613-7300 by using the self-addressed Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

FOREWORD

This revision has been prepared to satisfy a need for an unclassified document describing the fundamental "How-To's" of RED/BLACK engineering and installation. Its principles and guidance stress sound engineering practices to produce a safe environment to process or communicate classified defense information. Its unclassified nature permits its distribution to the lowest operating level to enhance an awareness of RED/BLACK and TEMPEST principles.

This document includes metrication. The handbook is not measurement sensitive. See the current edition of MIL-STD-962 for a discussion of measurement-sensitive metrication. The following conversion factors have been used for simplicity.

1 inch = 25 millimeters

3 feet = 0.9 meters

THIS PAGE INTENTIONALLY LEFT BLANK

CONTENTS

CONTENTS - Continued

CONTENTS - Continued

CONTENTS - Continued

CONTENTS - Continued

CONTENTS - Continued

CONTENTS - Continued

FIGURES

CONTENTS - Continued

CONTENTS - Continued

TABLES

APPENDIXES

CONTENTS - Continued

CONTENTS - Continued

FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

1. SCOPE

1.1 Purpose. This handbook provides guidance with the RED/BLACK concept for the engineering and installation of systems and facilities processing classified information. The engineering installation concepts contained herein should be selectively applied for control of TEMPEST at all Department of Defense (DoD) facilities where classified information is processed.

1.2 Applicability. This handbook addresses and applies to the following general areas:

a. Power distribution, installation, and protection.

b. Equipment installation and protection.

c. Signal distribution, installation, and protection.

d. Filters and isolators.

e. Grounding, bonding, and shielding (CBS).

f. Physical security.

g. Administrative telephones.

THIS PAGE INTENTIONALLY LEFT BLANK

2. REFERENCED DOCUMENTS

2.1 Government documents.

2.1.1 Specifications, standards, and handbooks. Unless otherwise specified, the following specifications, standards, and handbooks of the issue listed in that issue of the Department of Defense Index of Specifications and Standards (DoDISS) specified in the solicitation, form a part of this handbook to the extent specified herein.

SPECIFICATIONS

MILITARY

MIL-F-15733	Military Specifications for Filters, Radio Frequency Interference

STANDARDS

FEDERAL

FED-STD-1037	Glossary of Telecommunication Terms

MILITARY

MIL-STD-188-100	Common Long Haul and Tactical Communications Systems Technical Standards
MIL-STD-188-111	Subsystem Design and Engineering Standards for Common Long Haul and Tactical Fiber Optics Communications
MIL-STD-188-114	Electrical Characteristics of Digital Interface Circuits
MIL-STD-188-124	Grounding, Bonding, and Shielding for Common Long Haul/Tactical Communication Systems, Including Ground Based Communications-Electronics Facilities and Equipments
MIL-STD-188-200	System Design and Engineering Standards for Tactical Communications
MIL-STD-220	RFI Filters, Methods of Testing
MIL-STD-285	Military Standard, Attenuation Measurements for Enclosures, Electromagnetic Shielding, for Electronic Test Purposes, Method of

HANDBOOKS

MILITARY

MIL-HDBK-411	Power and Environmental Control for the Physical Plant of DoD Long Haul Communications
MIL-HDBK-419	Grounding, Bonding, and Shielding for Electronic Equipments and Facilities

2.1.2 Other Government documents, drawings, and publications. The following other Government documents, drawings, and publications form a part of this handbook to the extent specified herein.

Joint Chiefs of Staff

JCS Pub 1	Dictionary of Military and Associated Terms

National Communications Security Committee

NCSC-9	National Communications Security Glossary

National Security Agency

NACSI 4009	(C) Protected Distribution Systems (U)
NACSI 5004	(S) TEMPEST Countermeasures for Facilities Within the United States (U)
NACSI 5005	(S) TEMPEST Countermeasures for Facilities Outside the United States (U)
NACSIM 5100	(C) Compromising Emanations Laboratory Test Requirements, Electromagnetics (U)
NACSEM 5201	(C) TEMPEST Guidelines for Equipment/Systems Design Standard (U)
NACSIM 5002	(C) Suppression of Compromising Emanations Through Low Level Operation (U)
NACSIM 5203	(C) Guidelines for Facility Design and RED/BLACK Installation (U)
NACSEM 5204	(C) Shielded Enclosures (U)

Defense Intelligence Agency

DIAM 50-3	(FOUO) Physical Security of Special Compartmented Information Facilities (U)

Federal Communications Commission

FCC Reg Part 15 Subpart J	Rules and Regulations, Radio Frequency Devices; Computing Devices

National Bureau of Standards

FIPS PUB 94	Guideline on Electrical Power for ADP Installations

2.2 Other publications. The following document (s) form a part of this handbook to the extent specified herein. Unless otherwise specified, the issue of the documents which are DoD adopted shall be those listed in the issue of the DODISS specified in the solicitation. The issues of documents which have not been adopted shall be those in effect on the date of the cited DODISS.

National Fire Prevention Association

NFPA No. 70-19XX	National Electrical Code (NEC)
NFPA No. 78-19XX	Lightning Protection Code

THIS PAGE INTENTIONALLY LEFT BLANK

3. DEFINITIONS

3.1 Terms and definitions. Terms used in this handbook are defined in FED-STD-1037, JCS PUB 1, and NCSC-9, except as listed below, which are uniquely defined for the purpose of this handbook.

3.1.1 BLACK equipment area (BEA). An area in a limited exclusion area designated for the installation of equipment processing unclassified information or encrypted information.

3.1.9 Bulk filtering. The practice of using filters at the first service disconnect or on each power panel, thus filtering power to many items of equipment with one set of filters.

3.1.3 Cognizant TEMPEST agency. That agency within a department, service, or activity which, by virtue of its mission charter, has the knowledge to develop and the authority to implement rules, regulations, policies, criteria, and guidance to safeguard defense information, with specific emphasis on the implementation of the TEMPEST program.

3.1.4 Collateral. All national security information classified under the provisions of an executive order, for which special community systems of compartmentation (e.g., Sensitive Compartmented Information) are not formally established.

3.1.5 Controlled access area (CAA). The complete building, facility, or area under direct physical control which includes one or more limited exclusion areas, controlled BLACK equipment areas, or combinations thereof.

3.1.6 Controlled BLACK equipment area (CBEA). A BLACK equipment area which is not located in a limited exclusion area (LEA), but is afforded the same physical entry control which would be required if it were within an LEA.

3.1.7 Controlled space (CS). The three-dimensional space surrounding facilities that process classified information within which unauthorized personnel are: (a) denied unrestricted access, (b) escorted by authorized personnel, or (c) under continual physical or electronic surveillance.

3.1.8 Equipment radiation TEMPEST zone (ERTZ). A zone established as a result of determined or known equipment radiation TEMPEST characteristics. The zone includes all space within which a successful hostile intercept of compromising emanations is considered possible.

3.1.9 Hardened cable path. A path which provides physical protection for the cable such that a delay factor is applied against penetration or intrusion.

3.1.10 Limited exclusion area (LEA). A room or enclosed area where security controls have been applied to provide protection to the equipment and wire lines of a RED information processing system equivalent to the security required for the information transmitted through the system. An LEA must contain a RED equipment area.

3.1.11 Protected distribution system (PDS). An approved transmission adequate acoustical, electrical, electromagnetic, and physical safeguards have been applied to permit the transmission of unencrypted classified information. The associated facilities include all equipment and wire lines to be safeguarded. The major components are defined as follows:

a. Distribution system. The metallic wire paths or fiber optic transmission paths that provide interconnection between components of the protected system. The distribution system may be an internal PDS within the controlled space or an external PDS traversing an uncontrolled access area.

b. Subscriber sets and terminal equipment. The complete assembly of equipment, exclusive of interconnecting signal lines, located on the end user's or customer's premises. This includes such items as telephones, teletypewriters, facsimile data sets, input/output devices, switchboards, patch boards, consoles, or any other device which processes classified information.

3.1.12 RED equipment area (REA). The space within a limited exclusion area which is designated for installation of RED information processing equipment and associated power, signal, control, ground, and distribution facilities.

3.1.13 TEMPEST approved equipment or systems. Equipment or systems which have been certified within the requirements of the effective edition of NACSIM 5100, or TEMPEST specifications as determined by the department or agency concerned.

3.1.14 Uncontrolled access area (UAA). The area external or internal to a facility over which no personnel access controls can be or are exercised.

3.2 Acronyms and abbreviations. The following acronyms and abbreviations used in this Military Handbook are defined as follows:

a. ATDD - automatic telephone disconnect device

b. CBX - computer controlled branch exchange

c. DF - distribution frame

d. EESS - earth electrode subsystem

e. EIA - Electronic Industries Association

f. EM - electromagnetic

g. EMC - electromagnetic compatibility

h. EMI - electromagnetic interference

i. EMP - electromagnetic pulse

j. EPABX - electronic private automatic branch exchange

k. FOC - fiber optic cable

l. FPSS - fault protection subsystem

m. GBS - grounding, bonding, shielding

n. HEMP - high-altitude electromagnetic pulse

o. IDS - intrusion detection system

p. KSU - key service unit

q. KTU - key telephone unit

r. LAN - local area network

s. MDF - main distribution frame

t. MG - motor generator

u. MOV - metal oxide varister

v. NDI - nondevelopmental item

w. PABX - private automatic branch exchange

x. PBX - private branch exchange

v. PCZ - physical control zone (obsolete term, see 3.1.7)

z. PLC - power-line conduction

aa. PTF - patch and test facility

ab. RF - radio frequency

ac. RFI - radio frequency interference

ad. SCI - Sensitive-Compartmented Information

ae. SCIF - sensitive compartmented information facility

af. TPD - terminal protective device

ag. UPS - uninterruptible power supply

ah. VDU - video display unit

ai. VF - voice frequency

THIS PAGE INTENTIONALLY LEFT BLANK

4. GENERAL REQUIREMENTS

4.1 General. Section 4 provides minimum engineering-installation guidance for general application to all equipment and systems processing classified information, Two interrelated principles apply - the RED/BLACK concept (see FED-STD-1037) and TEMPEST (see NCSC-9). The RED/BLACK concept provides that electrical and electronic components, equipment, and systems processing classified plain text information be kept separate from those that process encrypted or unclassified information. TEMPEST, as used here, is those measures used to control compromising emanations. Figure I depicts a facility designed to RED/BLACK and TEMPEST guidance. While these terms are often used interchangeably, the concepts are separate and distinct. A facility properly designed to provide RED/BLACK separation may contain TEMPEST discrepancies. The guidance of this handbook presupposes the use of low-level balanced voltage digital signaling as defined in MIL-STD-188-114 and NACSIM 5002, except where specifically noted otherwise (e.g., unbalanced voltage digital signaling). Additional treatments may be required for all or part of a facility if high-level signaling is used. TEMPEST testing after installation and activation may indicate the need for additional protective measures. Such additional treatment will be determined by the cognizant TEMPEST authority on a case-by-case basis. Consideration will also be given to TEMPEST benefits derived from protection for electromagnetic pulse (EMP)/high-altitude electromagnetic pulse (HEMP), electromagnetic interference (EMI), and radio frequency interference (RFI). Although this handbook is not specifically directed to the measures used for EMP/HEMP protection, the attributes of EMP protection which may satisfy TEMPEST have been addressed (see appendix C). The design considerations of EMP and TEMPEST are similar - to protect signals and equipment in one area from activity in another area. The major differences are in the levels (voltage, current, and field strength, which are very high for EMP/HEMP signals and normally moderate to quite low for TEMPEST signals), and the direction of protection (outside to inside for EMP/HEMP and inside to outside for TEMPEST). The major differences in practices used to provide both types of protection are found in treatment of grounding paths and in the amount, and to some extent, the types of protection provided for any paths that are required between outside and inside. In general, any facility that is adequately protected from EMP/HEMP effects will provide a significant portion of the required TEMPEST protection. The requirements for effective RFI/EMI control are similar to those for EMP/HEMP and TEMPEST. RFI and EMI can be either external (keep it out) or internal (keep it from getting out). The practices to accomplish this containment are defined in electromagnetic compatibility (EMC) programs. The practices used to control each are very closely related to those for TEMPEST and EMP/HEMP. This handbook will provide the minimum guidance required for RED/BLACK installations. This guidance, where applicable, will track with practices required for control of RFI/EMI or EMP/HEMP effects. Six major design and installation techniques are used in the RED/BLACK environment.

a. Grounding.
b. Bonding.
c. Shielding.
d. Physical separation.
e. Physical protection.
f. Filtering and isolation.

These techniques will be used in varying degrees in every installation that processes classified information.

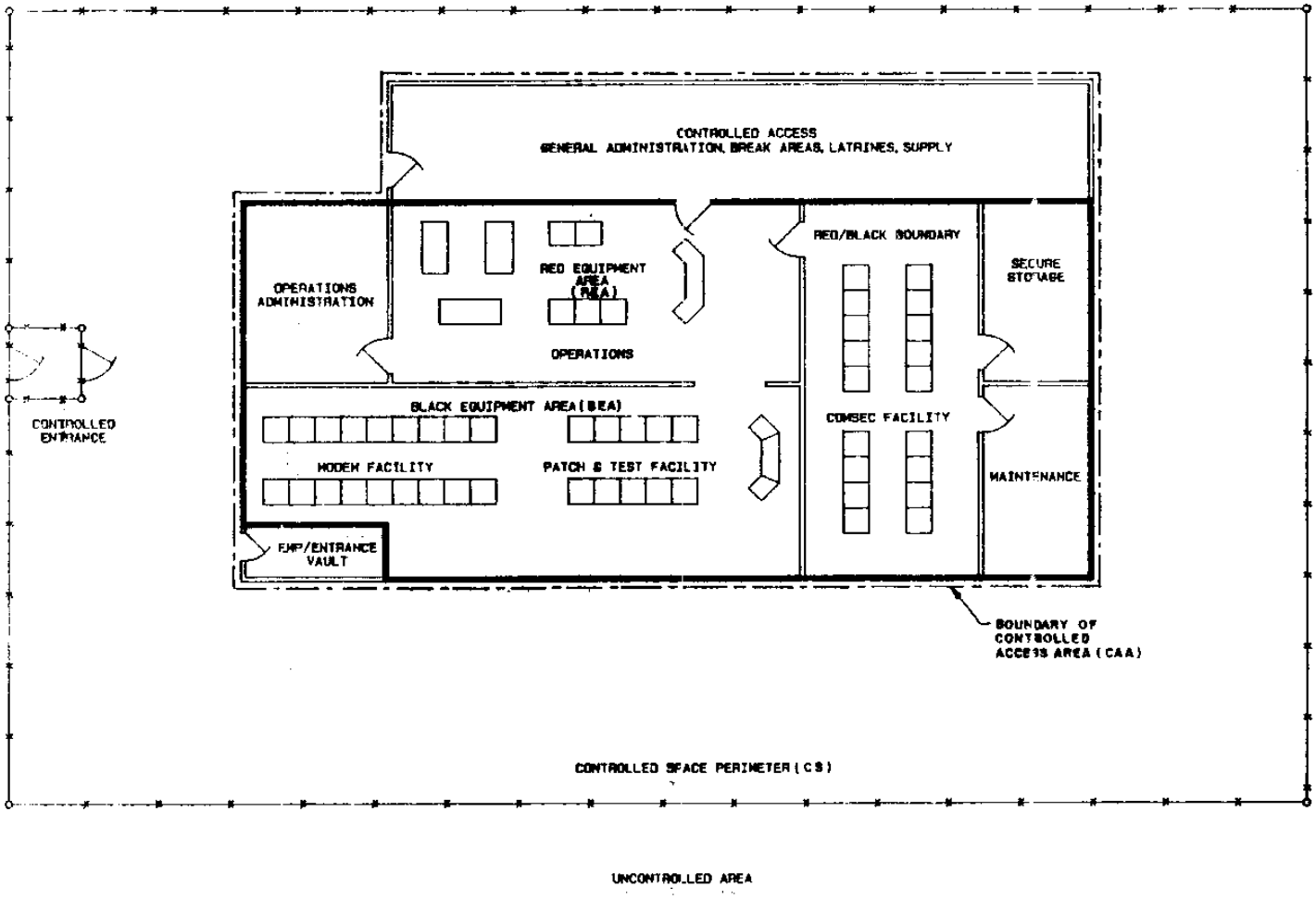


FIGURE 1. Typical facility.

4.1.1 System design verification. When a system or facility is designed or retrofitted, specific aspects are examined to determine the level of protection required. (See NACSI 5004 and NACSI 5005). The process involves developing a systematic approach to examine each aspect of the design to ensure it complies with the intended end result without compromising the information to be processed by the system or facility. Paragraphs 4.1.2 through 4.1.6 define areas which require constant review during the design process.

4.1.2 Environment. The geographical and geopolitical environment in which the facility exists must be defined. This includes examining the physical plant with regard to the level of security required, which defines the measures needed to protect the facility. Environment includes definition of power source, collocated activities (both mission and nonmission), existing security measures, and a review of service directives to identify additional requirements. The designer should consult NACSI 5004 and NACSI 5005 for procedures which define the threat environment.

4.1.3 Area boundaries. Based on the environmental review, boundaries are established for the various security levels needed. Subsequent reviews ensure these boundaries have been maintained.

4.1.4 Processing requirements. All functions in the mission should be reviewed to determine which area of the facility will contain those functions and what equipment will satisfy those functions.

4.1.5 Equipment and layout. A review of all equipment satisfying the mission requirements should be conducted to determine compliance with existing criteria, any special treatment required, or additional protective measures needed. This review may reveal additional requirements in other areas. Planned layouts can confirm that area boundaries are not violated.

4.1.6 Power, signal, and ground runs. Constant attention is required to ensure proper separation, isolation, and accountability. A grounding review ensures that all required paths exist and are effectively bonded, and that non-current-carrying conductors stay that way. Further, the review should verify the accountability of all conductors entering, caressing, or traversing the facility, and that protective measures for such conductors at all boundaries have been applied.

4.2 General guidance for power distribution. In general, the guidance in MIL-STD-188-124, MIL-HDBK-419, the National Electrical Code (NEC), and local building codes is adequate for power distribution where low-level balanced voltage digital signaling and TEMPEST approved equipment are used. If nonTEMPEST equipment and/or high-level signaling are used, separate RED and BLACK power distribution may be required. This separation must be as complete as possible and the isolation as high as practical. Power distribution must be designed and installed such that classified information cannot exit the protected areas via power lines that exit those areas. Power distribution must also be protected from external disturbances such as those caused by lightning or EMP/HEMP pulses. The design and installation of power in a facility is an integral r)art of the engineering effort. Consideration must be given to the source of power, types of distribution required, need for filtering, treatment of ducting, and special needs of the facility. Figure 2 depicts the typical power system. Guidance for power distribution in digital systems may also he found in FIPS PUB 94. The designer should be aware of the electrical codes and standards of foreign countries when designing facilities overseas. In such locations, the NEC may not be applicable. Details should be obtained from the appropriate facilities

engineers, civil engineers, or public work office.

4.2.1 Source. The source of power to a facility will determine the need for special treatments, particularly isolation and filtering. If at all possible, the prime generating source should be totally contained within the controlled space (CS). Since this is seldom possible, the designer must determine if power is a dedicated service feed or shared with other activities. That information will aid in the design of other elements of the power system.

4.2.2 Power systems. Power within a facility normally consists of a nontechnical system and a technical system (see figure 2).

4.2.2.1 Nontechnical system. The nontechnical system is provided to power air-conditioning, heating, lighting, and housekeeping functions. Normally, no special treatment is required other than the provisions of the NEC. However, it should be installed so that no equipment associated with the mission can be connected to it. The ancillary equipment served by the nontechnical system is transient producing. This equipment should he installed with sufficient electrical separation and isolation to prevent adverse effects on mission equipment. (See MIL-HDBK-411.)

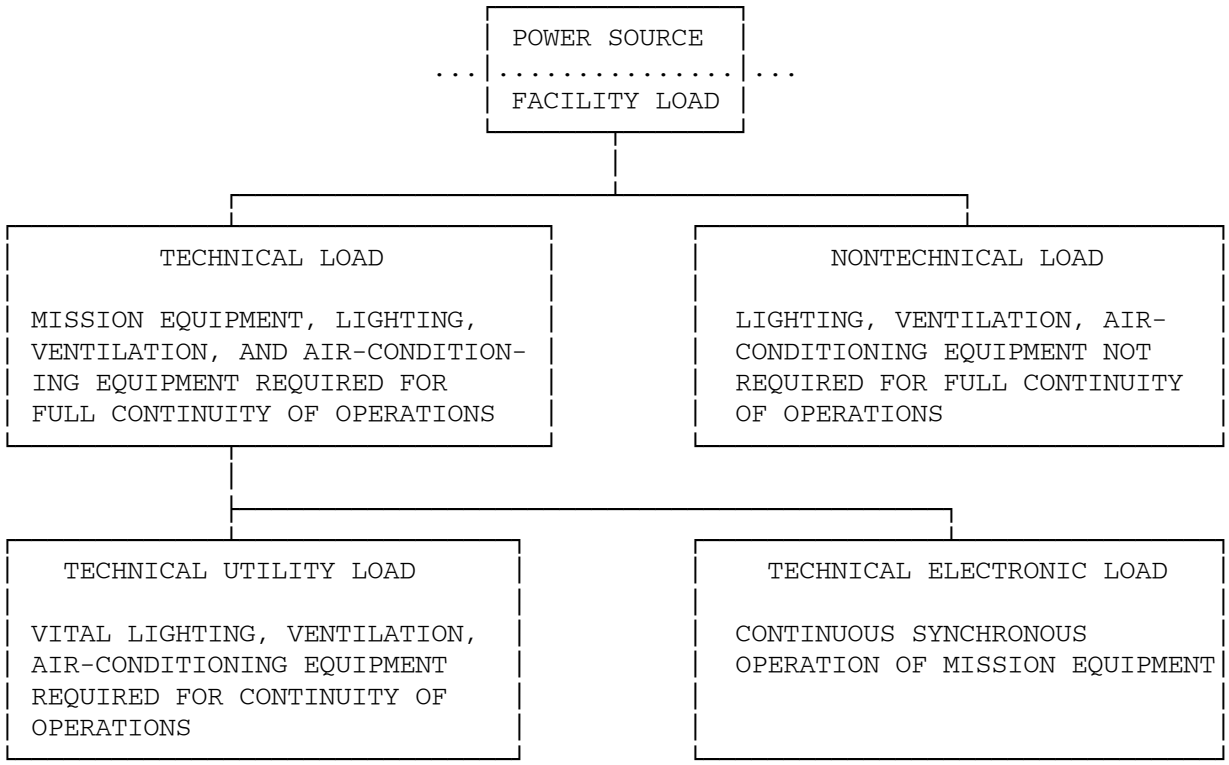


FIGURE 2. Power distribution

4.2.2.2 Technical system. The technical system is provided to power equipment associated with the mission. This includes any lighting and environmental equipment essential to system operation. If nonTEMPEST equipment is used as RED processors, the technical power should be divided into RED and BLACK power. RED power may be created by installing RFI/EMI filters on the power lines serving RED equipment, or by the use of dedicated motor generators (MGs).

4.2.3 Filtering. Filtering is a well established method of containing compromising conducted emanations. The methods of accomplishing this containment are as varied as the equipment being supported. The designer must consider the equipment in order to determine the facility requirement. All equipment which processes classified information should be filtered within the equipment enclosure. This allows the filter to be designed specifically to the parameters and characteristics of the equipment. If this has been accomplished, no other power filtering is required. If RED processing equipment does not contain filters and cannot be retrofitted to include filters, then filtered power panels are indicated. The service lines feeding the panel (each phase and neutral) must be provided with an appropriate size filter. BLACK processing equipment or utility equipment should not be powered from filtered panels. Where an entire facility has been provided with filtered power, BLACK equipment should not be terminated on the same panel as RED equipment.

4.2.4 Power panels. Other than the requirements of the NEC and local building codes, no special treatments of power panels are required. Within the limited exclusion area (LEA), panels serving RED equipment should be located within the RED equipment area (REA) and panels serving BLACK equipment should be located within the BLACK equipment area (BEA). In the REA, TEMPEST may indicate that RED panels should be RFI tight.

4.2.5 Ducting. All power distribution should be in metallic conduit, ducting, or wire way. This reduces the likelihood of magnetic fields from power interfering with equipment, and creates an electromagnetic (EM) barrier to stop free space radiation from coupling onto the power lines.

4.3 General guidance for equipment. For the purpose of this handbook, equipment will be divided into three general categories:

a. BLACK equipment, which can be located in a BEA, a controlled BLACK equipment area (CBEA), or a controlled access area (CAA).

b. Hybrid equipment, which by necessity, will be located in an REA. Hybrid equipment may have RED and BLACK inputs and outputs.

c. RED equipment, which by definition, will be located in an REA. Figure 3 depicts the complexity which can exist in a facility.

4.3.1 RED equipment. RED equipment is any equipment which processes classified information before encryption and after decryption, and should therefore be TEMPEST and physically protected. With the advent of computerized data processors, video processors, electronic message processors, and a host of other electronic information processing equipment, a traditional description of RED equipment no longer exists. RED equipment can be any type of device which can accept classified information by human input or from another RED device and perform some type of processing on that information. Certain procurements require the use of nondevelopmental items (commonly referred to as "commercially-available-off-the-shelf", Or "brand

name or equal"). Most of this equipment, when used as RED input devices, is not designed with TEMPEST protection in mind and therefore is not TEMPEST approved. Great care should be taken to provide the requisite protection to such devices. Grounding, bonding, shielding, physical isolation, filtering of all leads, and visual screening may be required in varying degrees and combinations. Each device must be evaluated separately, as well as the environment where it will he operated. In paragraph 5.3, installation concepts for a number of items of RED equipment are provided. The designer may wish to consult the cognizant TEMPEST authority to determine the availability of TEMPEST compliant equipment. TEMPEST compliant equipment is any equipment designed to NACSIM 5100, but not tested.

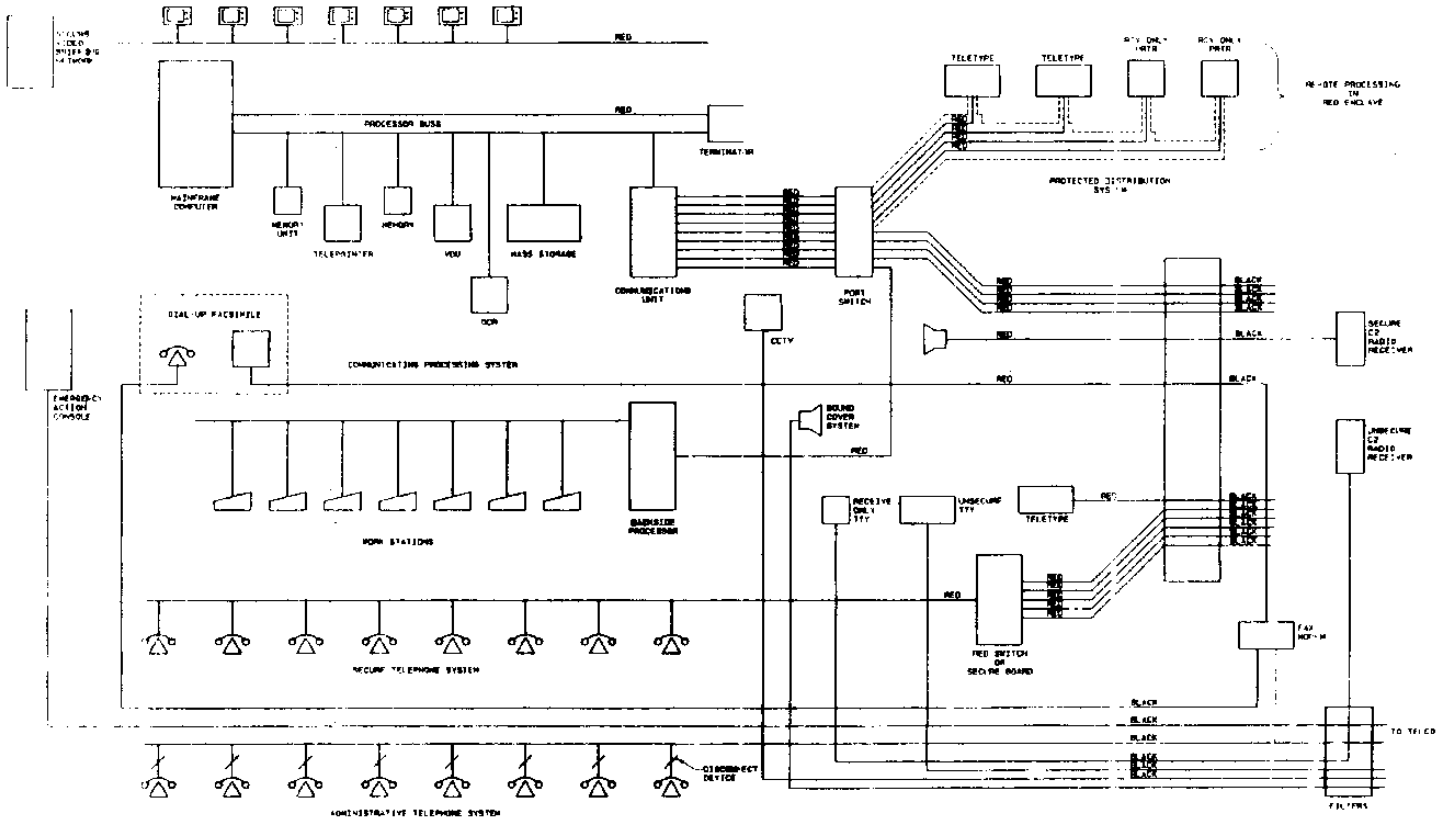


FIGURE 3. Complex RED equipment area.

4.3.2 General types of RED equipment. Any device with an information processing function can be used as RED equipment. Current commercially available telephone technology, coupled with inventory cryptographic devices, has been used to form switched secure voice systems in RED enclaves. In such cases, standard telephone instruments might be used as RED devices. Numerous micro-, mini-, or mainframe computers, as well as digital and analog facsimile devices, may be used as RED devices. Video transmitting and receiving equipment, with or without associated audio, may be classed as RED devices. Electronic/electric typewriters may be used as RED devices. There are numerous ancillary devices such as digital-to-analog or analog-to-digital converters, synchronizers, magnetic tape readers and recorders, and card readers/punches that may be classed as RED devices.

4.3.3 General techniques for RED equipment.

4.3.3.1 Teletypewriter devices. There is extensive use of teletypewriter devices throughout the Department of Defense (DoD). Advancements in technology have resulted in the introduction of numerous devices which incorporate microcomputer circuitry, tape recording/reproducing devices, and video display units (VDUs) to enhance the basic teletypewriter function. The type of equipment used and the operational environment will dictate the need for more stringent TEMPEST controls. Such controls might include additional shielding and separation from other equipment, and increased physical security such as visual screening of the VDU. Such additional treatment should be determined by the cognizant TEMPEST agency.

4.3.3.2 Secure voice systems. There are various types of secure voice systems being used within the DoD. Many of these systems are designed to work with unique telephone instruments and/or data and facsimile terminals which perform required control and indicator functions. Only approved equipment and configurations should be used as an integral part of these systems. There are systems, however, that are designed to be operated by using commercially available telephone systems. Any device in the system may be designated through a computer process as either a RED or BLACK terminal. Extreme caution must be exercised to ensure adequate protection of all equipment and wire lines. Thorough customer education must be provided to prevent possible compromise situations resulting from customer misuse. A RED telephone network should be totally contained within the CAA, but may have trunks coupled to the central office telephone exchange. These trunks should be encrypted.

4.3.3.3 Facsimile devices. Facsimile devices are of two basic types, analog and digital. Analog devices operate at a low speed and may require the use of an analog-to-digital converter to produce a digitized line signal that may be encrypted. New technology facsimile devices use digital signaling and do not require signal conversion prior to encryption. For either type, the principle RED/ BLACK installation practices include shielding, filtering, separation, and isolation.

4.3.3.4 Video devices. Video devices as RED processors are typically used in an area where the entire video distribution is among closely associated spaces within a single building or a small group of buildings. It is desirable to provide a protected distribution system (PDS) with the signals transmitted over one or more fiber optic cables (FOCs) within the PDS, thereby reducing the TEMPEST vulnerability of the system. (See NACSIM 4009.) However, the use of appropriate grounding, bonding, and shielding (CBS) for all wire lines within the system is still required. Some video devices may use radio frequency (rf) free space radiation between units instead of wire-line conduction between units. This requires that the signal be digitized and encrypted while in its baseband form. Remember, CBS is critical for this type of system.

4.3.3.5 Computers. This category includes a wide variety of devices from a microcomputer used as a word processor in a stand alone configuration to a large multicomponent, multiprocessing system which connects to varied types of terminals. Examples include moderate sized RED digital computerized telephone switches serving local areas, intrafacility computer networks with numerous work stations, or computer-aided design systems used for producing sensitive or classified drawings.

4.3.3.6 Ancillary devices. This category includes devices such as analog to digital/digital-to-analog converters, line controller units, crypto-bypass devices, line drivers, rate converters, rate buffers, synchronizers, and any other unit required between the user terminal and the encryption device. The common characteristic of an ancillary device is that it may be RED on both input and output and may not require any human attention during operation.

4.3.3.7 Storage devices. This category includes both on-line and off-line devices since the RED/ BLACK considerations are the same for both. It also includes any device in which classified information is stored in other than hard copy form, such as magnetic tape recorders/reproducers, magnetic disk, drum or card recorders/reproducers, and computer memories (magnetic or electronic).

4.3.4 Local area networks (LANs). When a LAN is designed or proposed for the purpose of processing classified information, the topology of the LAN must be determined in order to establish the protective measures required. Two topologies exist -- point-to-point and multipoint (may be called multipath or bus technology). Each requires different protection Additionally, the transmission media between LAN nodes becomes a significant issue in defining the topology.

4.3.4.1 Point-to-point topology. A point-to-point topology is characterized by dedicated paths between any two nodes. The paths are not shared (see figure 4). A point-to-point network may consist of any number of nodes. Each path will interconnect only two nodes. A node must have a path to a node with which it wishes to communicate. or must he switched through another node. This topology lends itself to being designed and installed using existing cryptographic devices to secure each path. Each node is installed using the RED/BLACK concepts defined in this handbook. Figures 5 and 6

depict point-to-point topologies that may be implemented using a private automatic branch exchange (PABX), or a broadband cable.

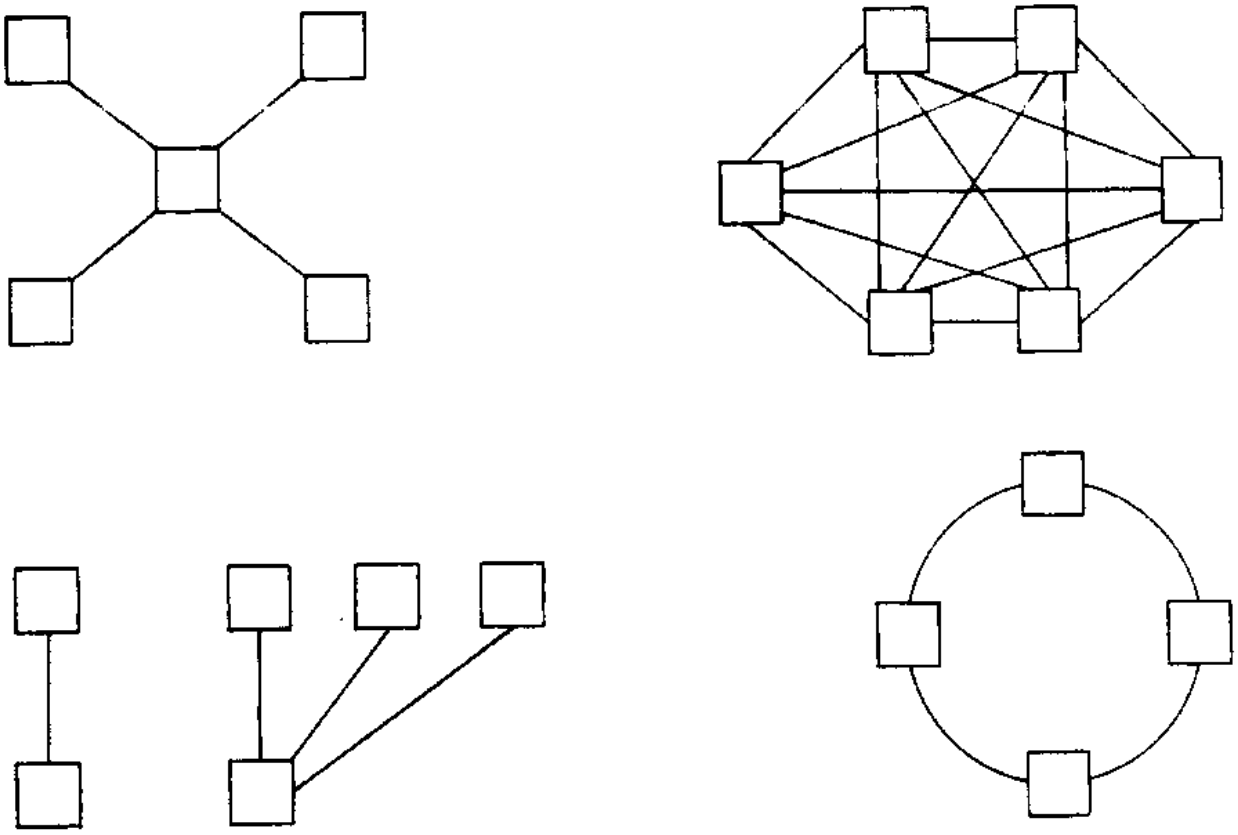


FIGURE 4. Point-to-point LAN topology.

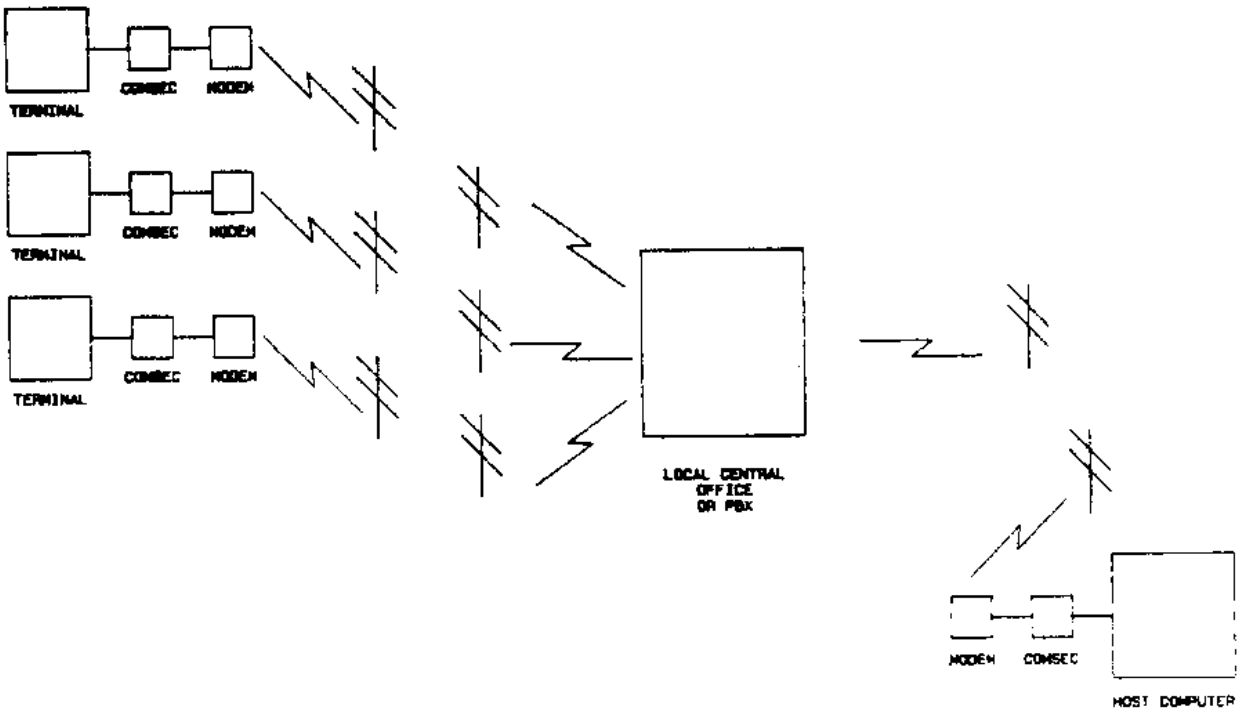


FIGURE 5. Point-to-point implemented through PABX.

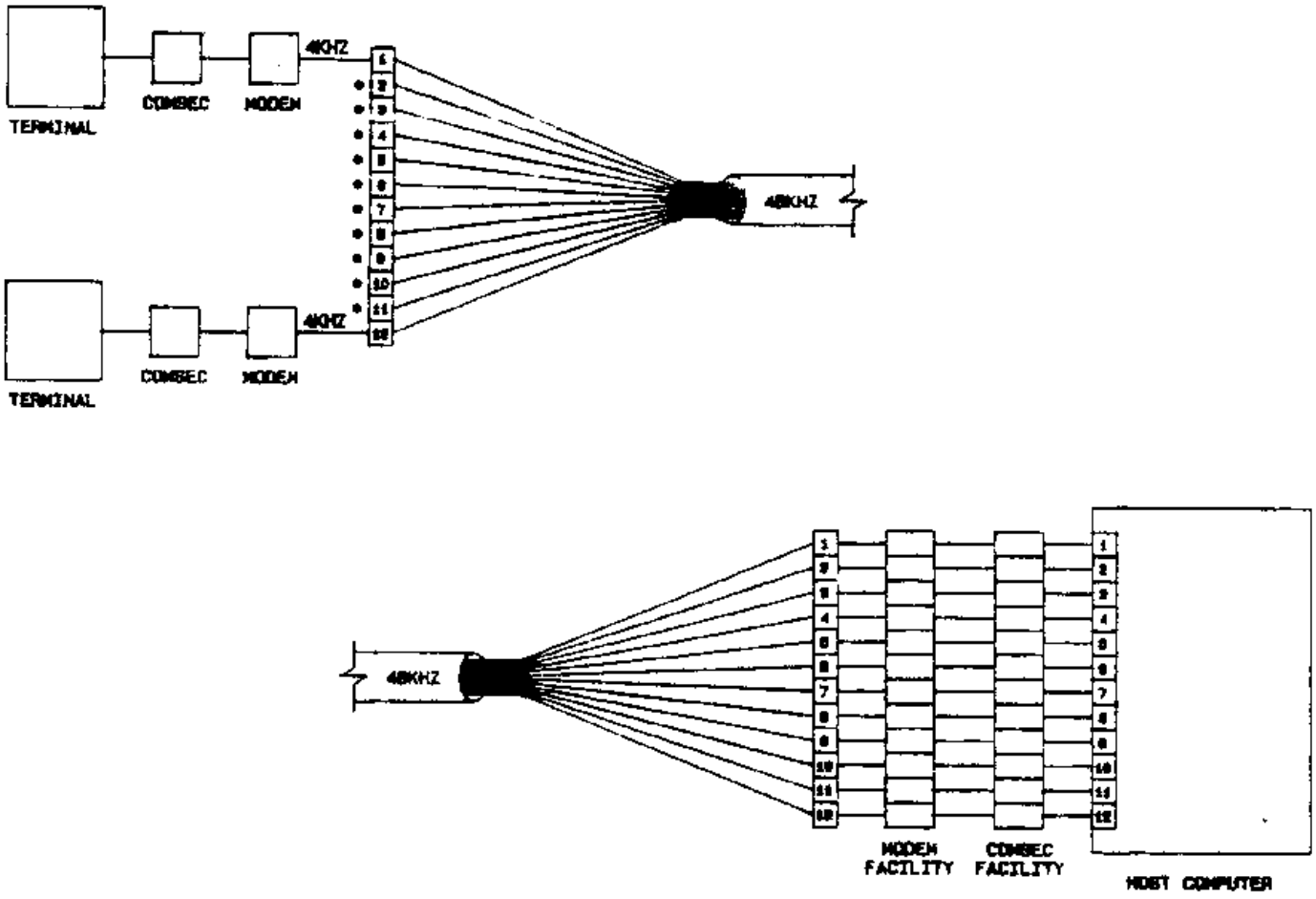


FIGURE 6. Point-to-point implemented through broadband cable.

4.3.4.2 Multipoint topology. The multipoint topology is typically implemented with all nodes interfaced to a single transmission medium (see figure 7). This configuration allows any node to communicate with any other node in the network. Present security technology does not permit such a network to be engineered in the RED/BLACK concept. The network, if installed to process classified information, can only be RED. All aspects of physical security must be applied. In facilities where the nodes are widely dispersed and the cable traverses an uncontrolled access area (U AA), the cable must be installed in a PDS. Installers are cautioned of an installation technique which, while being simple, may compromise the integrity of the cable shield. The technique uses a piercing tap to puncture the cable sheath and shield to make contact with the center conductor. These taps may be referred to as vampire taps. When the tap is removed, the puncture remains, leaving a hole in the shield. This hole could be an aperture for radiated emanations.

4.4 General guidance for signal distribution. The objective of signal distribution is to provide an organized scheme to transfer signals from the source to the sink in such a manner that:

a. RED/BLACK integrity is maintained.

b. Interference is not intercepted from other sources.

c. Interference is not created.

Figure 8 depicts a typical signal flow through a facility.

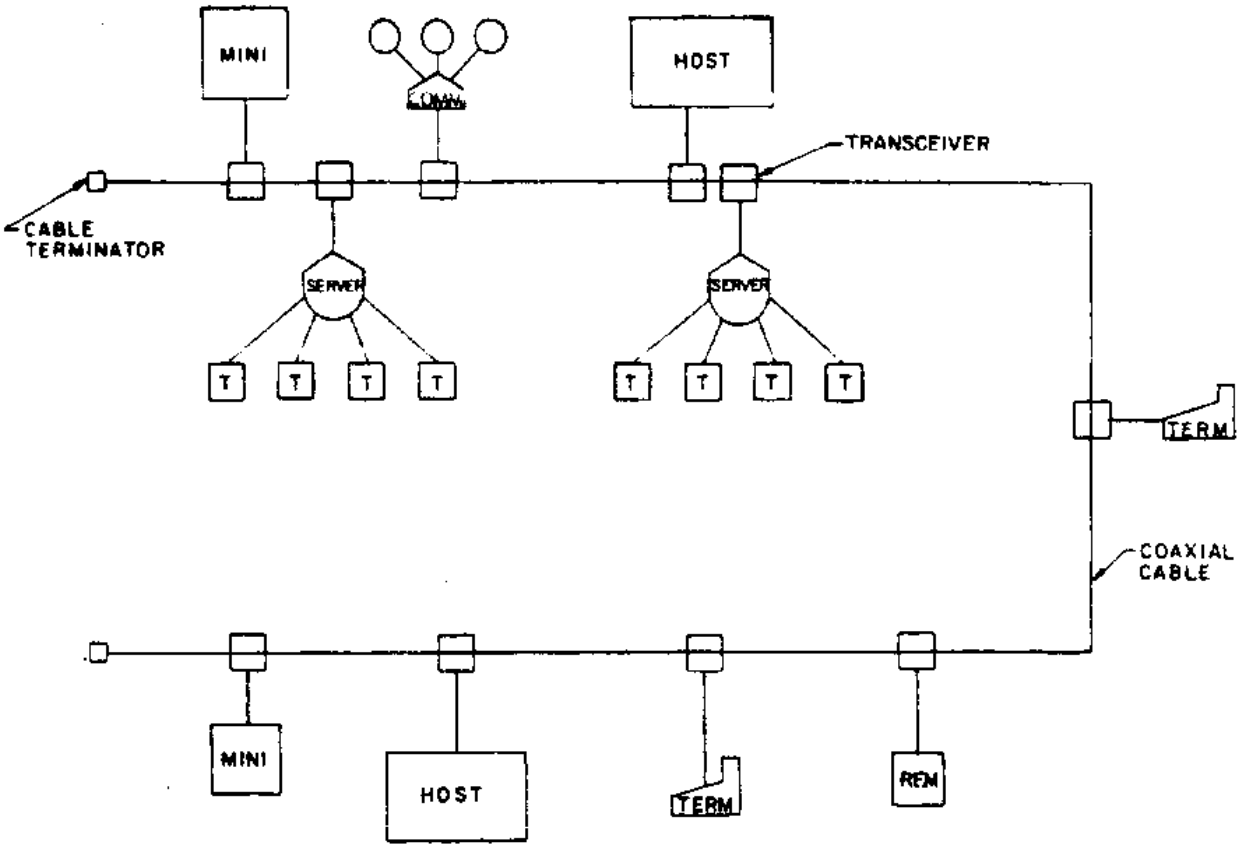


FIGURE 7. Multipoint topology.

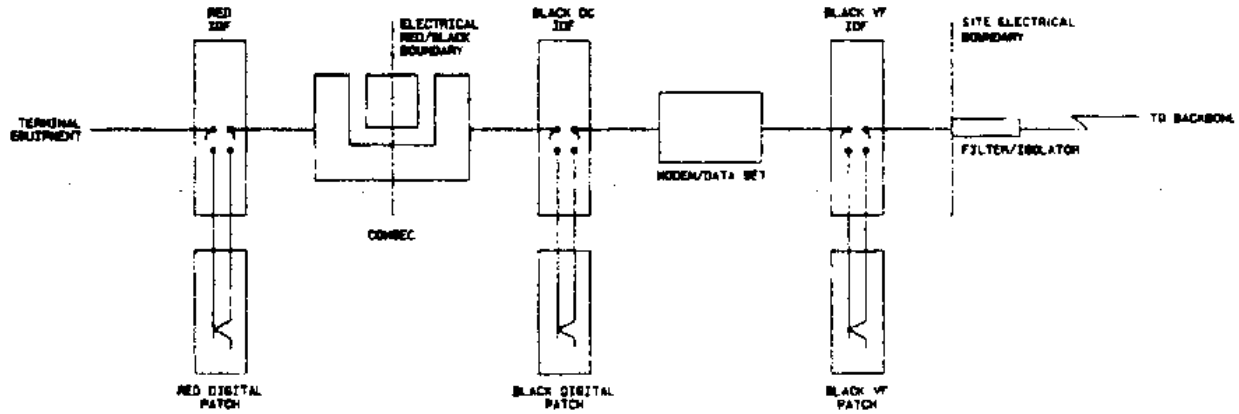


FIGURE 8. Typical facility signal flow.

4.4.1 Signal types. Signal distribution in a facility involves transmission of two types of signals -- analog and digital.

4.4.1.1 Analog signaling. An analog signal is defined as continuously variable in some direct correlation to another signal impressed upon It. In many facilities, quasi-analog signals exist as audio outputs of modems connecting the facility to the transmission medium, and the administrative telephone system. Such signals in a facility are in the voice frequency (VF) range of 300 to 4000 Hz. Other analog signals may exist within equipment reaching into the higher frequency ranges in specialized equipment such as magnetic tape transports, magnetic disk units, VDUs, or closed-circuit television. Specialized facilities may use radio with even higher frequencies, or use high frequencies in broadband LANS. The designer must use techniques which prevent cables carrying such signals from acting as antennas and thus transmitting or receiving signals. Grounding and shielding are essential in order to contain emanations, along with attention to proper cable selection, termination, and impedance matching.

4.4.1.2 Digital signaling. Digital signals are normally discontinuous, changing from one state to another in discrete steps. Digital signals represent the information being processed in a facility and may be used to modulate analog signals to transmit such information. Rate changes can typically occur in a range of 50 to several million bits per second. In the design of digital signal schemes, it is important to minimize the possibility of EMI by keeping: (a) voltage levels low, (b) all pairs properly terminated, and (c) shields properly closed and grounded.

4.4.2 Patching. Patch panels are provided in facilities to allow equipment and signal paths to be interchanged in the event of failure or alternate routing. Separate patching is provided for BLACK digital/analog, RED digital/analog, and the RED signals of special security levels. Panels are installed with protective schemes that assure patching cannot be accomplished between different types of signals or communities of interest.

4.4.3 Facility entrance plates. Facility entrance plates provide the demarcation point between the facility and the external transmission media. It is at this point that surge, transient, EMI/RFI, and EMP/HEMP protective measures are applied to signal lines entering and egressing the facility.

4.4.4 Distribution frames (DFs). DFs are points within the facility where cables are interconnected to equipment or other cables. DFs may be provided for BLACK analog, BLACK digital, RED analog, or RED digital terminations. Terminations may be made using connectors and plugs, crimped taper pins, wire wraps, solder wraps, or insulation displacement techniques.

4.4.5 Distribution planning. Distribution of signal cable in a facility is designed to ensure tile proper segregation and integrity of signals. It is a critical part of the RED/BLACK concept. The proper segregation of RED and BLACK signals is best accomplished by planning each cable run from source to sink. If the facility is viewed as a series of concentric rings, each defining a boundary, accounting for each signal run to a boundary before going to the next boundary should ensure RED/BLACK integrity. All cabling should be distributed in ducts, conduits, cable trays, or ladders. Separate runs are provided for RED and BLACK signals, with special attention to physical separation when such ducts/conduits must parallel each other. The use of ducts provides physical protection, ensuring control of separation and routing, while also providing a degree of shielding. In some instances, RED duct runs must egress the LEA and traverse a UAA. Such runs require a PDS. Guidance for a PDS is contained in paragraph 5.7.3.

4.4.6 Filtering. Filtering and isolation are used to ensure that only the intelligence intentionally placed on a line egresses the facility and that extraneous signals do not upset an operation. In the past, when most communications used analog transmission techniques, passive LC bandpass filters were used at the point of egress from the facility. This was known as shield point Isolation. Such filtering can still be used for analog signals. However, with the advent of digital transmission techniques and multilevel multiplexing, passive filters cannot he used for the mission bit streams. Filtering may not be indicated if: (1) TEMPEST approved equipment is used, (2) the line is encrypted, (3) proper RED/BLACK separation has been maintained, and (4) proper installation procedures have been used. Nonsecure lines supporting unclassified circuits and telephone lines may require filters. Where a facility has been designed to survive EMP/HEMP, all signal lines are equipped with surge arrestors, transient suppressors, filters, and other measures to prevent upset/burnout of equipment. Where passive filters cannot be used because of line speed/format, optical isolators can be used to provide isolation at the point of egress. Such devices typically function like repeaters, using opto-electronic coupling to provide the isolation. Some optical isolators, however, operate asynchronously, repeating any signal on the line within the electrical parameters of the device. This can be overcome by using clocking signals to gate the isolator. Clock signals should originate at the same point as the signal of interest; i.e., if the signal originates in the RED area, the clock should be RED. Such isolators may be used for all signal lines to aid in EMP or TEMPEST isolation if such devices use fiber optics between stages. In a shielded facility, the fiber optics would egress the LEA through waveguides-beyond-cutoff. In certain instances, signal lines originating in the REA must enter the BEA. These may be control lines or signal lines for nonsecure circuits in a switching system. In some cases, a RED/BLACK boundary needs to be established. Optical isolation inserted into all circuits crossing that boundary satisfies that need.

4.4.7 Special considerations. Because of the density of signal lines in a patch and test facility (PTF) and the unsecure nature of the administrative telephone system, the designer must consider the hazards associated with these areas. Paragraphs 4.4.7.1 through 4.4.7.3 present the special considerations that should be included in a facility design.

4.4.7.1 Patch and test facilities (PTFs). Most facilities will use patching equipment to allow swapping equipment and lines in the event of failure, or to provide alternate routing. Larger facilities also include provisions to manually or electrically configure testing equipment into circuits to monitor or test the circuits. Many of these facilities were designed using equipment and materials for technical control facilities. Some of these materials and equipment are satisfactory in an unbalanced environment, but are less than satisfactory in a balanced environment. Interconnect and distribution frames also present problems in properly maintaining shielding of signals. Crossconnecting in such frames also presents a hazard of creating antennas capable of radiating or receiving at higher frequencies. When designing and installing such facilities, the following guidance is given:

a. Provide separate patching facilities for RED and BLACK signals, and for BLACK digital and BLACK analog.

b. Provide separate DFs for each kind of signal group.

c. If RED communities of interest include nonsecure, collateral, and compartmented communities. separate patching and DF facilities are required. If this situation exists in a small facility, unique wiring

of such circuits may be used, subject to approval by the cognizant TEMPEST agency.

d. Provide patching and distribution facilities that can accommodate every signal and return line. Past practices typically did not include patching return lines.

e. Design the crossconnects to be as short as possible.

f. If automatic line quality monitoring is incorporated, provide separate monitoring equipment for RED and BLACK lines.

4.4.7.2 Administrative telephones. The treatment of administrative telephones is discussed in other portions of this handbook (see 4.8). This paragraph emphasizes certain installation criteria. First, telephone cable is installed in completely separate distribution facilities. Second, if party lines or shared lines are used within the LEA, such lines will not be shared with users outside the LEA. Third, all telephone lines may require filters or isolators. See appendix D for treatment of special features.

4.4.7.3 Fiber optics. Many facilities are using FOC to interface equipment. Because FOC does not use an electrical medium, it is relatively immune to the effects of EMI/RFI. Further, its radiation characteristics are negligible. Therefore, it is ideal for signals caressing an LEA and for interconnecting LEAs separated by a UAA. However, the designer and installer must provide physical protection and security to the cable. The designer must also include EMP protection at facility penetrations such as waveguides-beyond-cutoff for FOC that penetrates the facility entrance plate or other EMP barrier. The designer must also be aware that FOC is susceptible to fogging during an EMP and must be protected.

4.5 General guidance for the use of filters and isolators. The function of filters and isolators is similar to that of shields -- the attenuation of undesirable signals which attempt to pass through. Filters and isolators are applied to conducted signals, while shields are used against free space radiated signals. Filters attempt to block signals by shunting to a return path, thus reflecting the unwanted signals back to the source. Isolators attempt to present an open circuit to unwanted signals. Engineering considerations for the use of filters and isolators are somewhat dissimilar because of the differing mechanisms used to perform these functions. Because a filter operates by shunting the interfering or compromising energy to a return path and reflecting it back to the source, the path provided to the return must (a) be able to carry the amount of current which may be delivered, and (b) present minimal impedance to ground to the shunted current at all frequencies of interest. When a filter is used at the point where a conductor passes through a shield, the desired effect is accomplished by directly bonding the filter return (usually its chassis) to the shield. Isolators, conversely, shunt no current, but must he able to withstand whatever voltage may develop across the internal open circuit. Isolators connected to lines which may carry lightning or EMP transients will be subjected to considerable stress (see 4.6). In general, the external barrier of a facility should use filters (preceded by surge arrestors) in preference to isolators, because of the difficulty of preventing arcing when a large incoming voltage transient encounters an open circuit. Figures 9, 10, 11, 12, and 13 provide general information on filter function.

4.6 General guidance for grounding, bonding, and shielding (GBS). Control of compromising emanations, EMP/HEMP protection, and RED/BLACK isolation depends fundamentally on proper CBS. MIL-HDBK-419 provides a detailed discussion of GBS theory and practice. MIL-STD-188-124 mandates the requirements for long-haul and tactical communications facilities. The

latest version of these publications should be referred to for amplification of the principles underlying the following discussions.

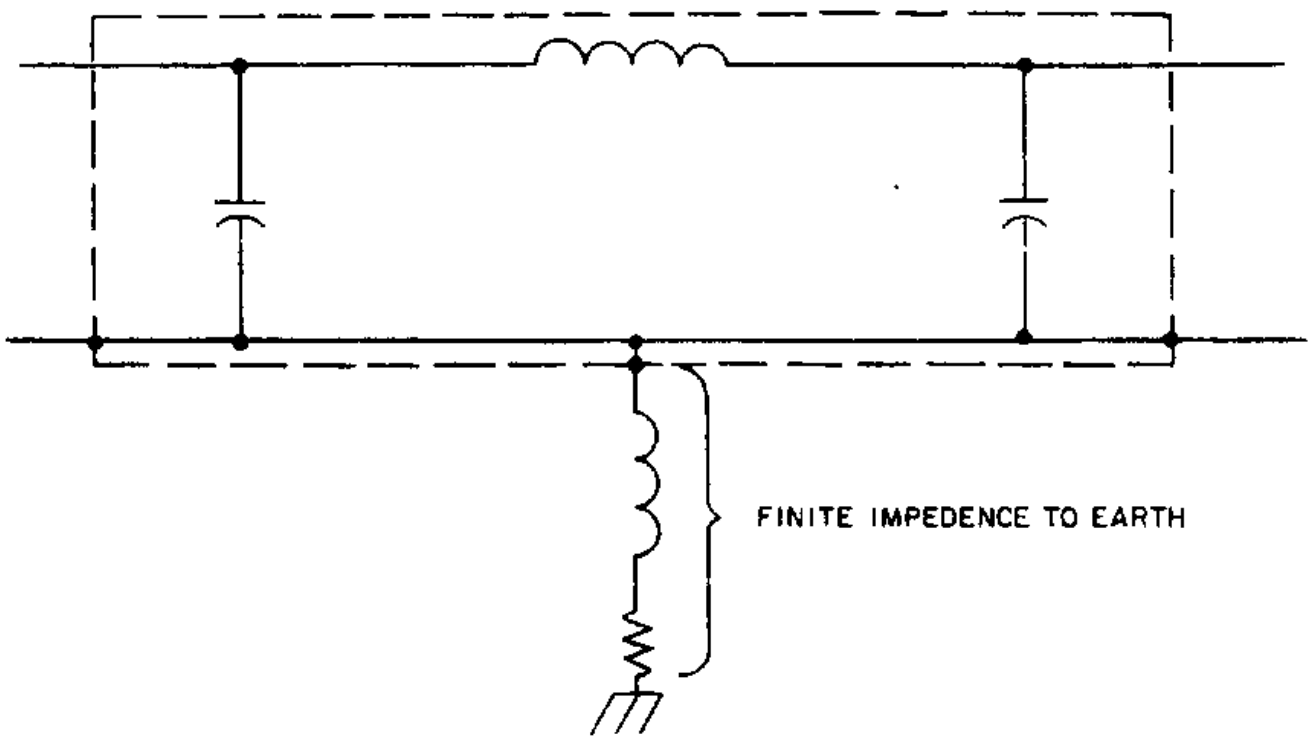


FIGURE 9. Typical signal or power-line filtering.

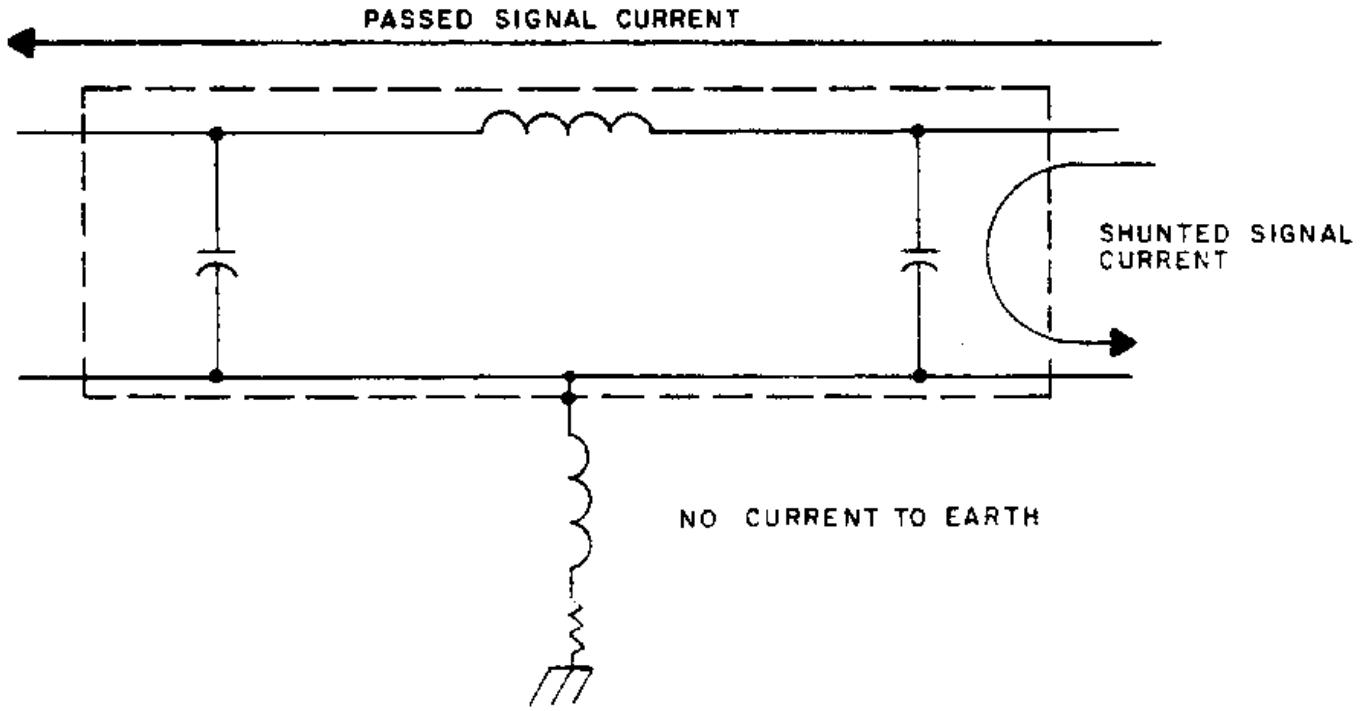


FIGURE 10. Normal filter operation.

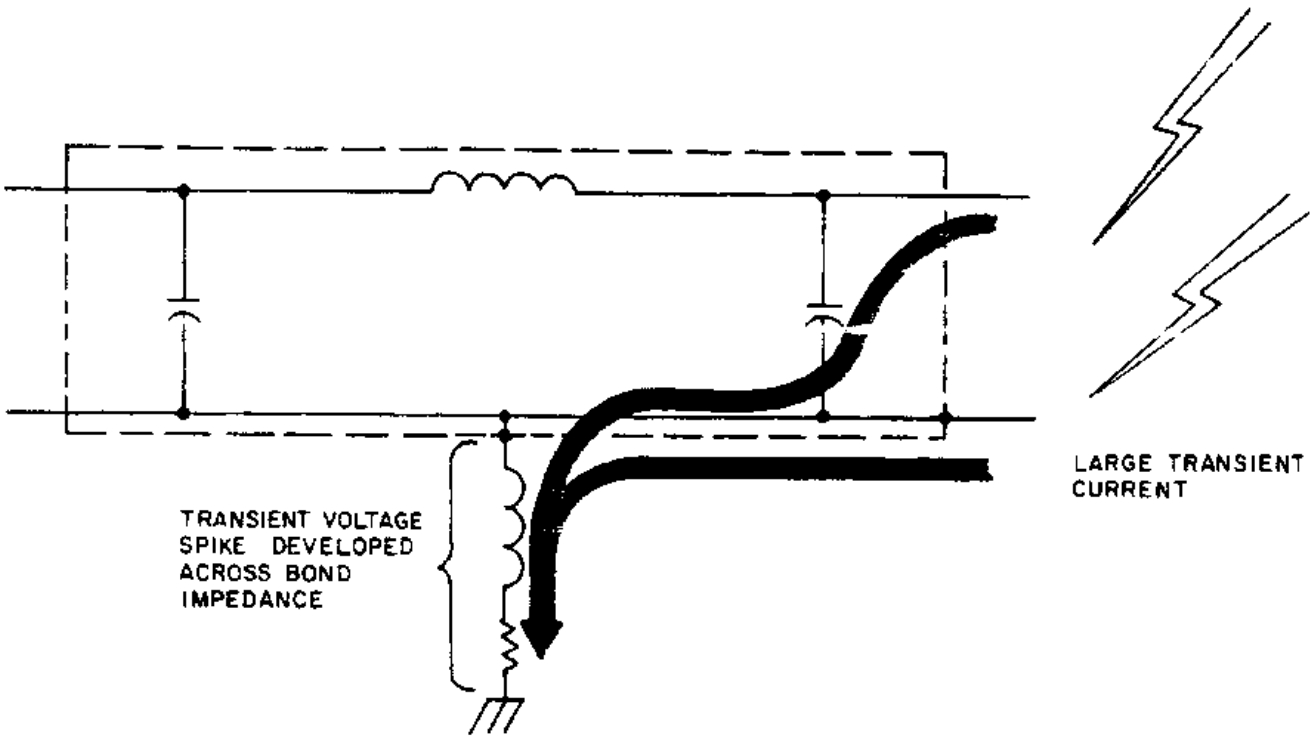


FIGURE 11. Filter transient operation.

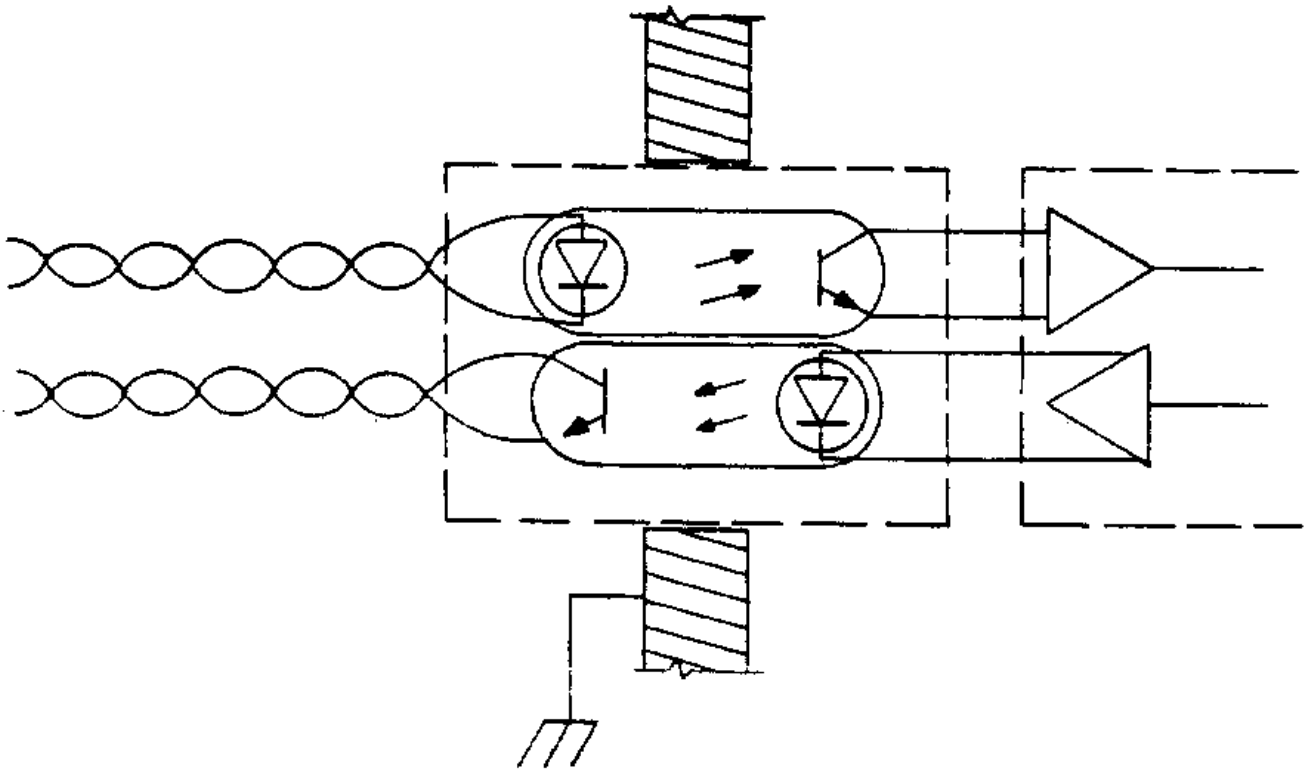


FIGURE 12. Typical optical isolator operation.

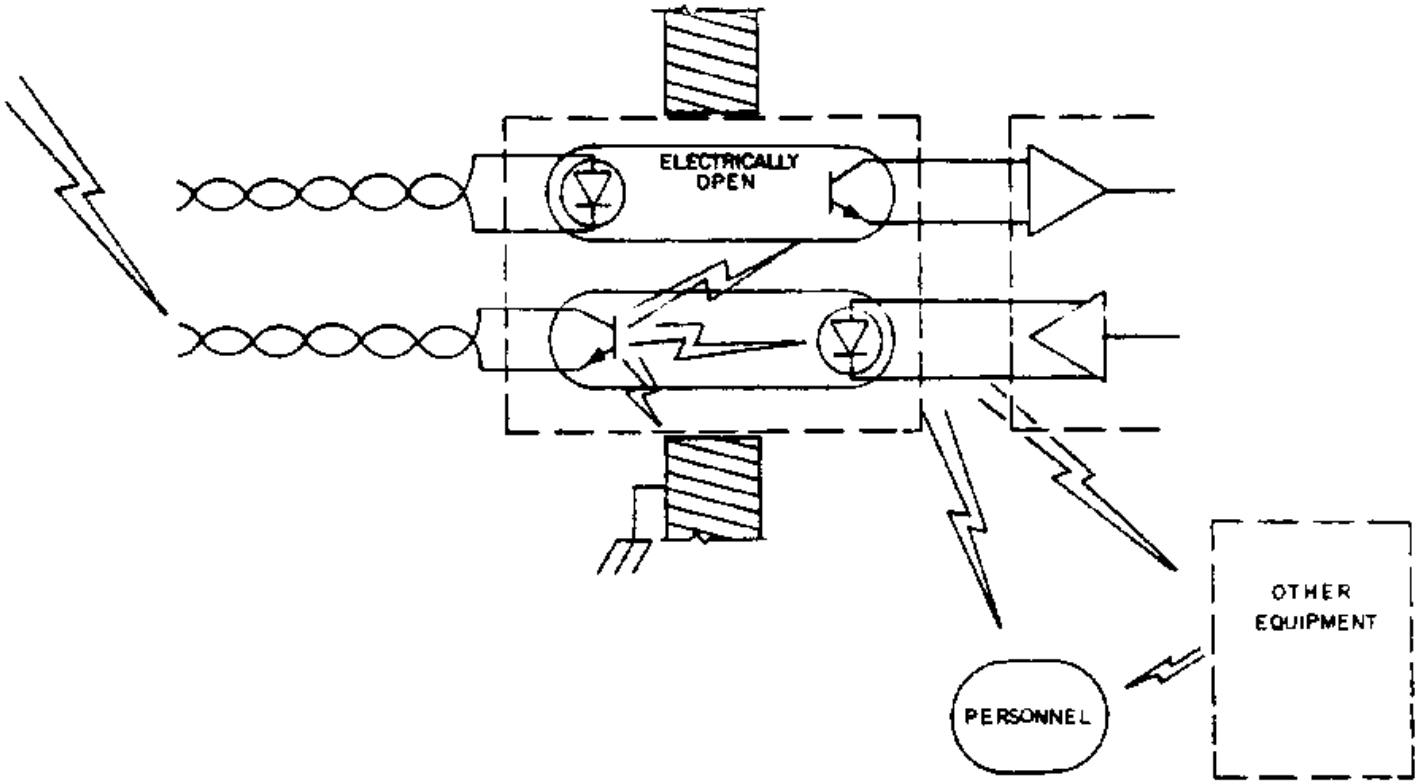


FIGURE 13. Uncontrolled arcing.

4.6.1 Grounding. Proper understanding of what "grounding" means is essential to engineering an effective grounding system. For signals, ground is merely an agreed-upon potential to which signal voltages may be referenced. It is not necessary, may not be desirable, nor in some cases be possible, to cause signal return currents to flow through the earth. The equipotential ground plane or ground bus providing the signal ground reference, however, is returned to the earth electrode subsystem (EESS). This is done to provide a dump for induced high currents. Other sources of current are at some potential relative to earth, and these currents must be provided a low impedance path to the earth. Examples include lightning, EMP, and power system fault currents.

4.6.2 Bonding. Bonding means connecting two conductors in such a way that the impedance through the connection is not appreciably greater than the impedance in the conductors themselves. Welding is the preferred bonding method. Soldering is acceptable where the bond will not carry fault protection for ac power, lightning, or EMP/HEMP currents. Pressure bonds such as split bolts can be used with proper rare, but are not recommended. Bolts require constant checking for tightness.

4.6.3 Shielding. Shields are used to attenuate electrostatic, magnetic, or EM fields. Ferrous metals are required to contain magnetic fields. Nonferrous metals are sufficient to exclude or to contain an electrostatic field. To be completely effective, a shield must be closed and grounded.

Shields should provide protection to comply with criteria in NACSEM 5204.

4.6.3.1 Facility shields. When a facility shield is required, it should be designed and installed using EMP guidelines, as well as those for containing compromising emanations. Consult the Defense Nuclear Agency for EMP guidance.

4.6.3.2 Cable shields. Al) cables in a facility (signal and power, RED and BLACK) should have at least an overall nonferrous circumferential shield. In addition, ferrous shielding should be used for high-level signals, or where indicated by TEMPEST tests. All cable shields shall be closed at both ends by bonding the shield circumference to the equipment enclosure (case, rack, etc.). A circumferential bond through a connector is achieved by using a connector which has a conductive shell that makes 360-degree contact with both the shield and with the mating connector. The requirement for an overall shield may be satisfied by complete enclosure within conduits, ducts, and equipment cabinets.

4.7 General guidance on physical security. The purpose of physical security Is to make access to a facility so difficult that a potential intruder will be (a) thwarted in attempting penetration, or (b) apprehended should the attempted penetration be successful.

4.7.1 Scope. It is not economically possible, nor theoretically necessary, for every facility that processes classified information to achieve the same degree of physical protection. How much physical protection is prudent in any particular case depends on factors such as type of facility, classification level of information stored/processed, threat of hostile intelligence forces, geopolitical climate of the area, location of the facility, and existing physical security measures.

4.7.2 Objectives of physical security. Physical security programs are designed to prevent unauthorized access to classified facilities, equipment, material, and documents, and to protect against espionage, sabotage, and theft. Physical security provides protection against human intelligence (HUMINT) and images intelligence (IMINT). By protecting vital communications and similar equipment, physical security also provides protection against some aspects of signals intelligence (SIGINT). (See JCS Pub 1.)

4.7.3 Facility security. Security of a facility begins by establishing a CAA within the facility in order to control access to classified information. Figures 14 and 15 are representations of this concept.

4.7.4 Audio security. Audio security is implemented to suppress the possibility of classified conversations being intercepted by clandestine means. Sound cover systems, special treatment of administrative telephones, and acoustic suppression techniques within buildings are the principle methods of audio security.

4.7.5 Intrusion detection. Intrusion detection systems (IDS) use sensors to monitor specific conditions within a CS and to alert security personnel when an undesirable condition exists. Guidance for such systems is defined by service/agency directives. The design may, in some cases, be incorporated into the facility cable design and may require protection as defined in this handbook.

4.7.6 Technical security. Ducting, wire ways, or race ways in a facility may require protection to prevent the introduction of clandestine devices. If ducts that contain transmission media, transporting classified plain text information, traverse nonsecure areas, then specific protection is mandated, such as a PDS.

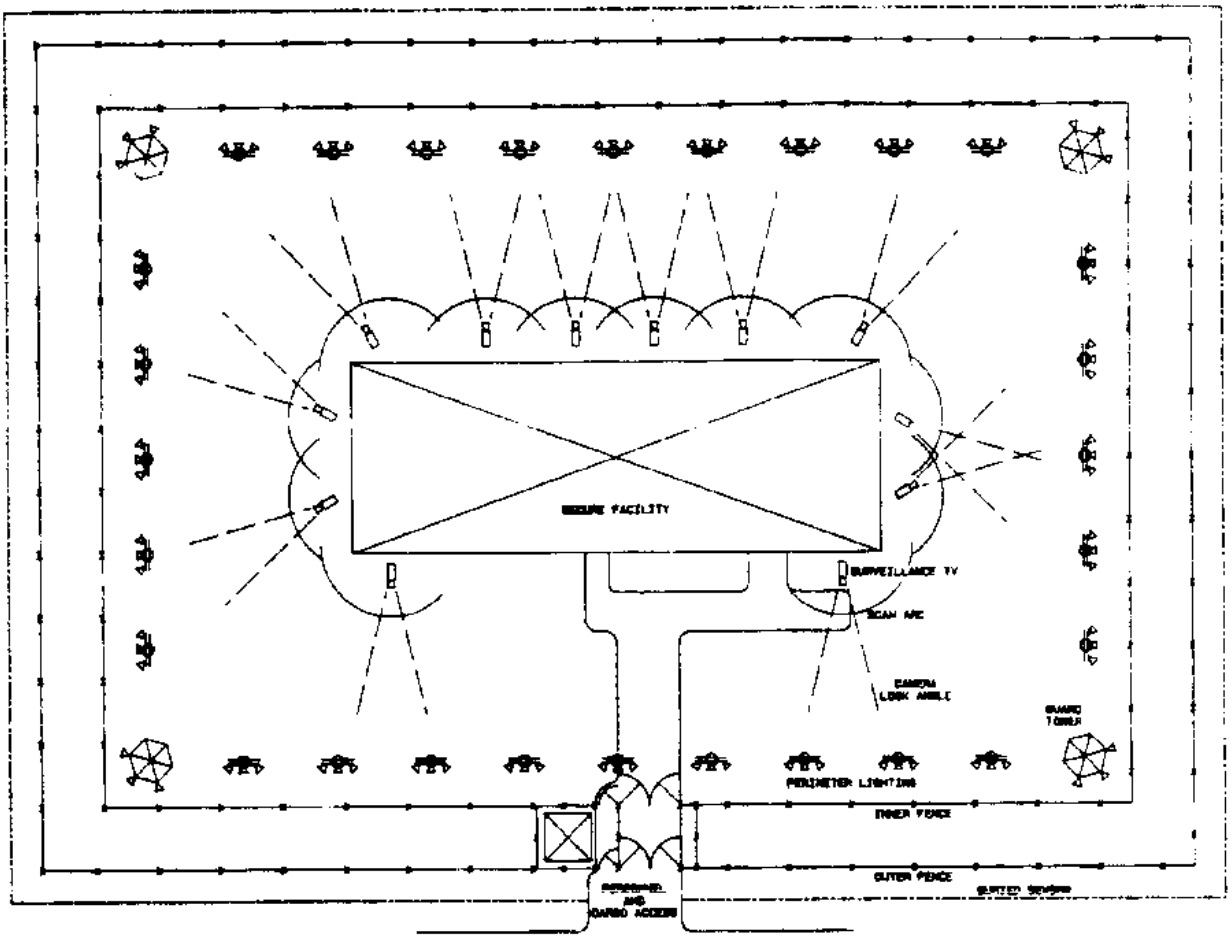


FIGURE 14. Facility security (exterior).

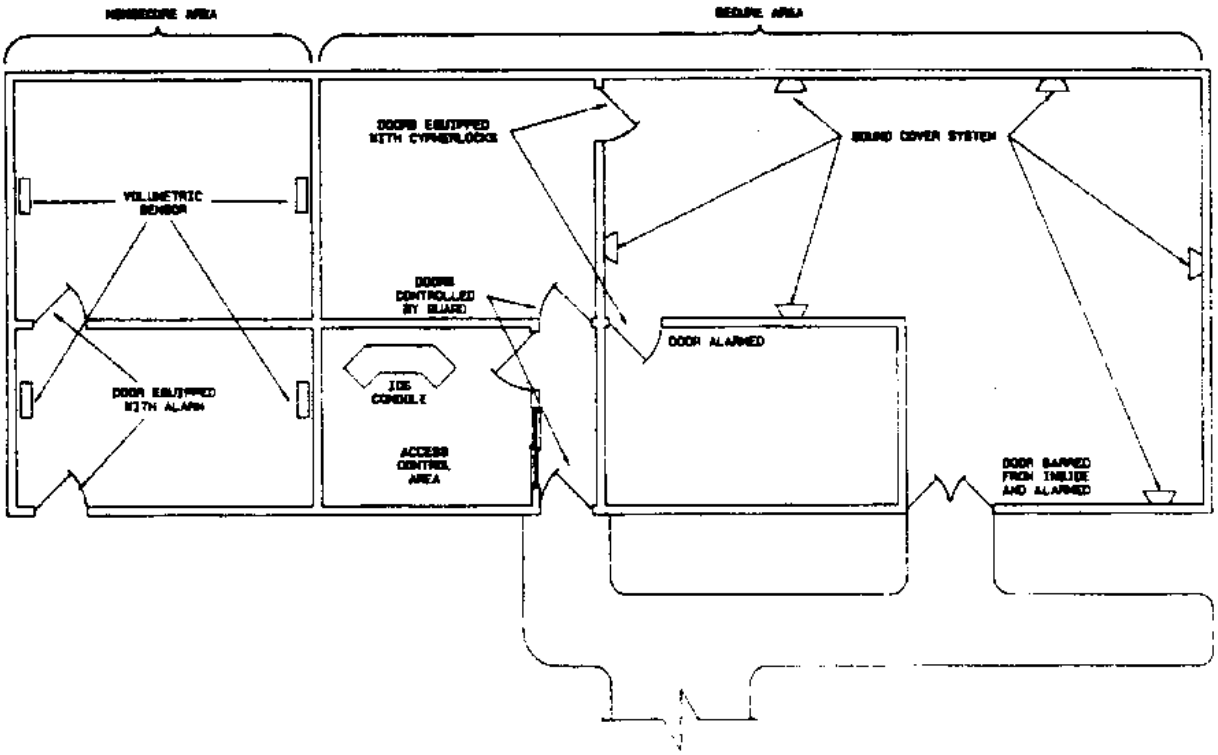


FIGURE 15. Facility security (interior).

4.8 Administrative telephones. The administrative telephone system in a facility must be installed so that signals emanating from RED processors cannot couple onto egressing lines, and classified conversations cannot be monitored during on-hook conditions. The design and installation must assure total separation of telephone signal lines from all other signal Disconnect devices, noninductive ringers, and speech suppression techniques should be used to prevent the telephone from being used as a fortuitous, surreptitious probe into the LEA.

5. DETAILED GUIDANCE

5.1 RED/BLACK system design. RED/BLACK system design begins with definition of areas, barriers, risks, and system functions. Paragraphs 5.1.1 through 5.1.2.5 define such issues. The designer should consult with the cognizant security authority and the cognizant TEMPEST authority during this phase of the design to ensure compliance with current directives.

5.1.1 Physical and electromagnetic (EM) barriers. The central requirement for a RED/ BLACK system design is the security of the information processed and of the facility assets, both personnel and equipment. Achieving this security requires that barriers of an appropriate design to erected to prevent the escape of information, injury to personnel, and damage or destruction to the equipment or facility. These barriers are of two types: physical and electromagnetic.

5.1.1.1 Physical barriers. The facility must have at least one physical barrier at the perimeter. It may require internal physical barriers to limit access within the limited exclusion areas (LEAs) (see 5.7). Physical barriers must be designed to serve three purposes. First, protect the facility assets from physical harm. Second, prevent covert physical access to any classified information contained within the facility. Third, ensure that the EM barriers are not compromised (i.e., that the earth electrodes in the grounding system are not degraded or tapped, or that pickup devices are not introduced within the volume protected by the EM barrier).

5.1.1.2 EM barriers.

5.1.1.2.1 EM barrier functions. Within a RED/BLACK facility, EM barriers exist to contain or exclude two EM hazards. The barriers must contain any compromising emanations produced by the information processing equipment, and exclude any external EM disturbances, whether natural (e.g., lightning) or man-made (e.g., EMP/HEMP). EM barriers designed using this handbook will serve these functions because these functions are interrelated.

5.1.1.2.2 EM barrier components. The EM barrier of a facility consists of a perimeter barrier and several internal barriers. The barriers exist to isolate RED power and signals from BLACK power and signals, and to reduce the ambient level of EM transients and noise to a level tolerable within equipment.

5.1.1.2.3 Perimeter EM barrier. A perimeter EM barrier is made up of the following components:

a. Facility entrance plate.

b. Power entry.

c. Utility entrance.

d. Signal entry.

e. Facility ground system.

f. Earth electrode subsystem.

5.1.1.2.3.1 Facility entrance plate. All facilities designed using this handbook should use a facility entrance plate, whether or not a facility shield is installed. All conductors entering the facility shall pass through this plate. This plate is connected via a low impedance path to the low impedance earth electrode subsystem (EESS). This plate provides an ideal place to decouple compromising emanations from conductors egressing the facility and provides a low impedance shunt for lightning and electromagnetic pulse (EMP)/high-altitude electromagnetic pulse (HEMP) transients to earth to prevent them from entering the facility.

5.1.1.2.3.2 Power entry. The power enters the facility as described in paragraph 5.2. Terminal protective devices (TPDs), installed on all current-carrying conductors, are installed to provide a low impedance path for shunted current to earth via the facility entrance plate. This may often be best accomplished by bonding the ground electrode of the TPD directly to the facility entrance plate. The TPD must be installed in the power lines as near as possible to the entry plate to minimize the lead length which may carry high power transients (lightning or EMP) within the facility. Where motor generators (MGs) with nonconducting shafts are installed, the technical power is effectively isolated from conductors caressing the facility. An uninterruptible power supply (UPS) may also provide isolation between the source of power and technical power load, as well as isolating differing classes of loads where a separate UPS serves each load. Installation of an UPS also provides continuity of operation in the event of sustained disruption of utility power.

5.1.1.2.3.3 Utility entrance. All utility pipes (water, fuel, etc.) shall enter the facility through the facility entrance plate. Metal pipes are circumferentially bonded to the plate. If the facility is shielded, plastic pipes should pass through the plate via a waveguide-beyond-cutoff which is circumferentially bonded to the plate. (A waveguide-beyond-cutoff is a metallic pipe which has a length that is five times its diameter.) Any large ducts, such as air ducts, which enter the facility are grounded at the entry point and have waveguide-beyond-cutoff honeycomb installed across the entire cross section of the duct at the point of entry. This is in addition to physical security requirements.

5.1.1.2.3.4 Signal entry. All signal cables, whether used for data, timing, control, telephone, or any other purpose, enter the facility through the facility entrance plate. All cables should be shielded within the facility. The shields of all cables passing through the facility entrance plate shall be circumferentially bonded to the plate. (Shielded connectors are permissible where the mating surfaces make a 360-degree contact and the connector mounted on the plate is circumferentially bonded to the plate.) The signal conductors passing through the plate are either filtered or isolated, and protected by surge arrestors and other protective devices. It is important that the shunting conductor of the filters and surge arrestors have a low impedance path to the entry plate.

5.1.1.2.3.5 Facility ground system. The facility ground system serves to attenuate both internally generated emanations and external disturbances, but not to the extent that would be achieved by shielding the facility. The ground resistance should not exceed 10 ohms. (Design objective, MIL-STD-188-124.)

5.1.1.2.3.6 Earth electrode subsystem (EESS). The EESS provides an essential part of the low impedance path to earth for shunting each referenced disturbances such as power-line faults, lightning, and EMP/HEMP. It typically consists of a ring ground around the facility, augmented by an

array of varying length rods that are driven near the facility entrance plate to provide low impedance to earth.

5.1.1.2.4 Internal RED/BLACK EM barrier. The internal EM barrier between RED and BLACK equipment consists of several components:

a. The physical separation between RED and BLACK equipment, power and signal distribution facilities, and patch bays.

b. Shielding of all signal cables.

c. Encrypting or filtering all signal lines which connect RED and BLACK equipment. All cable shields must be grounded to the equipotential plane via a low impedance path at every convenient point.

5.1.1.2.5 Internal EM environmental barrier. The ambient EM environment in most information processing facilities contains transients of sufficient magnitude to disrupt the functioning of the processing equipment if allowed to couple into the internal circuitry of the equipment. Consequently, equipment is manufactured to provide some attenuation to such transients, mostly at the point where external power enters the equipment. This built-in protection is enhanced and expanded to provide a full barrier by providing a closed shield for the equipment that is properly bonded to the equipotential ground plane. The closed shield consists of the equipment case, metallic power distribution facilities, and the required signal cable shield, all of which must be circumferentially bonded together.

5.1.2 Facility design and layout. A sample layout of a medium-to-large facility is shown in figure 16. Several principles to be used in laying out any facility are summarized below.

5.1.2.1 Facility entry plate. Only one facility entry plate may be installed. If more than one were installed, tremendous currents would flow between them during a lightning strike or EMP, reducing the effectiveness of the facility EM barrier. Therefore, the mechanical room should be located adjacent to the EM vault, as shown in figure 16. These rooms should be located at that portion of the building which is nearest to a good site for the array of ground rods which must be driven into the earth to adequately ground the entry plate.

5.1.2.2 Power conditioning room. This room contains the UPS or MG sets, batteries for the UPS (one or more solid state online UPS), and the switchgear, and therefore should be adjacent to the EM vault.

5.1.2.3 Main distribution frame (MDF). The MDF is the.point of entry for signal cables into the technical area. The MDF should be located as near as is practical to the EM vault.

5.1.2.4 Equipment areas. Based on connectivity considerations, BLACK equipment is grouped together near the MDF, RED equipment is grouped together some distance away (as dictated by separation requirements), and crypto-equipment is located between the two. In many installations, there may be more than one RED equipment area (REA), BLACK equipment area (BEA), or crypto-area. The layout should group related equipment to minimize cable length and therefore reduce the probability of emanations and pickup of interference.

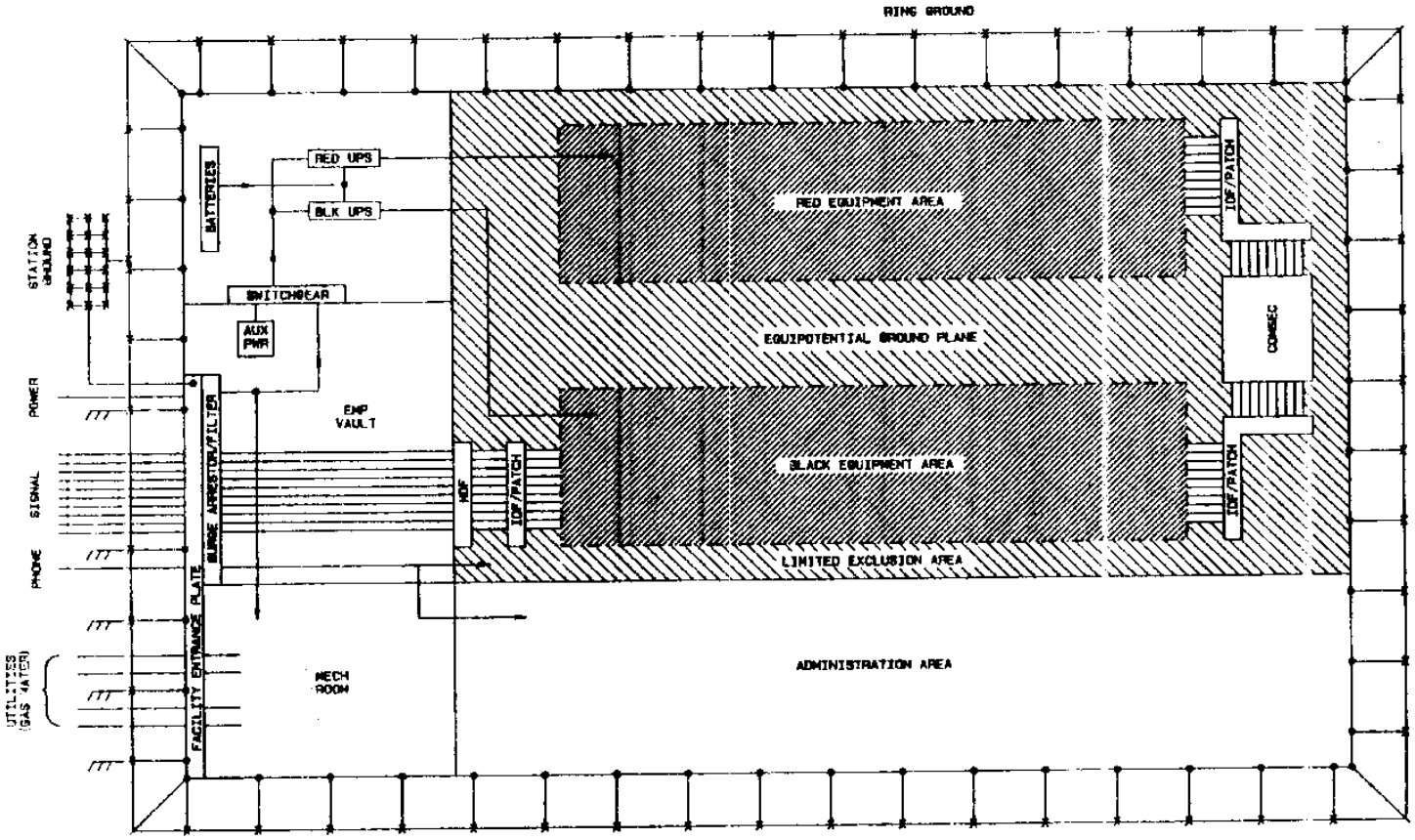


FIGURE 16. Large facility grounding system.

5.1.2.5 Equipotential ground plane. To function properly the equipotential ground plane must extend under or above all RED and BLACK equipment, distribution frames (DFs), etc. It will also he connected at regular intervals to the EESS and at every convenient point to metallic structural members of the building. The facility design should include specifications for where and how the plane will be installed and connected to the earth electrodes and facility structure. (See MIL-HDBK-419.)

5.2 Power distribution. The power distribution system must accomplish two objectives. First, it must provide quality power, free of abnormalities which could cause loss of synchronization, discontinuity of switching functions, or physical damage to the system. (See MIL.HDBK-411.) Second, it must be designed to provide electrical protection of classified information, and the equipment processing that information from EMP, electromagnetic interference (EMI)/radio frequency interference (RFI), and TEMPEST hazards, as required. The design and installation of the power system involves two components - the power source and the facility load. The design requires judicious selection of the primary and auxiliary power sources, UPS or other power conditioning equipment, secondary substations, protective measures, and the distribution system in order to attain the maximum overall system performance with the most cost effective design. The designer is cautioned to check local electrical codes when engineering facilities in overseas locations.

5.2.1 Source. The ideal situation is to have the prime power source for the facility located totally within the controlled space (CS). This would imply a power generation station located within the CS. Since this situation applies only to a few facilities, other options must be explored. Guidance for power source installation is contained in MIL-HDBK-411.

5.2.1.1 Self-generated power. The objective of self-generation is to provide isolated power which is distributed only to the facility and is not shared with other activities (see figure 17). This isolation ran be realized using MG and no-break generator sets. An MG consists of an ac or de motor driving a generator. If the drive shaft connecting the motor to the generator consists of nonconductive sections, the MG not only provides clean isolated power, but may satisfy EMP/TEMPEST isolation requirements (see figure 18). A no-break generator set is similar to an MG in that an ac or de motor normally drives the generator. The generator includes an inertia wheel connected to a diesel engine. When prime power is lost, the inertia wheel keeps the generator supplying power while the engine is started and brought up to operating speed.

5.2.1.2 Uninterruptible power. Many facilities in recent years have used an UPS. These UPS are intended to provide stable, clean power for the mission. Any UPS system must be evaluated to determine the extent of isolation between the power line and the service loop. Where an UPS used, and separate RED and BLACK feeds are required, separate UPS may be considered (see figures 19 and 20). Some UPS include a bypass mode which connects the load to the incoming line in case of UPS failure. This feature cannot he employed when the UPS feeds RED equipment.

5.2.1.3 Base power. In most instance, the facility will be provided with commercial or base power. Either source requires the most stringent controls to ensure isolation and prevent distribution of compromising emanations by power-line conductions (PLCs). Three configurations of the source may be encountered (see 5.2.1.3.1, 5.2.1.3.2, and 5.2.1.3.3).

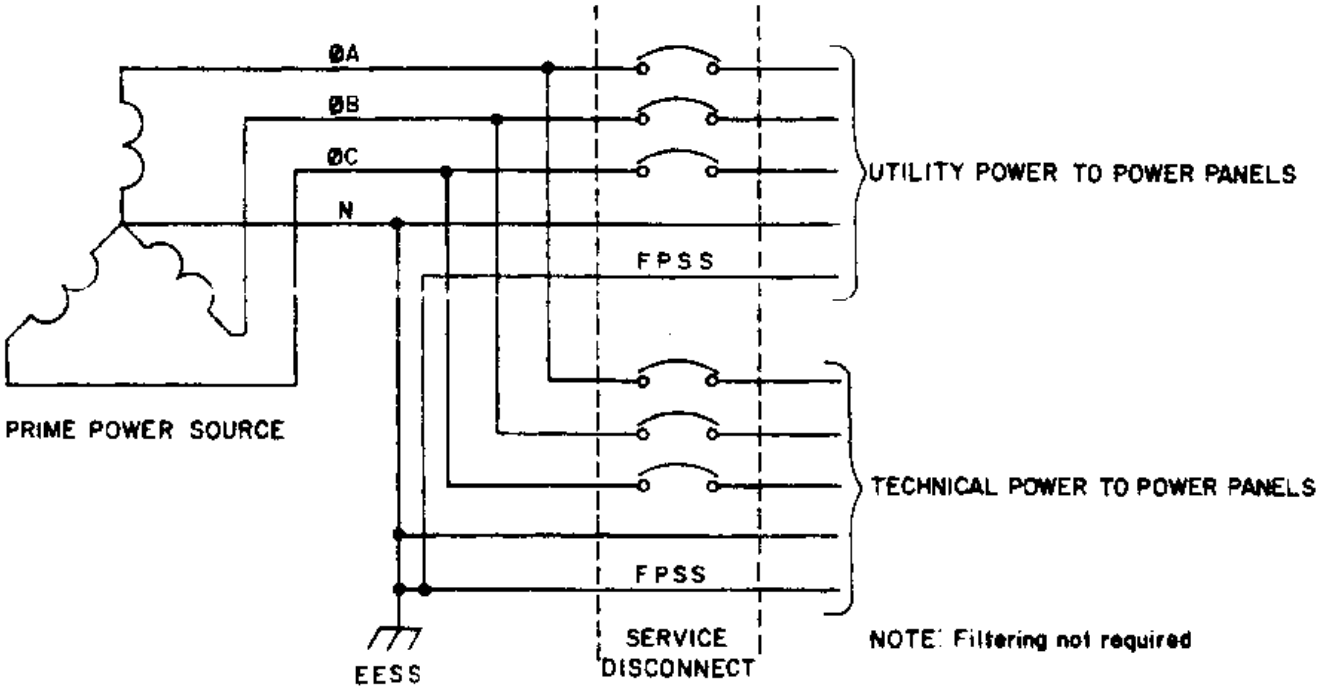


FIGURE 17. Self-generated power source.

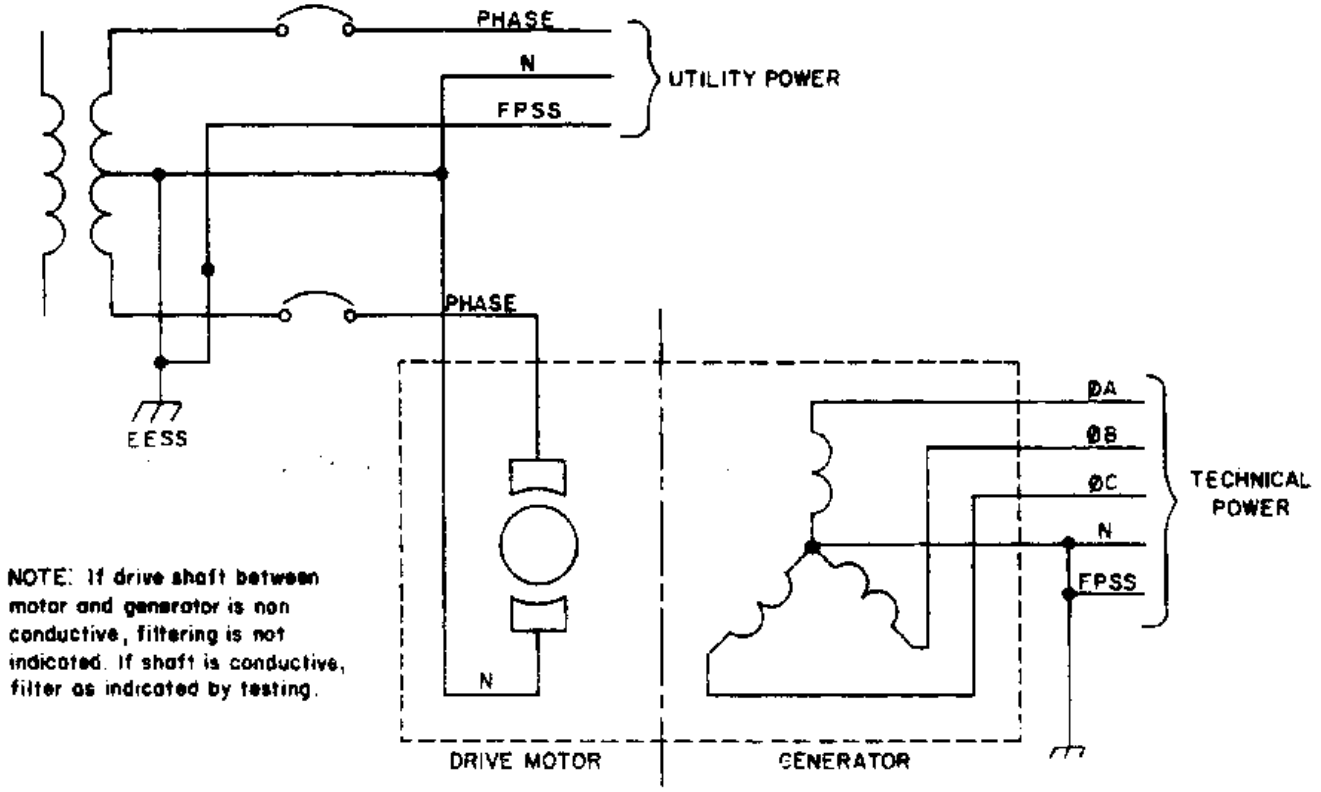


FIGURE 18. Motor generator.

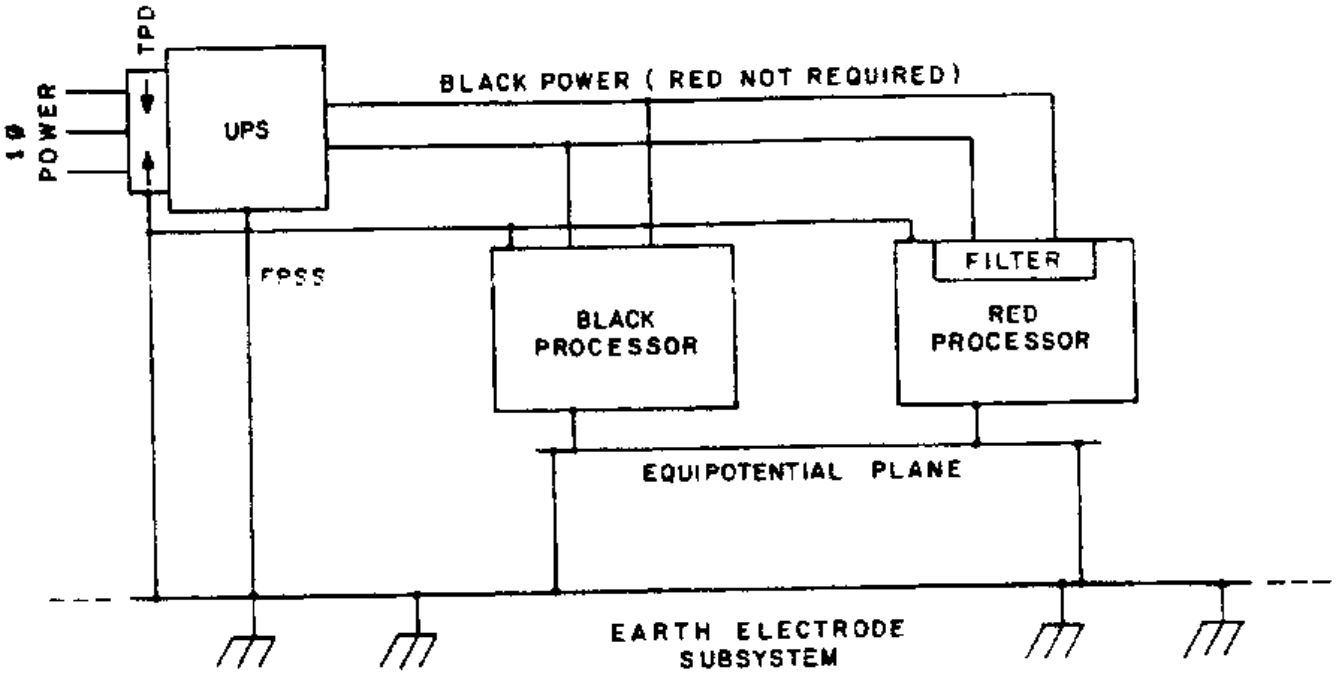


FIGURE 19. UPS, TEMPEST facility.

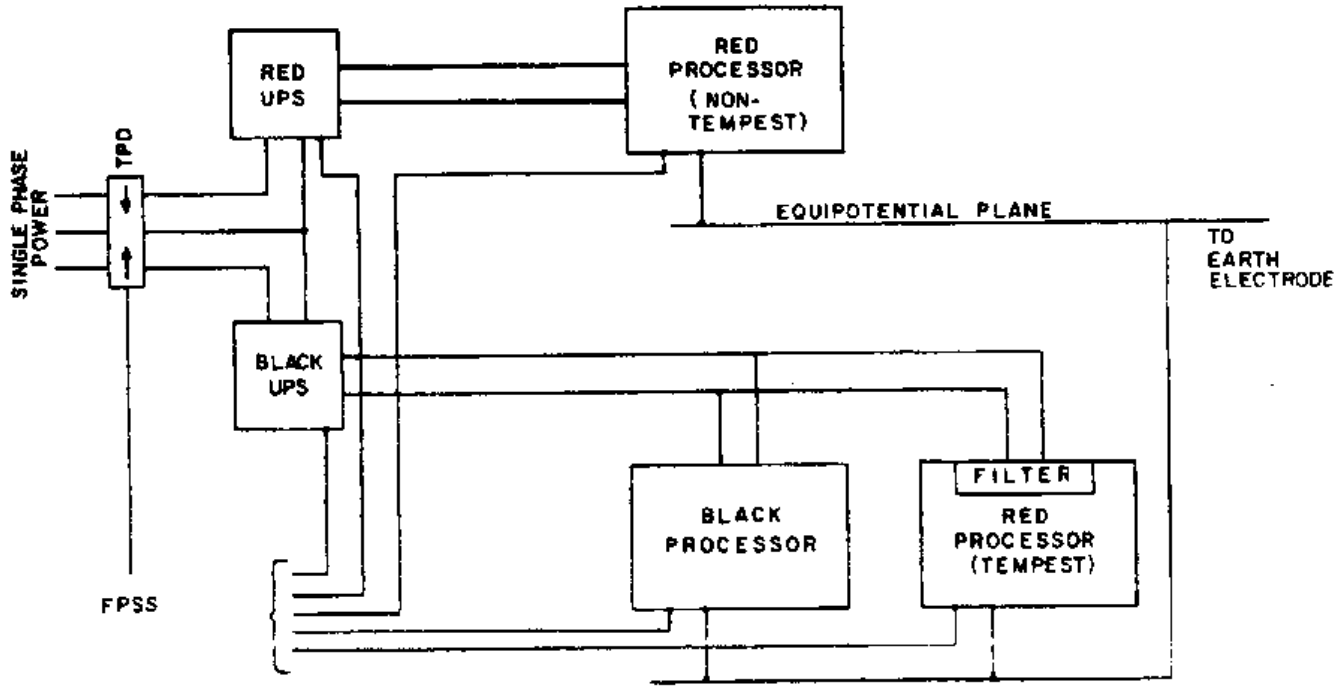


FIGURE 20. UPS, nonTEMPEST facility.

5.2.1.3.1 Dedicated service. A large facility would most likely be served by a dedicated feeder transformer. This may be a delta-wye configuration providing three phase leads and a neutral conductor grounded at the transformer or first service disconnect. A fifth wire is included as the fault protection subsystem (FPSS) (see figure 21) to provide a return path for fault currents. Some isolation may be available through the transformer. Filtering may be required if testing indicates insufficient suppression of PLC. Care must be taken during installation and design to assure the loads are balanced across the phases to reduce neutral currents.

5.2.1.3.2 Pole power. A smaller facility may be served by a single phase pole transformer. In such cases, two energized leads, a neutral conductor, and an FPSS conductor are provided (see figure 22). As in the large facility, testing must be conducted to determine the extent of PLC and the preventive measures required. This application is served well by an MG which isolates the load from the source. Such MGs should use a dielectric shaft between the motor and generator with separated housings.

5.2.1.3.3 Shared power. A smaller facility may be served from the source for the entire building in which it is located. In such cases, significant problems arise in controlling PLC and accounting for the distribution of power. Filtering is indicated if RED power is required. An MG is also appropriate if RED power is needed.

5.2.2 Power systems. Two power systems are usually established within each facility -- non-technical power and technical power (see figure 2).

5.2.2.1 Nontechnical power. Nontechnical power is established to provide heating, lighting, ventilation, and other services that are not required for full continuity of operation. Nontechnical service is provided to prevent equipment upset in the event of drops and surges caused by other equipment cycling. Motor-driven fans, blowers, and pumps are inherent surge sources. No special treatment is normally required, except that distribution should be in conduit or armored cable with the conduit or armor grounded. Nontechnical power is provided separately from technical power. Additionally, the distribution should be designed so that nontechnical power cannot be used to power the technical equipment. The need to filter utility power should be determined on a case-by-case basis. The designer or installer may have no control over the way nontechnical power may have been installed in the facility. In such cases, the design and installation of the remainder of the facility require that more stringent controls be established.

5.2.2.2 Technical power. Technical power is provided to power that equipment which supports the mission. It is distributed in areas as required and may be further divided into RED and BLACK power. RED power is created by filtering selected lines a nd controlling distribution (see figure 23) or by using MGs. Application of filtering is specified in paragraph 5.2.6.

5.2.2.3 Distribution. Distribution of power should be in metallic duct, wire way, or conduit. Flexible conduit may be used for short runs from wire ways or junction boxes to equipment ("short" means no longer than necessary for vibration or minor placement adjustment). Care must be exercised to ensure the electrical integrity and conductivity between the wire way/junction box and equipment case, because flexible conduit often uses plastic or nonconducting bushings in fittings that jeopardize continuity. Where RED and BLACK power are established, each shall be distributed separately. Power is not run in ducts with any other cable. Nontechnical and technical power should be distributed in separate ducts/conduits (see 4.2.2.1 and 4.2.2.2).

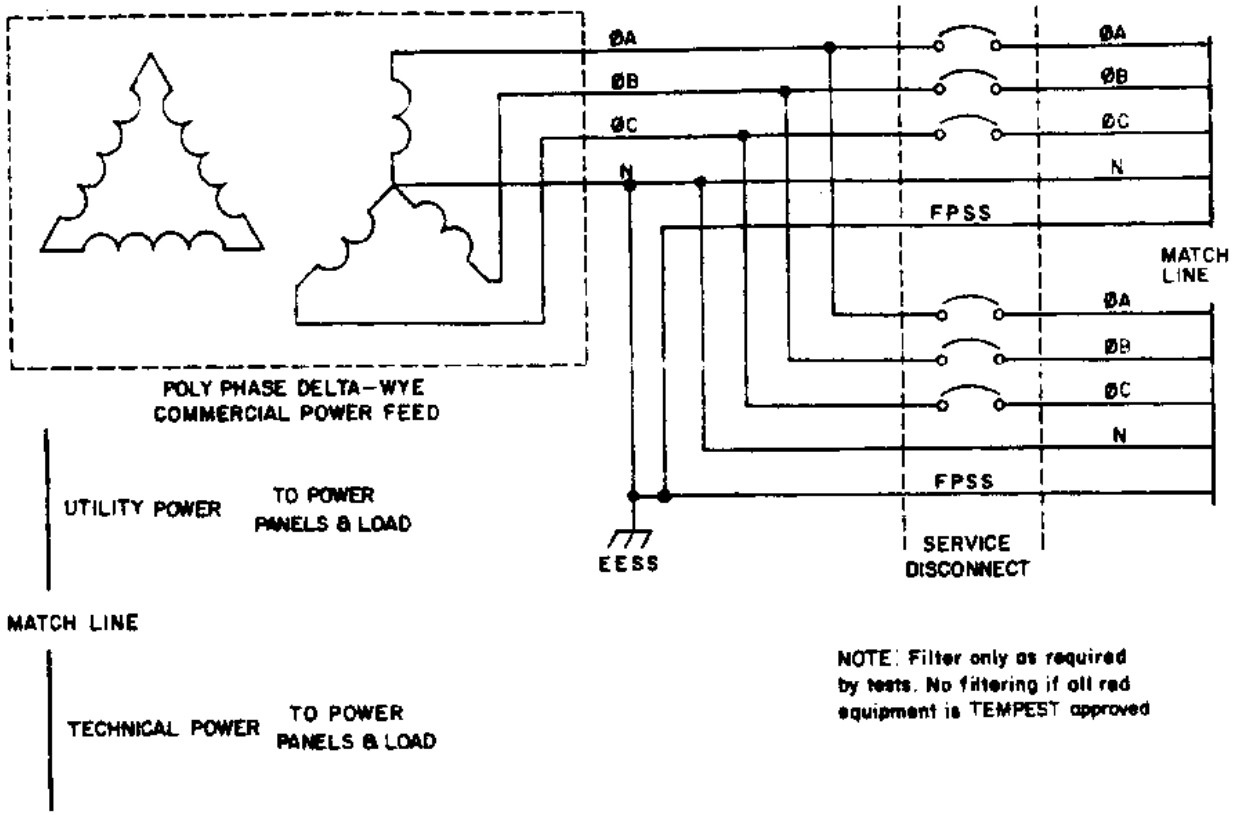


FIGURE 21. Dedicated transformer feed.

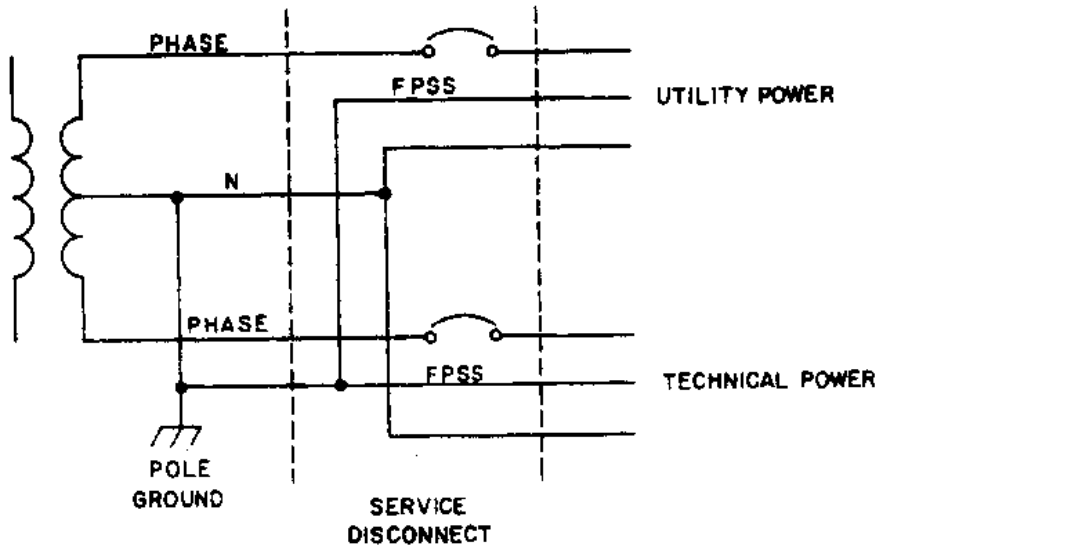


FIGURE 22. Pole power feed.

5.2.3 Power panels. Power panels require no special installation other than placement. Panels should, if possible, be located within the vicinity of the equipment being served. If RED power is established, separate panels are provided for RED and BLACK distribution. Nontechnical power will not be mixed with technical power. Panels should be marked with appropriate use labels.

5.2.4 Terminations. Equipment terminations should be consistent with equipment design. If the equipment uses conventional ac plugs, plug boxes or plugmolds should be located within the enclosure or rack. In all cases, the runs from the power panels to the equipment shall be three continuous wires run in a single run (for single phase use). In no case will the phase, neutral, or ground conductors be run in separate conduits or ducts to equipment.

5.2.5 Grounding. Grounding of power is in accordance with MIL-HDBK-419, MIL-STD-188-124, and the National Electrical Code (NEC). Specifically, the neutral conductor will be grounded to earth at the service transformer or first service disconnect. The grounding point should be, in order of precedence: (a) a network of earth driven rods forming the facility EESS, (b) structural steel, (c) metallic cold water piping system, or (d) other continuous metallic system. The installer and designer are cautioned to be aware of grounding problems in some commercial equipment. MIL-STD-188-124 states, "The ac neutral shall be insulated from the equipment chassis and case." Many items of commercial equipment and older Government equipment use the chassis for a neutral reference. In such cases, it is not possible to isolate the neutral and FPSS wire. The design engineer should group all such equipment on a single power panel. This technique is meant to reduce the safety hazard associated with tying these lines together. Grounding techniques are also discussed in FIPS PUB 94, along with suggested solutions for digital systems.

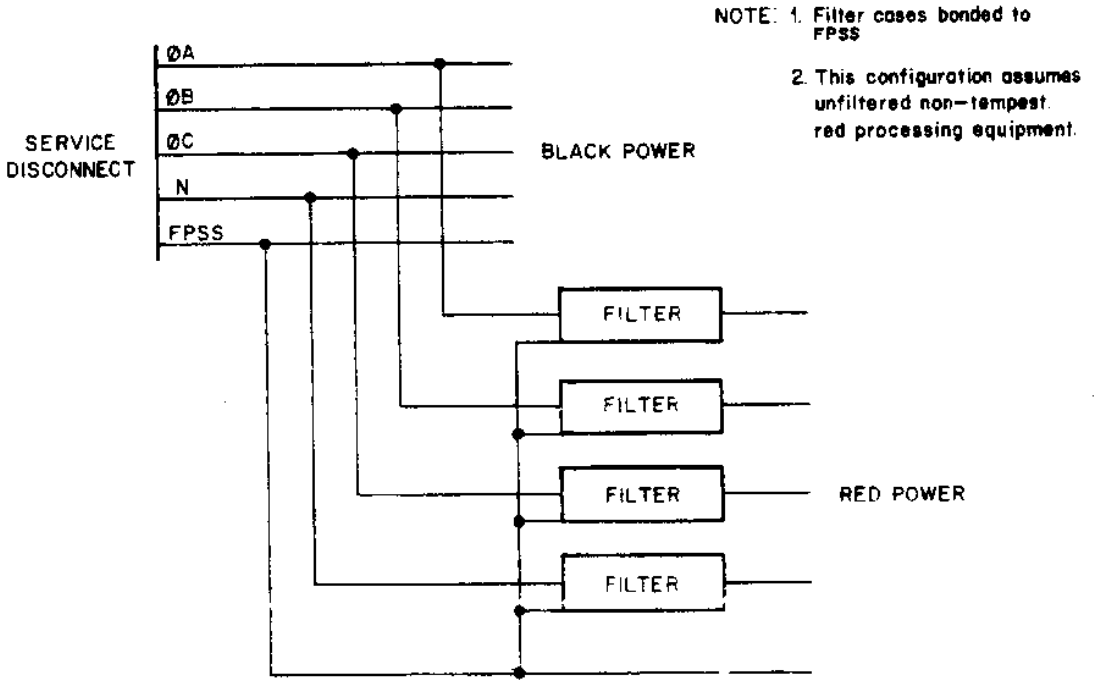


FIGURE 23. RED/BLACK technical power.

5.2.6 Filters. The source of power and the type of equipment used will define what filtering, if any, is required. Practices in the past include filtering of all technical power. If all BLACK runs have been properly installed and the conduits are properly grounded and adequately separated from RED runs, the need for such filtering is eliminated or greatly reduced. The designer should engineer the power installation so that if additional filtering is indicated by instrumented tests, a retrofit can be accomplished with minimal effort. Designers are cautioned that filtering power lines to equipment containing filters must be avoided. Filters in series effectively operate as a single composite filter with entirely different characteristics, which may present other problems or may fail to operate as required (see figure 24 and 5.5). If the source of power is totally contained in the CS, power filtering may not be needed. If MGs or no-break systems are used, filters may not be needed if sufficient isolation exists between the feed and load to prevent PLC. This situation would have to be confirmed with instrumented tests by a cognizant TEMPEST agency of the department or activity. If other power sources are used, then the type of equipment supporting the mission dictates the need for filtering. Ideally, each equipment processing RED information would be filtered. In such cases, no additional filtering should be required, and the technical power would be considered BLACK power. Such filtering is preferred because the filter then matches the equipment. All TEMPEST approved equipment meet the criteria. Filters are included in the design of some commercial equipment. These filters, however, probably will not conform to the attenuation requirements of MIL-F-15733. Such equipment should be retrofitted, if possible. Bulk filtering is indicated when RED processing equipment does not include filters, or contains filters which do not conform to standards. Such nonconforming filters should be removed. Bulk filtering involves installing filters of appropriate size on the feeder lines to a power panel. The filters should be located at the point of entrance to the LEA. Power on the load side of the filter is considered RED power.

POWER SOURCE: 120 VAC, 60 HZ 25A LOAD

EQUIPMENT: 120 VAC, 60 HZ .5A LOAD

FILTER TYPE: SINGLE STAGE L NETWORK LOWPASS

DESIGN: IMAGE PARAMETER METHOD

SOURCE FILTER (S)

$L_S = \frac{R}{\pi f_C}$ $\quad C_S = \frac{1}{\pi f_C R}$

$L_S = \frac{4.8\Omega}{\pi(60\ Hz)}$ $\quad C_S = \frac{1}{\pi(60\ Hz)(4.8\Omega)}$

$L_S = 2.54 \cdot 10^{-2}h$ $\quad C_S = 1.1 \cdot 10^{-3}fd$

EQUIPMENT FILTER (E)

$L_E = \frac{R}{\pi f_C}$ $\quad C_E = \frac{1}{\pi f_C R}$

$L_E = \frac{2.4 \cdot 10^{2}\Omega}{\pi(60\ Hz)}$ $\quad C_E = \frac{1}{\pi(60\ Hz)(2.4 \cdot 10^{2}\Omega)}$

$L_E = 1.27h$ $\quad C_E = 2.21 \cdot 10^{-5}fd$

EQUIVALENT FILTER

$L_T = L_S + L_E = 2.54 \cdot 10^{-2}h + 1.27h = 1.29h$

$C_T = C_S + C_E = 1.1 \cdot 10^{-3}fd + 2.2 \cdot 10^{-3}fd = 1.12 \cdot 10^{-3}fd$

$F_{C_T} = \frac{1}{\pi\sqrt{L_T C_T}} = \frac{1}{\pi\sqrt{(1.29h)(1.12 \cdot 10^{-3}fd)}} = 8\ Hz$

FIGURE 24. Consequences of double filtering.

5.3 RED equipment installation. The goal of any RED equipment installation is to create physical, electrical, and EM barriers around equipment that processes classified information to prevent that information from being exploited by hostile intelligence service activities. The design begins by establishing an REA within the LEA. The space is established to contain the RED processing equipment and related support functions with barriers to exclude all other functions. The ideal situation is to establish the REA adjacent to the REA such that the LEA is contiguous (see figure 1). This may not be possible for some facilities (see figure 25). In some instances, the cognizant security agency and cognizant TEMPEST agency should assess the facility for the protective measures required to interface the respective areas. See paragraph 5.7.3 for requirements of a protected distribution system (PDS).

5.3.1 Contiguous LEA. Figure 26 depicts a typical small facility in which an REA has been established by segregating all RED equipment away from all BLACK equipment. Where TEMPEST approved equipment is used, or the equipment radiation TEMPEST zone (ERTZ) is known, such designs rely upon the use of separation tables or the ERTZ data to size the REA. Figure 1 depicts a typical large facility. In this case, separate but adjacent rooms compose the LEA with each area physically separated.

5.3.2 Equipment separation. The separation of equipment in the LEA is dependent upon the class of equipment, e.g., TEMPEST approved, nonTEMPEST, low-level or high-level signaling. Figure 27 depicts a single-line secure teletypewriter system using TEMPEST approved equipment. The equipment layout keeps dissimilar equipment separated by at least 2 inches (50 mm). Signal and power runs associated with this installation are also separated by 2 inches (50 mm). Should the RED and BLACK signals cross at 90-degree angles, the separation may be reduced to 1 inch (25 mm). All equipment should be located at least 3 feet (0.9 m) from the walls to aid in visual technical inspection. Figure 1, which depicts a large facility, follows the same minimum separation requirements. Typically, greater separation is used in the design due to specific installation practices such as minimum cable bending radius plus size of interconnecting ducts and conduits. An additional requirement is separation of long parallel RED and BLACK duct runs. Where these runs exceed 100 feet (30 m), separation should be increased to 6 inches (150 mm) over the length of the run. Figure 28 depicts a small single-line teletypewriter facility using nonTEMPEST, high-level equipment. In this type of installation, the communications security (COMSEC) equipment establishes a bench mark for equipment separation. All RED equipment, including patching and distribution frames, are separated from the COMSEC by at least 3 feet (0.9 m). All BLACK equipment is also separated from the COMSEC by 3 feet (0.9 m), resulting in a separation of 6 feet (1.8 m) between RED and BLACK equipment. Separation of signal and power ducts and conduits is as with low-level TEMPEST equipment. See tables I and II for specific separation requirements.

5.3.3 Special considerations. Some systems are procured under restriction to use commercially available nondevelopmental items (NDIs) . When such a situation occurs, the engineer should design to the separation requirements of high-level systems, unless a known equipment profile exists. Consult the cognizant TEMPEST authority.

5.3.3.1 Interface to other equipment. Many NDIs use the EIA-RS-232C standard to interface with other equipment. This standard allows as much as 15 volts on interface lines. Unless the device is demonstrated to operate at levels defined in MIL-STD-188-114, high-level installation is indicated. If the device can comply with MIL-STD-188-111, the shorter separations may be

possible (table I). This should be confirmed by instrumented TEMPEST tests by the cognizant TEMPEST agency. (See NACSIM 5201.)

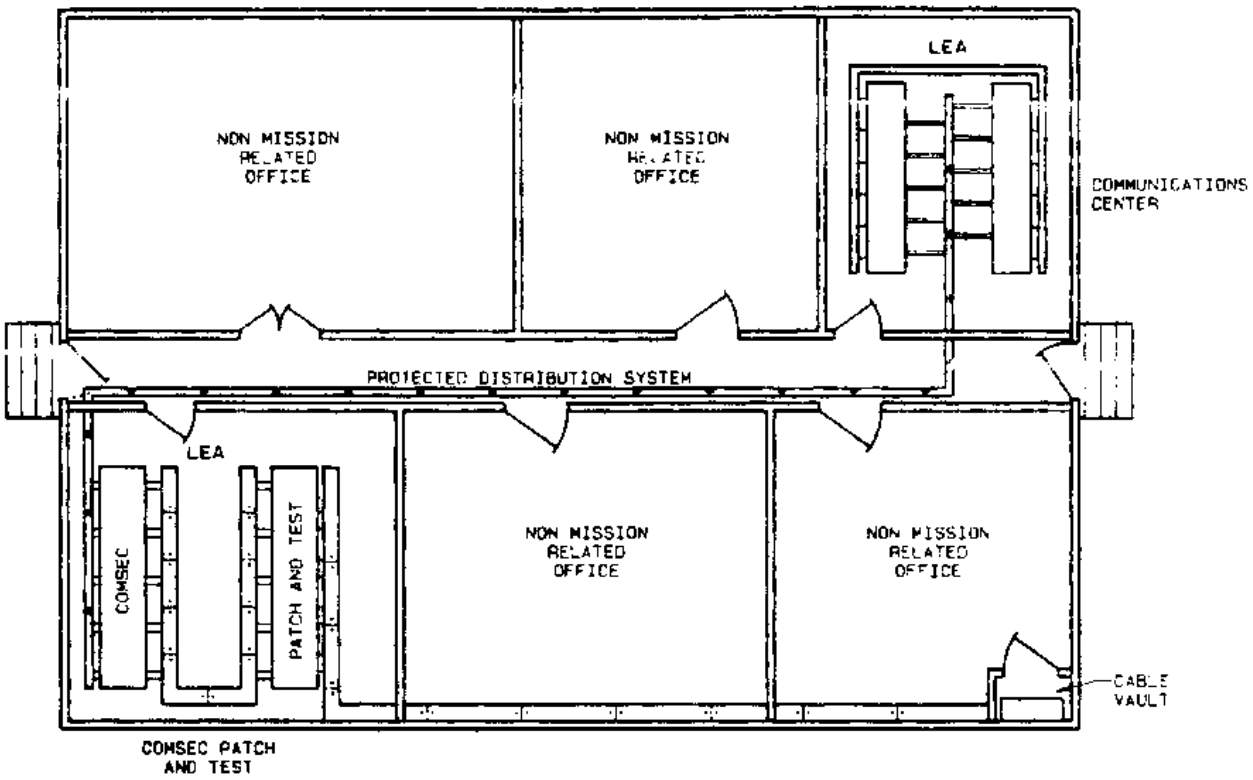


FIGURE 25. Noncontiguous LEA.

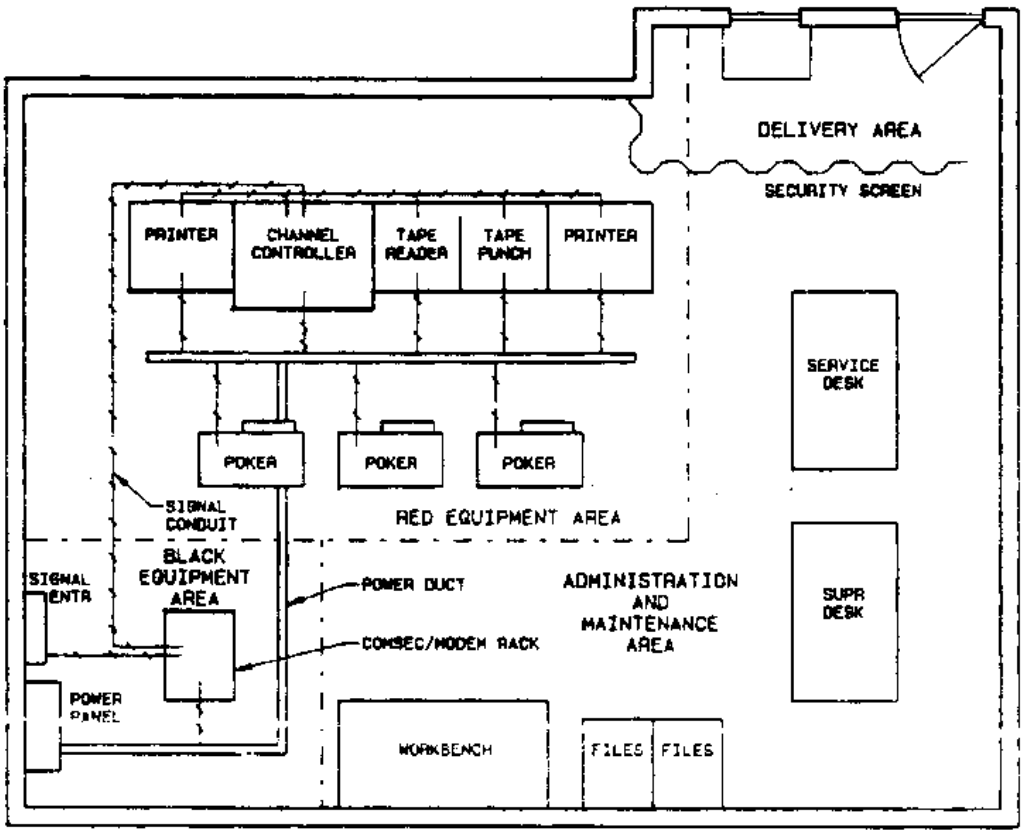


FIGURE 26. Small facility.

MIL-HDBK-232A

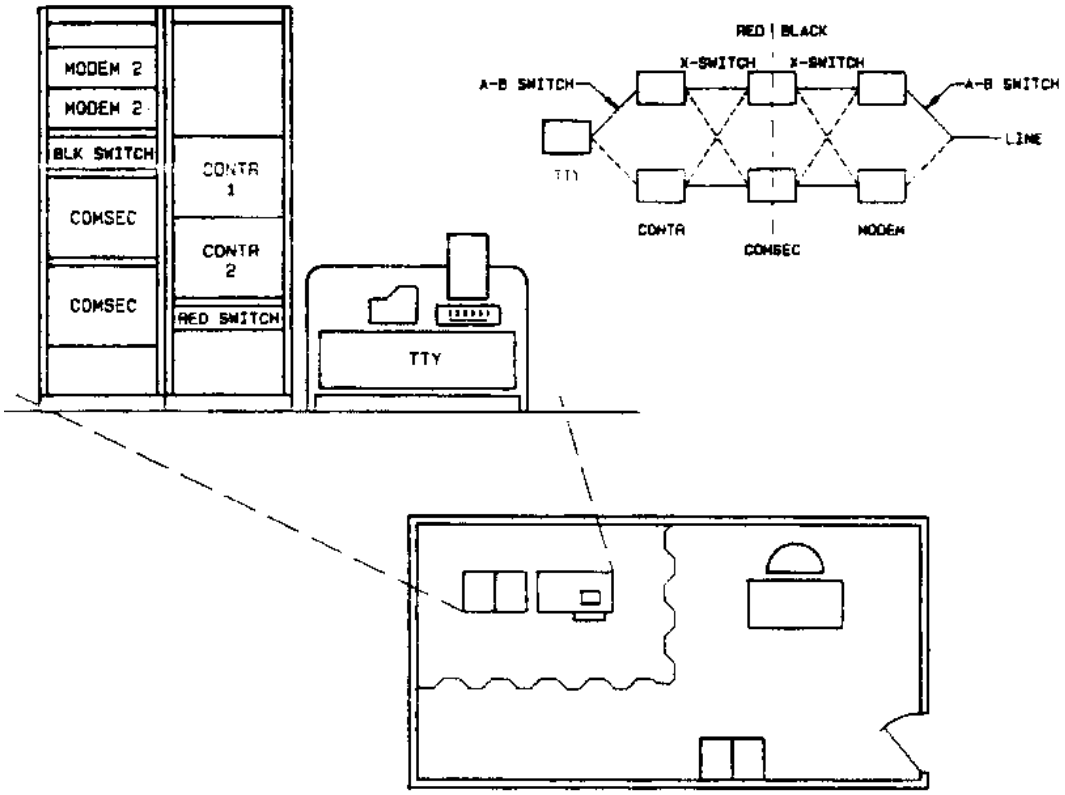


FIGURE 27. Small facility (TEMPEST).

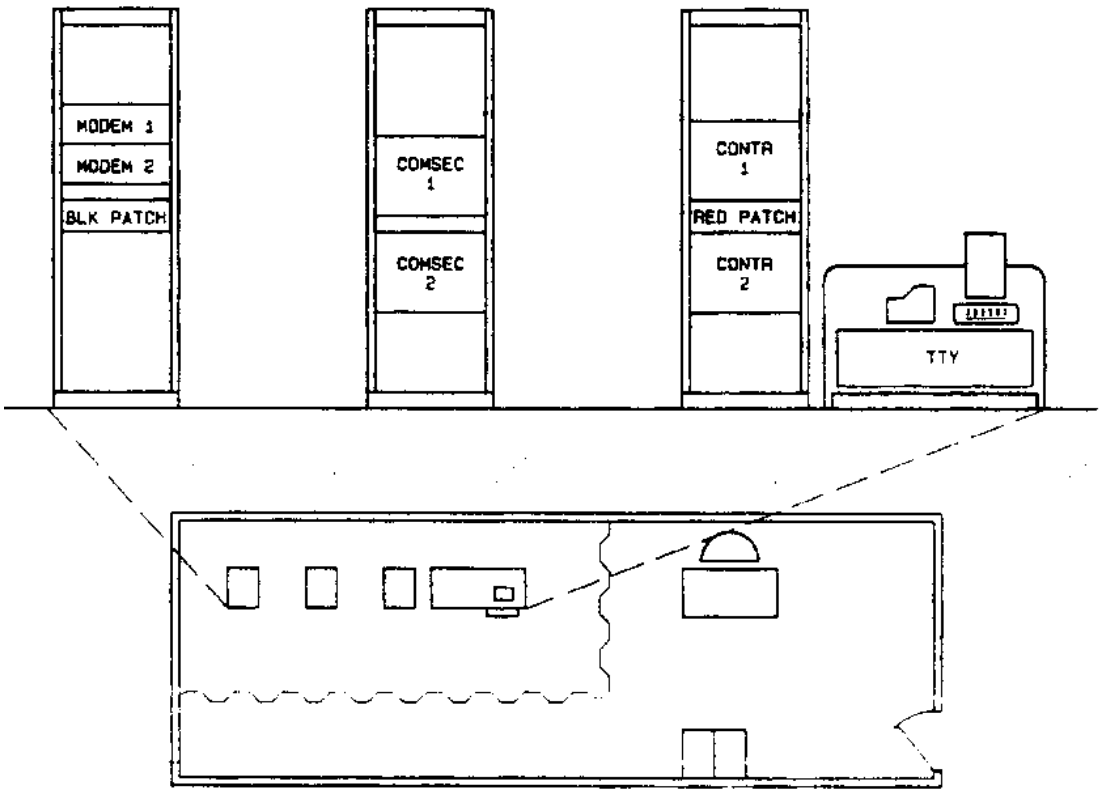


FIGURE 28. Small facility (nonTEMPEST).

TABLE I. Separation requirements — TEMPEST/low level.

CRYPTO AND BLACK EQUIPMENT / CRYPTO AND RED EQUIPMENT	Wire line distribution facilities less patch panels, frames, electronic panels, etc.	Cord type patch panels.	Electronic panels (switch, crossbar, matrix, etc.).	Distribution frames, intermediate distribution frames, main distribution frames, etc.	Without isolator or filter.	BLACK end processors with wire lines egressing controlled access area via isolator or filter.	Crypto-ancillary equipment.	Unit designated modem tied to wire line leaving controlled access area.	Unit designated modem but not tied to wire line leaving controlled access area.	Electromechanical, line relays, duplex repeaters, etc., tied to wire line leaving controlled access area.	Walls with no outside control, or internal condition or walls unknown (controlled, uncontrolled).	Walls with outside control, inside walls made of wood, plasterboard, etc.	Power, signal ground distribution facilities including components therewith associated.	BLACK dc supplies.	Crypto-equipment.
Wire line distribution facilities less patch panels, frames, electronic panels, crossovers, etc.	2" 1" @ 90°	2"	2"	2"	2"	2"	2"	2"	2"	2"	2"	2"	2"	2"	0"
Cord type patch panels.	2"	2"*	2"	2"	2"	2"	0"	3'	2"	3'	2"	2"	2"	2"	0"
Electronic panels (switch, crossbar, matrix, etc.) nonregenerative.	2"	2"	2"	2"	2"	2"	0"	2"	2"	2"	2"	2"	2"	2"	0"
Distribution frame (combined intermediate distribution frame).	2"	2"	2"	2"	2"	2"	2"	2"	2"	2"	0"	0"	2"	2"	0"
Crypto-equipment (case exception).	2"	2"	2"	2"	2"	2"	0"	3'	2"	3'	3'	2"	2"	2"	0"
RED end processors.	2"	2"	2"	2"	2"	2"	2"	3'	2"	2"	3'	2"	2"	2"	2"
Poke positions.	2"	2"	2"	2"	2"	2"	2"	3'	2"	2"	3'	2"	2"	2"	2"
Power, signal ground distribution facilities including components therewith associated.	2"	2"	2"	2"	2"	2"	2"	2"	2"	2"	0"	0"	2"	2"	0"
RED dc supplies.	2"	2"	2"	2"	2"	2"	2"	2"	2"	2"	2"	0"	2"	2"	0"

* Additional separation greater than the patch cord length is required if physical safeguards against inadvertent crosspatch are not provided.

** 1" = 25 mm 2" = 50 mm 3' = 0.9 m

TABLE II. Separation requirements — high level.

CRYPTO AND BLACK EQUIPMENT / CRYPTO AND RED EQUIPMENT	Cord type patch panels.	BLACK end processors with wire lines egressing controlled access area without isolator or filter.	BLACK end processors with wire lines egressing controlled acess area via isolator or filter.	Crypto-ancillary equipment.	Unit designated as modem tied to wire line leaving controlled access area.	Unit designated as modem but not tied to wire line leaving controlled access area.	Electromechanical, line relays, duplex repeaters, etc., tied to wire line leaving controlled access area.	Crypto-equipment.
Cord type patch panels.	3′	3′	2″	2″	3′	2″	3′	3′
RED end processors.	3′	3′	3′	3′	6′	3′	3′	3′
Poke positions.	3′	3′	3′	3′	6′	3′	3′	3′
Crypto-equipment.	3′	3′	3′	0″	3′	2″	3′	0″

* 2″ = 50 mm 3′ = 0.9 m 6′ = 1.8 m

5.3.3.2 Electromagnetic interference (EMI)/electromagnetic compatibility (EMC). Any installation design should include an EMC analysis as part of the design process. Certain commercial items must comply with Federal Communications Commission Regulations, Part 15, Subpart J, for EMI. This should be taken into consideration when convicting the EMC analysis to determine what benefits this requirement may have in reducing the threat of exploitation of the system.

5.3.3.3 Interface among RED equipment. MIL-STD-188-114 defines interface requirements for equipment in a low-level environment. The standard recognizes, however, that interfaces among equipment in the RED area that constitute a system may not be required to comply. In these cases, the engineer must consider the technology used in the interface. Other than EIA-RS-232C interfaces (see 5.3.3.1), interfaces having signal levels below 6 volts pose a low risk, while those above 6 volts should be afforded extra safeguards, such as individually shielded pair cable and metallic race way or conduit. Such measures should be taken, as indicated by instrumented TEMPEST tests and analysis.

5.3.3.4 Low-risk technology. Some equipment may use laser and xerography technologies to produce copies of classified information. That portion of the device is inherently low risk due to the nonexistence of emanations. The risk area is the electronics driving such equipment. If the electronics uses technology at levels of 6 volts or less, a low risk may be achieved. (Consult NACSIM 5100.)

5.3.3.5 Converted equipment. Equipment exists in the Department of Defense (DoD) inventory that was procured with high-level components and subsequently retrofitted for low-level operation. If such equipment is used in a system, the designer is cautioned that some of this equipment was only partially converted. Converters were installed in the signal lines, but no change was made to the internal electronics. If converted equipment is used, it should be separated as if it were a high-level device, unless it is known that all electrical components were property converted.

5.3.3.6 Video devices. Equipment using cathode ray tube displays present a source of free space emanations. Such devices may require shielding around the display, particularly across the face of the display. Shielding glass and metallic housings are commercially available to accomplish this containment of emanations.

5.3.3.7 Magnetic disk memories. A common commercial installation practice in systems with magnetic disk memories is to remove the cabinet sides of a group of units and bolt the chassis together as a single unit. This practice should be avoided as the arrangement negates the shielding effectiveness of the cabinet. Each unit should be installed as a stand alone with separate grounding and bonding.

5.3.3.8 BLACK equipment installed in RED areas. Certain operations require installation of BLACK equipment in RED areas, such as emergency action consoles in Command and Control facilities. In such cases, the BLACK equipment will be separated from RED equipment by 3 feet (0.9m) if the BLACK equipment is low level or 6 feet (1.8 m) if high level. However, BLACK voice equipment will require 6 feet (1.8 m) separation regardless of the level. (See 5.8 for other telephone requirements.) (See tables I and II.)

5.3.4 Telephone networks and instruments. There are various types and configurations of secure telephone networks and instruments in use within the DoD. Due to this variety, it is difficult to develop a standard procedure which would apply to all elements of the secure voice community.

5.3.4.1 Secure telephone switches. Secure telephone switches such as AUTOSEVOCOM are used to provide switching capability for secure voice terminals and to provide interface capability between various types of equipment. Physical security precautions should be commensurate with those for other REAs and adequate for the level of classification of calls processed by the switch. As a minimum, the area should be designed as an REA. When a secure voice switch is collocated with secure or nonsecure data systems, it is recommended that the switch be installed in an area which is remoted from the other system(s). All signal and control lines should utilize cable which uses an overall nonferrous shield with the shield circumferentially grounded at both ends. All wire lines, to include signal, control, and power, should be installed in ferrous-type conduit. This is necessary to provide maximum protection, and to isolate RED/BLACK line.3 and digital and analog systems. An equipotential ground plane should be used for all grounds except the ground FPSS, which should be connected to the ground bus of the servicing power panel. Separate grounds should be run for all pieces of equipment with the conductors being continuously run, i.e., not spliced. RED and BLACK equipment should be separated in accordance with table I.

5.3.4.2 RED voice systems. A RED voice system is an unencrypted voice network with physical protection and distribution such that it may be used for classified communications. RED voice systems may be used within an LEA as an internal secure telephone network within a RED enclave. When this type of system exists, all cables should have a nonferrous overall shield. All cables, to include signal, control, and power, should be installed in ferrous conduit. No unencrypted telephone lines should penetrate the LEA barrier. Lines which must connect to other secure telephone systems or the dial central office should be connected to a secure voice switch or other encryption device prior to the point of egress of the LEA.

5.3.4.3 Secure voice terminals. Approved secure voice terminals, such as a TSEC/KY-3, may be installed in or external to LEAS. When installed in an LEA, where other communications equipment is used, all cables should be installed in ferrous conduit. The terminal should be separated from other electronic devices in accordance with table I. Only those telephone instruments and cables designed for the specific system should be used. If the telephone instrument is remoted from the terminal, the interconnecting cable should be installed in ferrous conduit. Terminals that are installed external to an LEA should be installed a minimum of 6 feet (1.8 m) from other electronic equipment. Conduit for wire lines is not required if other electronic devices are not used in the same general area. Grounding may be provided by structural steel.

5.4 Signal distribution. The objective of signal distribution is to take a signal from one point to another in such a manner that the signal is not interfered with, does not cause interference, and is not misrouted. The designer and installer must consider:

a. What type of signal is being distributed.

b. What type of cable best supports that signal.

c. What special treatment is required for that signal.

d. What effects can degrade that signal.

e. What effects can that signal cause.

5.4.1 Treatment of signal types.

5.4.1.1 Analog signals. Analog signals in a facility can be grouped in six categories. (Including quasi-analog signaling as defined in FED-STD-1037.)

a. Quasi-analog signals supporting wire-line modems.

b. Analog signals originating in radios.

c. Analog signals in administrative telephone systems.

d. Quasi-analog signals in secure voice systems.

e. Quasi-analog signals supporting video systems.

f. Quasi-analog signals associated with broadband local area networks (LANs).

5.4.1.1.1 Wire-line modems. Quasi-analog signals from wire-line modems are the most common such signals encountered in a facility. The distribution of these signals, which are typically BLACK, is the least complex. Typical routing is from the modem to an analog frame and patch bay, to a DF, to the facility entrance plate. Cabling between units typically uses twisted pairs and may have each pair shielded. All cables should be filtered at the facility entrance plate. All cabling should be contained in metallic wire ways, ducts, or conduits. Where analog signals are RED, separate distribution and patching facilities are required in addition to physical security measures.

5.4.1.1.2 Radio. Radio transmitters should not be located within the LEA. However, in specialized facilities, the exclusion of radios may not be operationally possible. Such radios may be used for voice or data transmission. Treatment of signal distribution for radios begins with proper separation of the radio from all other equipment. In applications involving voice communications in Command and Control facilities, it is assumed that microphones or radio telephone handsets will be located in an operations area which may be an REA. In such cases. the cables must be distributed from the radio rack to the REA in dedicated conduit, with separation similar to that for administrative telephones. The cables should also he filtered at the REA. Microphones and handsets should be equipped with push-to-talk, push-to-listen switches. In applications involving data communications, it is assumed that the circuit will be secure, and the input to the radio is digital and probably encrypted. In such cases, the input distribution is the same as any digital circuit. The output of the radio, regardless of its use in an LEA, is treated to prevent RFI/EMI. At the entrance plate, the cable should be filtered with a bandpass filter appropriate for the frequency of the radio.

5.4.1.1.3 Administrative telephones. Administrative telephone signal distribution in an LEA is separate from all other distribution. All cables enter at the facility entrance plate where filtering and EMP treatment is applied. This applies to telephone for voice communications only not

telephone lines used for data communications. Telephone lines used for dedicated, full-period data communications would be treated as analog lines, From the facility entrance plate, all cables are run in conduit to the areas where the end instruments are located. The conduit should be extended to the desk, rack, or table on which the instrument is located. Overall shielded cable should be used. For other requirements see paragraph 5.8.

5.4.1.1.4 Secure voice. Analog extensions of secure voice systems should be run in separate conduit from the security equipment to the end instrument. Cables should be shielded. Analog runs on the BLACK side of the security equipment should be as described in paragraph 5.4.1.1.1.

5.4.1.1.5 Video. Video systems in an LEA display the most diverse conditions requiring treatment. Two categories of video equipment are discussed here -- video display units (VDUs) used as terminal devices and televisions as part of briefing and display systems. Video equipment, used as terminal devices in the generic sense, are directly connected to the terminal device controller and require no installation criteria. Some units., however, will use an rf modulator in the controller for interfacing to the display unit. Such connection would be made with coaxial cable, with the VDU in the immediate vicinity of the controller. In some cases, the VDU/keyboard is remoted from the controller. The video cable should be run in conduit. If conduit cannot be used, triaxial cable should be used instead of coaxial cable. Specialized facilities may use a closed circuit television system for briefing and display schemes. This system would be interconnected with coaxial cable or fiber optic schemes. Distribution is in dedicated conduit due to the high frequencies involved. Triaxial cable should be considered for additional shielding. Because of the inherent radiation of the rf stage in most TVs, the system should operate at baseband instead of broadband, with external channel switching. If baseband cannot be used, then the use of triaxial cable or a filter optic scheme is indicated.

5.4.1.1.6 Local area networks (LANs). Broadband and baseband LANs are implemented using coaxial cable to interconnect the nodes. Fiber optic cable (FOC) may be substituted for coaxial cable. Since most LANs will come from commercial sources, additional treatments are necessary. Ethernet, for example, requires a specific type of coaxial cable which is normally installed in overhead plenums. Connection of nodes is accomplished using vampire taps. This design allows easy reconfiguration. In a secure environment, this feature is lost since the cable should be run in conduit for physical security, with pull boxes installed at the points required for taps. Where possible, fiber optics should be used instead of metallic schemes.

5.4.1.2 Digital signals. Digital signals are found between processing equipment in a facility. These signals may be interfaced in either a balanced or unbalanced mode. Balanced interfaces are always distributed with twisted pair, while unbalanced interfaces, by equipment design, may be distributed with single wire or twisted pair.

5.4.1.2.1 Balanced signals. Balanced voltage digital signaling requires a dedicated current return for each signal line from the receiver back to the transmitter. The arrangement depends upon a differential between the two lines to determine signal state. Of concern for the designer and installer is the treatment of all pairs in DFs and patching facilities. DFS should not be wired for bused returns, but should include provision for all pairs. Likewise, patching facilities also should include provisions to patch all pairs. (See figure 29.)

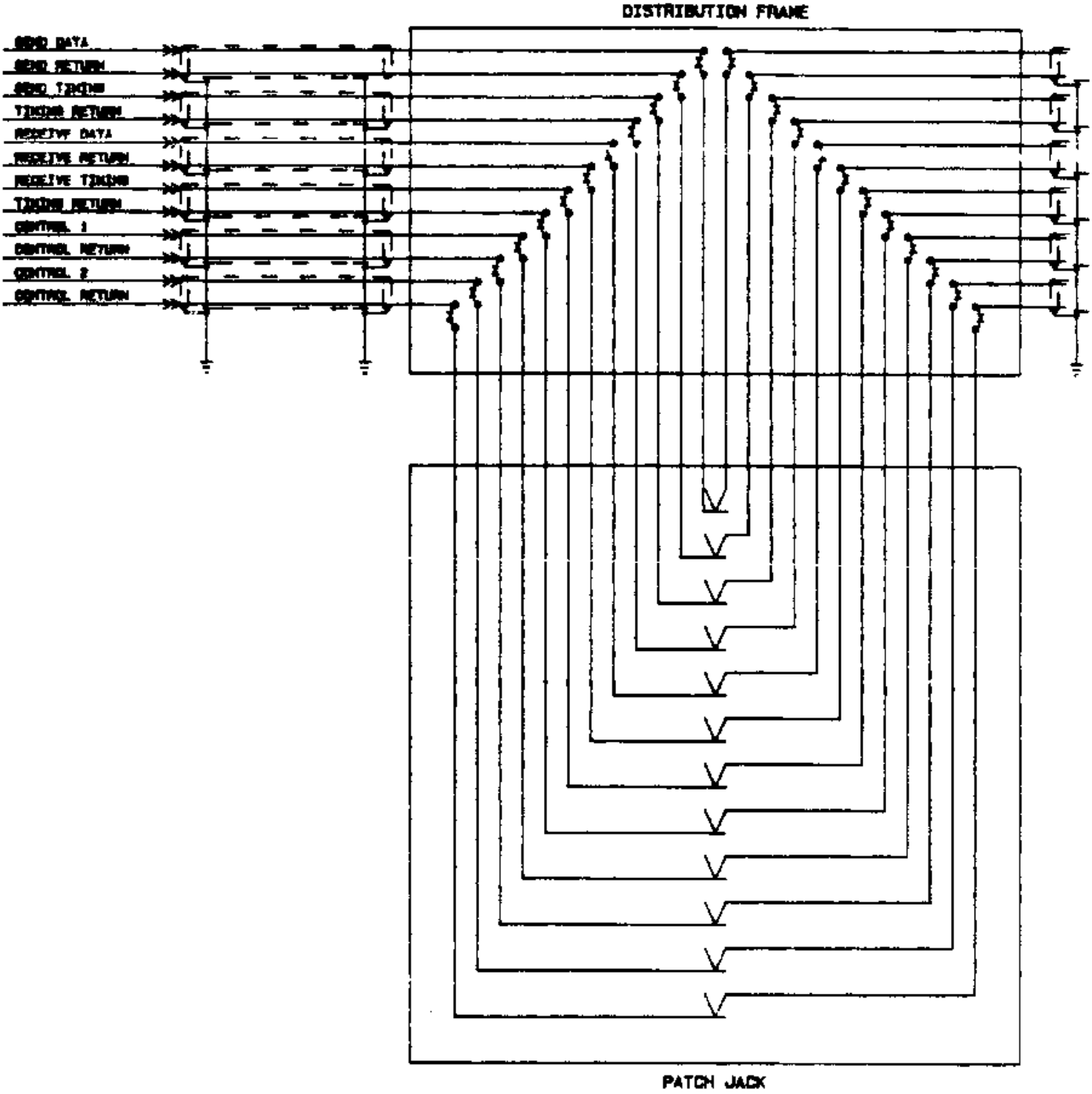


FIGURE 29. Balanced voltage digital signaling patching.

5.4.1.2.2 Unbalanced signals. Unbalanced voltage digital signaling depends upon a voltage relationship of a single line referenced to a signal ground. This may be implemented by a single signal ground wire in each cable between two devices, a return link for each signal with all returns terminated on a common bus at each end, or each device referenced to a station ground system. A separate return for each signal is preferred. because this arrangement reduces crosstalk between pairs, and increases the distance which a signal may be driven. It further permits single-ended drives to interface balanced receivers. (See MIL-STD-188-114.) Signals between devices should not he referenced solely to the station ground system.

5.4.2 Installation. Cable installation techniques contribute significantly to reducing RFI/EMI in a facility. Two cable types are predominant with variations -- twisted pair and coaxial cable.

5.4.2.1 Twisted pair. Twisted pair wire is the most common medium used. It is normally installed with multipair cables. Whether to use one overall shield or individually shielded pairs depends on the application. Many applications can be satisfied with one overall shield. Typically, the use of individually shielded pairs results in approximately 3 dB additional attenuation. Twisted pair may be terminated with crimp on solderless connectors, soldered to terminal posts, or wrapped around a Post in tight spirals. Wire wrap is the best technique for terminations because the post bites into the wire, creating a more positive bond. Solder is the least acceptable method due to the high probability of cold solder joints which increases the resistance of the bond.

5.4.2.2 Coaxial cable. Coaxial cable is used in applications where high frequencies are required. Coaxial cable, with its center conductor equally spaced from the outer shield throughout its length, exhibits wide bandwidth due to reduced skin effect and reduced distributed capacitance. Coaxial cable should be terminated only with appropriate connectors.

5.4.2.3 Variations. Triaxial cable is coaxial cable with an additional shield. Its termination should be in accordance with manufacturer’s instructions. Twinaxial cable is twisted pair, encased in a dielectric foam, covered with a braided shield. It may be used where balanced drive at higher frequencies is required and where a high probability of EMI exists. Quadraxial cable is twinaxial cable with an additional shield.

5.4.3 Terminations.

5.4.3.1 Facility entrance plate. Any signal cable entering a facility should pass through a facility entrance plate. The facility entrance plate serves as the point where undesired signals are shunted to ground. where shields are grounded to dissipate induced currents, and where TPDs are installed. Filters on signal lines are circumferentially bonded to the plate, in order for shunted currents to have a low impedance path to ground. Some signal lines may not require filtering at the entrance plate if filtered at the last equipment, provided the plate has not been installed for EMP purposes. The facility entrance plate then serves as the point to bond the shield to a low impedance path to ground. Fiber optic lines should penetrate the shield through waveguides-beyond-cutoff. A waveguide-beyond-cutoff is sized at a 5 to 1 ratio of length to maximum cross-sectional dimension. Typically, attenuation of 136 dB can be achieved at frequencies well below cutoff. Cutoff frequency is calculated at wavelengths equal to twice the largest dimension of a rectangular waveguide. Thus, 0.5-inch conduit has a cutoff frequency of approximately 1 GHz, while a 1-meter by 2-meter personnel

tunnel has a cutoff frequency of 75 MHz. Each conductor entering and exiting the facility must be equipped with protection devices to shunt the high voltages, high currents, and high-frequency pulses caused by power faults, lightning, or HEMP. Metal oxide varisters (MOVs), gas-filled spark gaps, and carbon blocks are used in various combinations to achieve protection. Low-voltage protection devices are also installed on the facility entrance plate.

5.4.3.2 Distribution frames (DFs). DFs are used to provide a means to configure internal equipment for various applications. Typically, DFs connect egressing lines to modems, modems to COMSEC devices, and COMSEC devices to terminal equipment. A DF must be sized to accommodate every signal line and its return and to provide a point to ground the shields to the equipotential ground plane. The shield grounding scheme must allow for the shortest possible exposure of unshielded pairs. This scheme must also provide a minimum impedance path to the equipotential ground plane. Where possible, the DF should also incorporate shielded pairs to effect crossconnects. DF technology includes taper pins, connectorized backplanes, solder lugs, insulation displacement techniques, and wire wraps (see figure 30). Taper pins are simple to terminate, but tend to corrode rapidly, resulting in poor bonding. Connectorized backplanes do not provide sufficient backshell contact to assure shield integrity unless the shields are terminated separately in some manner other than the backshell. Insulation displacement techniques rely on spring tension to grasp conductors but lack a large surface area contact. Solder lugs are prone to cold solder joints. Wire-wrap methods are the most reliable termination techniques due to high mechanical reliability and large surface area contact. DFs should be contained in metallic cabinets in RED areas. Separate DFs are needed for each application (i.e., a RED digital DF for the RED equipment to RED patch bays to COMSEC; a BLACK digital DF for COMSEC to BLACK patch bays to modems, etc.). If DF's are housed in metallic cabinets, the cabinets should be sized large enough for maintenance access.

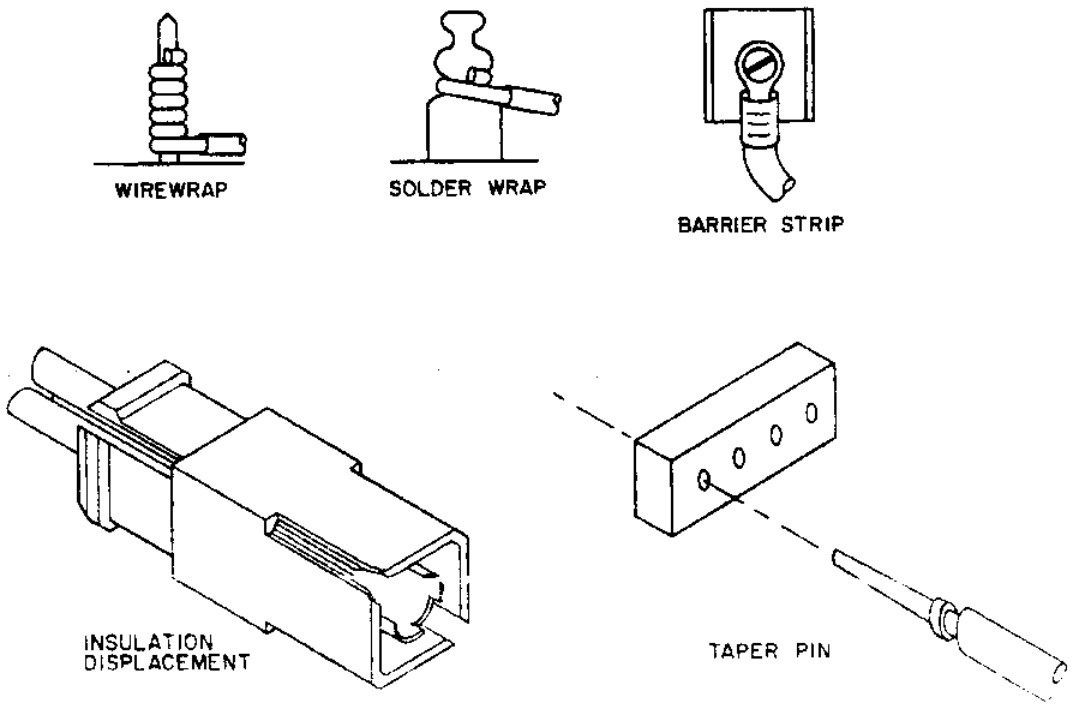
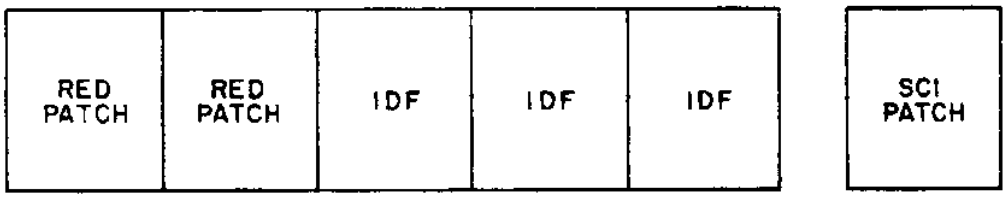


FIGURE 30. Termination techniques.

5.4.3.3 Patch panels. Patch panels are used to substitute equipment or lines when failures occur. Patch panels must be designed to allow all required signals to be transferred from one equipment or line to another equipment or line with the least effort. Each patching position must have sufficient contacts to transfer not only the signal lines, but all returns (see figure 29). The Designer should consider all signals to be balanced and provide the appropriate patching. For RED patching where like items of equipment serve different communities of security, separate patching for each community is required. These panels must be physically separated to prevent patching from one to another (see figure 31). It is preferred that different patching media be used (see figure 32). If separation and physical difference cannot be used, then dissimilar wiring of each patch position may be used (see figure 33). The dissimilar wiring should take a form that effectively inhibits circuit operation when an operational mispatch is made. For instance, if a signal line used to initiate a crypto-resynchronization were to be reversed with a clock line, should a mispatch occur, the crypto-equipment would be continually in resynchronize mode, but could not operate due to the lack of the clock signal. Dissimilar wiring should be used only if other methods cannot be used. Small facilities should use crossover switches in lieu of patch panels (see figures 34 and 35).

5.4.3.4 Equipment terminations. Equipment terminations present the designer and installer with a variety of possible termination techniques. Termination may be on barrier strips with crimp connectors, wire wrapped to backplane pins, fanned and soldered to printed wire boards, or on wide variety of connector plugs. However, some general rules can be applied. The designer and installer must be aware of typical interface schemes in order to understand the termination scheme and take actions to overcome the shortcomings of particular interfaces. Digital interface schemes can be classed as follows: balanced voltage digital signaling, unbalanced voltage digital signaling (see figure 36), and loop current (see figure 37).



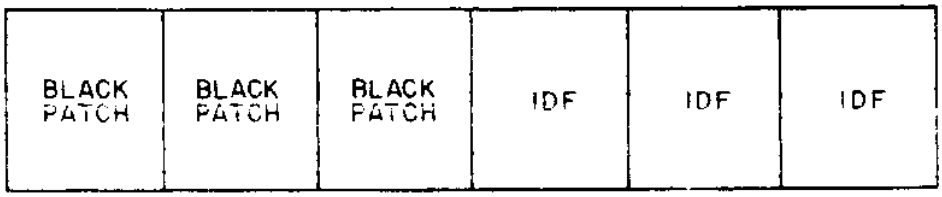


FIGURE 31. Patch facility layout.

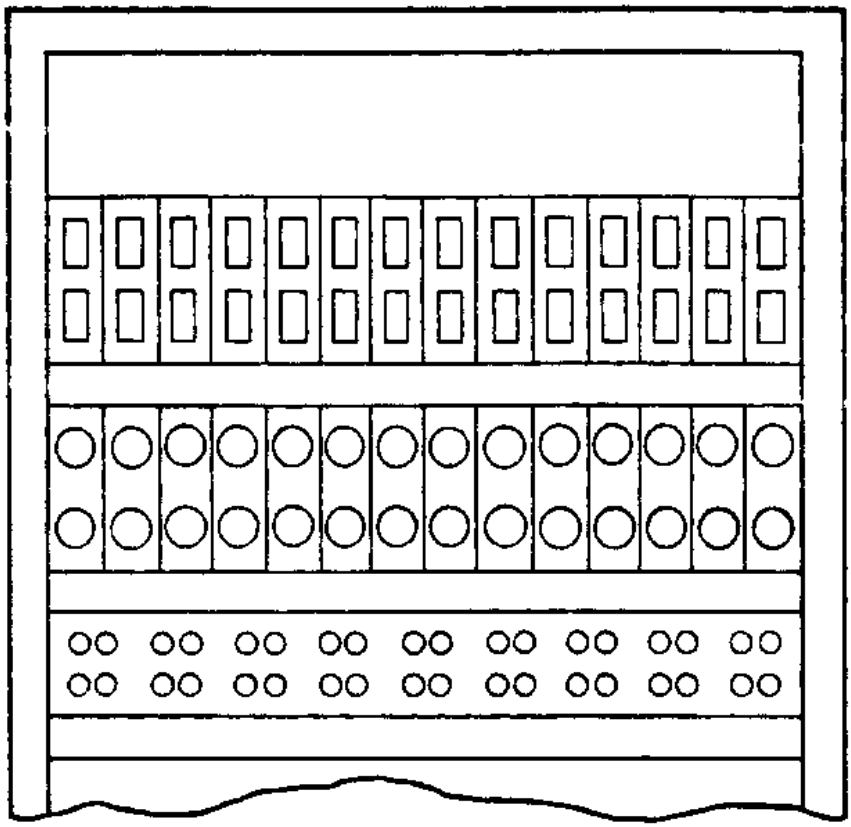


FIGURE 32. Dissimilar patching.

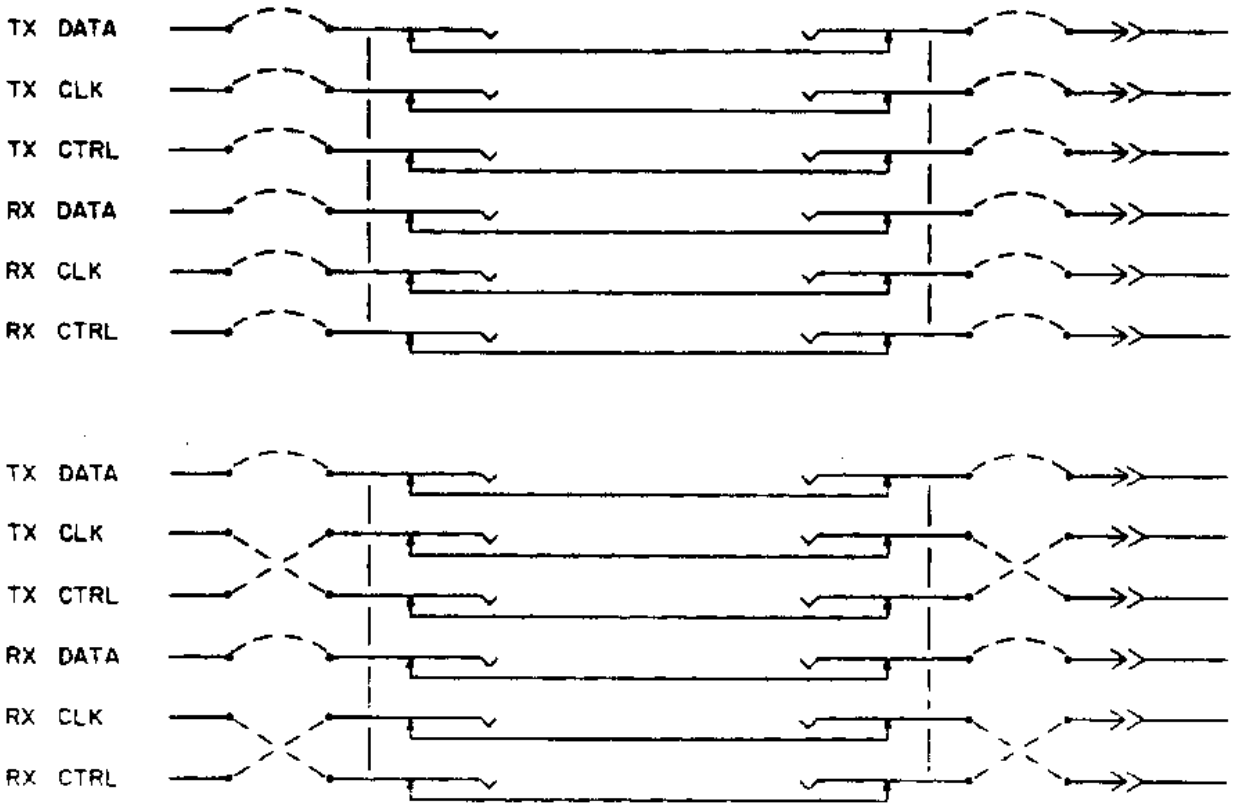


FIGURE 33. Dissimilar wiring.

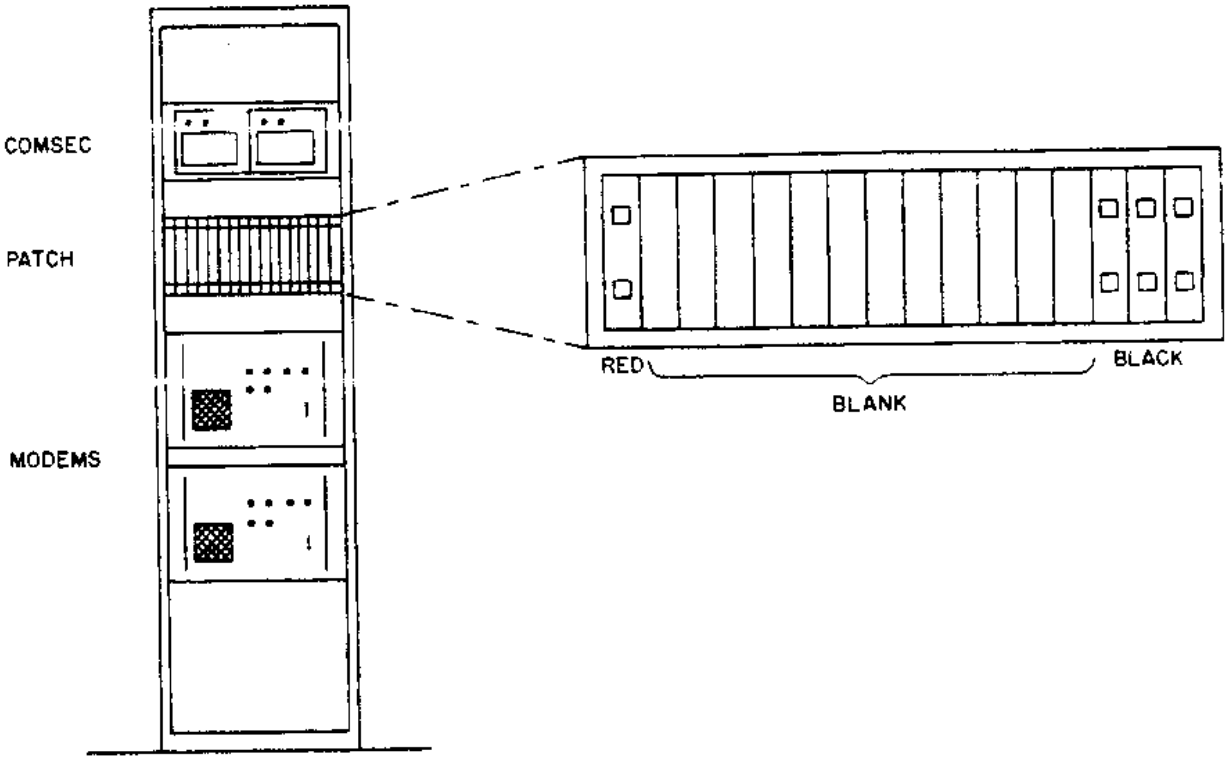


FIGURE 34. Small facility cross switching.

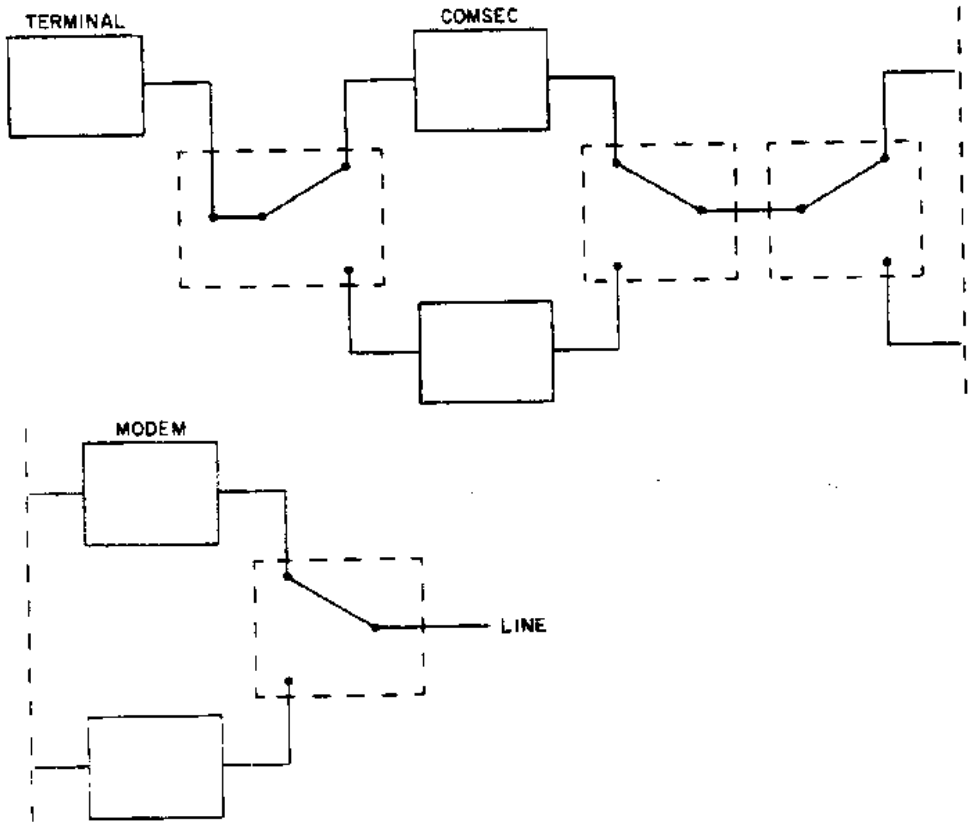
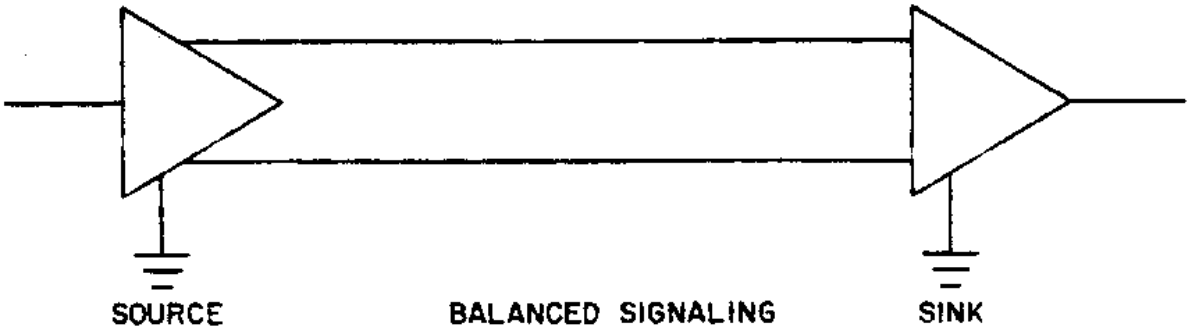


FIGURE 35. Small facility cross switching (schematic).



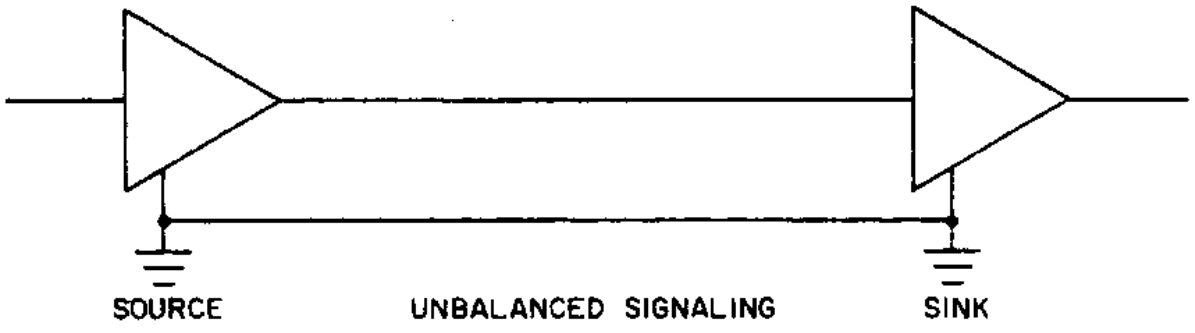
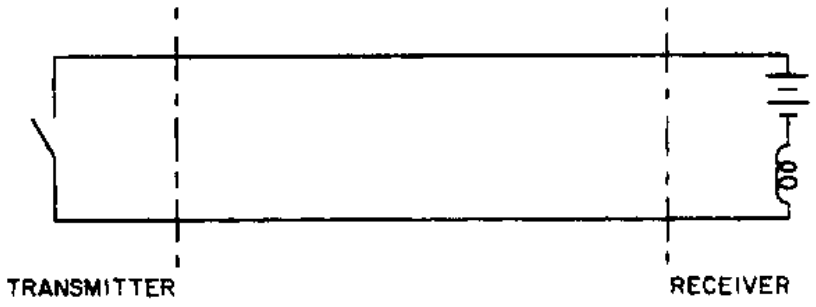
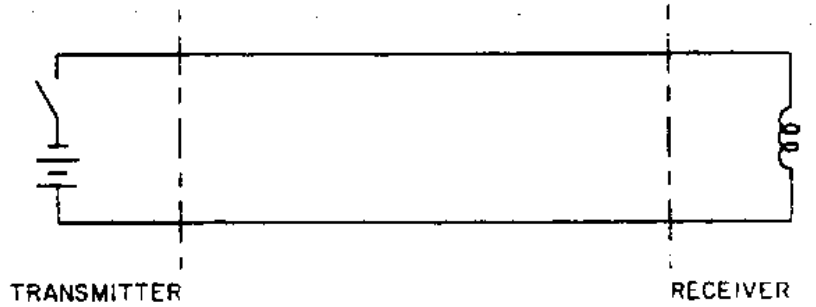


FIGURE 36. Signaling interfaces.



DRY CONTACT SIGNALING



WET CONTACT SIGNALING

FIGURE 37. Loop current.

5.4.3.4.1 Balanced voltage digital signaling. The preferred signaling method is balanced voltage digital signaling. Balanced voltage digital signaling relies on detection of a specific difference of potential between two points, regardless of the relation of either line to a ground reference. balanced voltage digital signaling's most significant characteristics are reduced crosstalk and greater distance at higher speed. This is achieved by a constant difference of potential between conductors over the length of the cable.

5.4.3.4.2 Unbalanced voltage digital signaling. Unbalanced voltage digital signaling differs from balanced in that the signal line difference of potential is to a common signal reference point. A poor installation, or excessive distance between the source and sink, often results in a significant difference of potential between the signal and the reference.

5.4.3.4.3 Loop current. Loop current has been predominantly used in teletypewriter or telegraph applications. Loop current interfaces should be treated as high level (see 5.2.2). Currents of 20 or 60 milliamperes are common. A loop current circuit consists of a loop which is alternately opened and closed to allow current to flow, or alters the polarity of current. Two types of current loops are prevalent -- dry contact and wet contact. In dry-contact signaling, the current source is in the receiver. The transmitter closes and opens the circuit, providing a complete path for the current. In wet-contact signaling, the current source is in the transmitter. The most common loop-current signaling schemes are neutral (single current) and polar (double current). Polar is the more prevalent of these schemes.

5.4.3.5 Commercial standards. The designer and installer may be faced with commercial interfaces which may or may not allow the use of individual returns. The more commonly used commercial interfaces include Electronic Industries Association's (EIA) RS-449 and RS-232C. Most commercial interfaces share a common problem which jeopardizes shielding and could be a potential TEMPEST problem. Connector backshells typically are plastic, which does not provide a means of closing the shield. While some metallic backshells may be available, most cannot be relied upon to be RFI tight. Further, the mechanical mating schemes often do not provide sufficient bonding to permit adequate electrical shield integrity. In general, the designer may find commercial equipment to be a source of RFI, unless procurement specifications clearly dictate that adequate measures be taken by the supplier to correct such deficiencies.

5.4.3.5.1 EIA RS-449. This interface conforms to the basic assumption of this handbook in that all data and clock signals have individual returns. The interface is implemented using a 9-pin connector (simplex, send only) and a 37-pin connector (full duplex). The 9-pin connector may not be provided. The interface, has a significant shortcoming. Pin 1 is designated to terminate the cable shield. As typically implemented, pin 1 takes the shield currents into the equipment in order to shunt those currents to ground via the power FPSS. In some equipment, this may be the chassis, which may also be the neutral reference. This may result in noise on the power or neutral currents being introduced on the shield. The shield, then, should not be terminated on pin 1. If the equipment is provided with a metallic backshield, and the shield is circumferentially bonded, a shield grounding wire should be attached to the backshell and run to the equipotential plane.

5.4.3.5.2 EIA RS-232C. This unbalanced interface is the more prevalent interface used in commercial equipment. The electrical characteristics are similar to the unbalanced interfaces defined in MIL-STD-188-114. A single signal ground/common return is provided on pin 7, which is identified as circuit AB. This is contrary to the guidance of this handbook, which advocates separate return paths (see 5.4.3.5.4). Cables should be manufactured on site to provide a separate return for each signal using twisted pair cable. At the connector, the returns are tied together, then terminated on pin 7. An alternative is the use of a commercially available RS-232-to-RS-449 adaptor plug. Cables are available to support RS-449, thus negating the need to make new cables. The standard also presents a problem with proper signal grounding. These items of equipment typically do not provide a signal ground stud that connects the equipment to the signal ground reference. The EIA standard states, "A protective ground is provided in the interface cable, terminated on pin 1 identified as circuit AA. Pin 1 is further bonded to the equipment frame. It may be further connected to external grounds as required by applicable regulations. Most often this is connected to the fault protection subsystem. The signal ground/common return which establishes the signal reference is brought to ground only in the data communications equipment. Provision is made to connect circuit AB to circuit AA, which may be removed on site." (See figure 38.) This portion of RS-232C presents very serious problems. First, a fault current on one chassis may flow into the second chassis, causing damage to the equipment and cable. Second, signal return, being coupled to the FPSS, presents the possibility of RED data appearing in the BLACK area. The standard further states circuit AA is optional, while circuit AB is mandatory. To overcome.this situation, the following retrofit actions are suggested:

a. If circuit AB is strapped to circuit AA, remove the strap.

b. In the cable connector, terminate the circuit AA lead on the circuit AB pin.

c. Provide a method to run a low-impedance signal ground conductor to the equipotential ground plane. (See MIL-HDBK-419.)

NOTE: Equipment designed to commercial standards and some Government equipment is designed for environments in which the only available ground is the FPSS. Typically, the equipment chassis may serve as the neutral power reference and signal reference. Such conditions may violate codes and standards. Further, the FPSS is bonded to the frame. In such situations, it is impossible to properly separate the grounds. As a minimum, the protective ground must not be taken between equipment via the interface cables.

5.4.3.5.3 Other interfaces. Other interface schemes exist which have not become de facto standards. The designer should use the knowledge of the problems in the EIA interfaces to examine other interfaces to determine and correct any problems which may be encountered.

5.4.3.5.4 Mixed interfaces. An installation may include equipment with RS-449, RS-232C, and MIL-STD-188-114 balanced and unbalanced interfaces that must be interfaced together in various combinations. Figures 39 and 40 depict how these interfaces may be accommodated. Whether balanced or unbalanced voltage digital signaling is used, a dedicated signal return should be provided for each clock and data signal. While this required in balanced voltage digital signaling, it is not typical in unbalanced voltage digital signaling of RS-232C. The rationale for dedicated returns is threefold. First, by using twisted pair wire, the potential for crosstalk is reduced because the magnetic field created by the current in the return

cancels that on the signal line. Second, where multiple signals are in a single cable, the multiple return currents are not concentrated in a single conductor. Third, the use of a separate return assures the source and sink reference the same ground potential. In some instances, greater speed, distance, and improved performance may result. MIL-STD-188-114 contains extensive detail on considerations to be taken when terminating mixed interfaces.

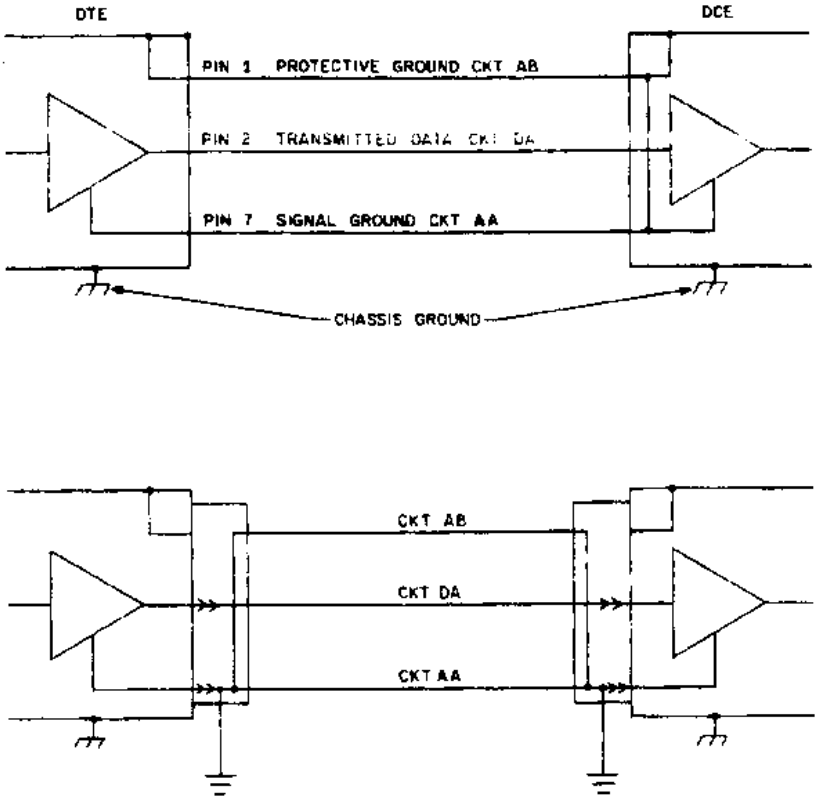


FIGURE 38. RS-232C interface.

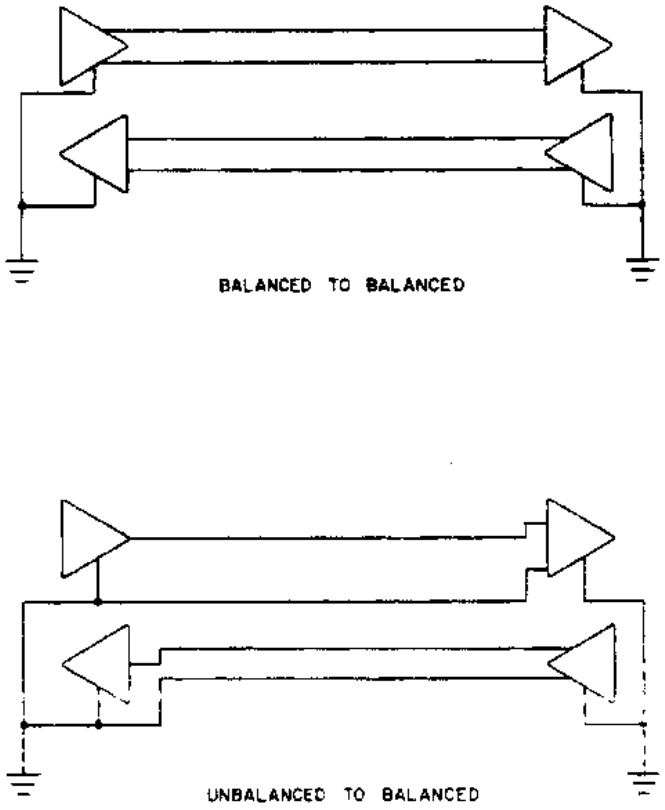
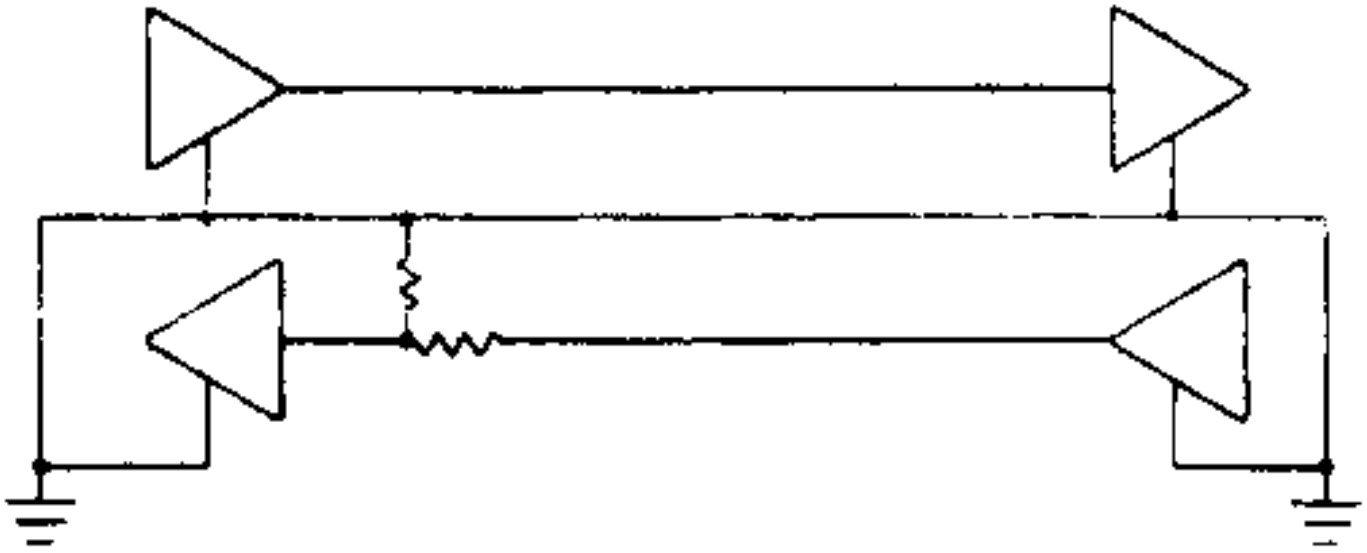
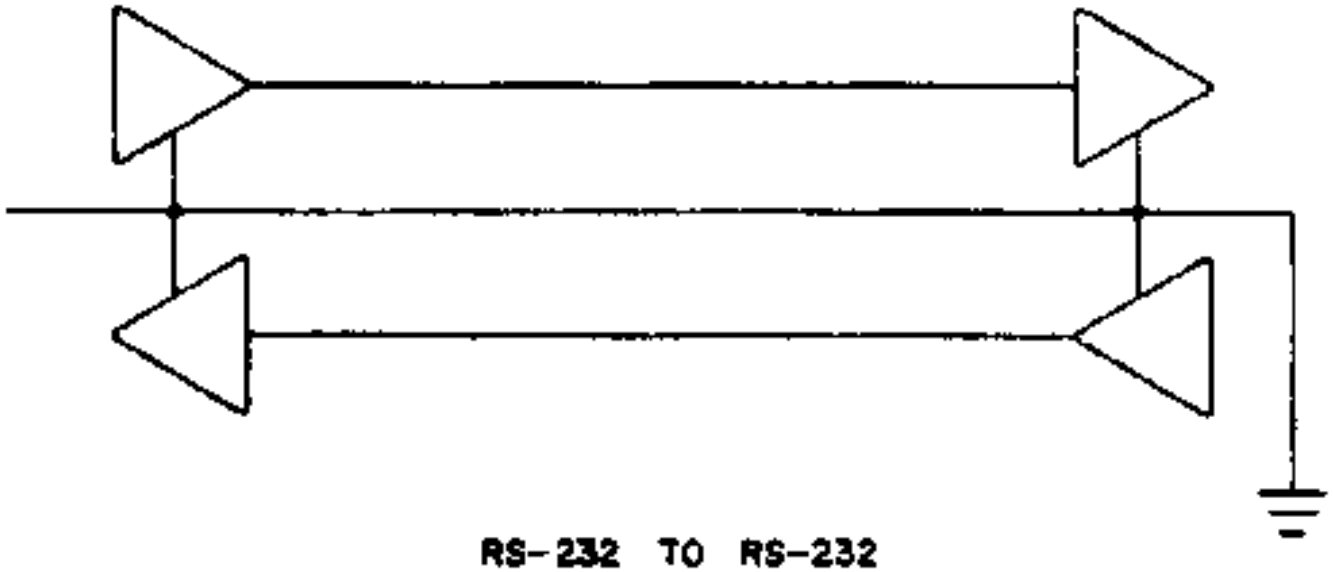


FIGURE 39. Mixed interfaces (general).



MIL-188-114 UNBAL TO RS-232



RS-232 TO RS-232

FIGURE 40. Mixed interfaces (specific).

5.4.4 Cable distribution. Cable distribution engineering and installation should be done in a sequence from the terminal equipment outward to the egress of the LEA. This method assures all required lines are in place, RED/BLACK boundaries are maintained, and all lines are accounted for and properly treated. Cabling is classed in three groups: cables between equipment in the RED area, cables from RED equipment to COMSEC devices, and BLACK cables.

5.4.4.1 Routing. Where signal cables have at least one overall shield, cable ladders and trays may be used to route cables. Where unshielded cables are used, totally enclosed ducts, wire ways, and conduits are required. The use of unshielded cable should be avoided. Where positive barriers between RED and BLACK runs are deemed necessary, and extra physical protection is required, totally enclosed ducts, wire ways, and conduits are appropriate. Where RED and BLACK race ways must run parallel or cross, race ways will be separated per table 1. RED and BLACK cables are never run in the same wire ways, conduits, ducts, or cable ladders. RED and BLACK signals will not be

mixed in the same cable. Certain control signals associated with a channel are generated in the RED area and must be routed to the BLACK area to control some channel functions. If such signals are routed in the same cable as RED data, then the signals should be considered RED. Some isolation method must be incorporated at the RED/BLACK boundary for these signals (see 5.5.2).

5.4.4.2 Sensitive compartmented information facilities (SCIFs). Where Sensitive Compartmented Information (SCI) is processed in a joint classified facility, RED SCI cables and other RED cables may use the same wire way or conduit. Such signals will not be jointly routed in the same cable.

5.4.4.3 Nondevelopmental items (NDIs). Where NDIs are used as RED processors, the design of such items may not accommodate the use of shielded cable. In such cases, the designer and installer must exercise extreme caution in maintaining separation of RED cables. It may be necessary to distribute cable between NDI equipment separate from all other cables.

5.4.5 Filters and isolators. All lines egressing a facility may require filters or isolators at the point of egress of the LEA. Within the LEA, filtering might be used in the equipment design to prevent RFI/EMI. The designer should be aware of the possible existence of such filtering. In no case should a line be multifiltered between two points (see 5.5).

5.4.5.1 Filters. Filters are typically housed in RFI tight cabinets. Cavities within the cabinets have penetrations inward to the equipment, or outward toward the transmission media, but not both. The filters are firmly bonded to the walls to assure electrical integrity. Provision must be made at the entrance of the cabinet to bond and terminate the cable shields. When selecting filters, the designer must assure the filter impedance is compatible with the equipment driving the filter (see figure 41). The filter cabinet must be firmly bonded to the equipotential ground plane.

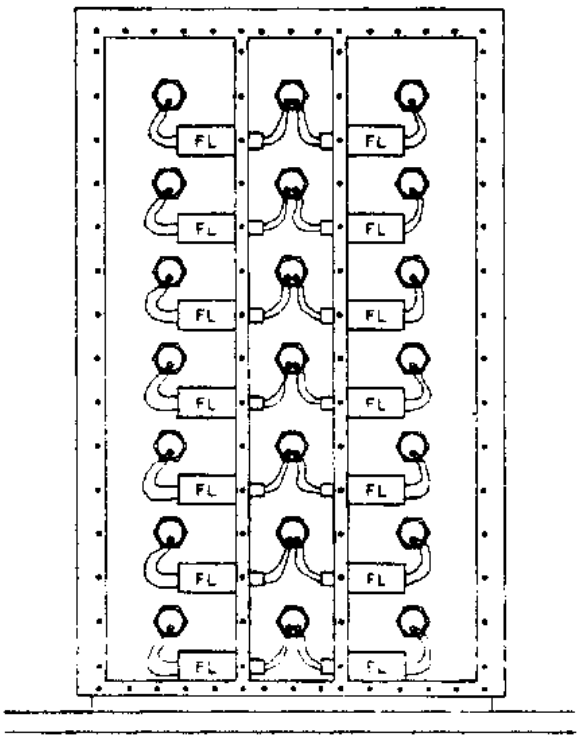


FIGURE 41. RFI filter cabinet.

5.4.5.2 Isolators. Isolators may be used at the point of egress or may be used to establish the RED/BLACK boundary, if so required (see figure 42). At the point of egress, optical or photon coupled isolators may be used. When used in a shielded facility, a drive module is coupled to a receive module via a FOC that penetrates the shield through a waveguide-beyond-cutoff. The isolators may be housed in RFI cabinets bonded to the shield to further guarantee the shield integrity. In order to limit the number of penetrations of the shield, channels may be multiplexed to drive the fiber optic isolator, then be demultiplexed after exiting the facility. Within the facility, a RED/BLACK boundary may be required for signal lines which must traverse both areas but do not pass through COMSEC devices. For lines which are used for control, have a low-frequency rate of change, and do not have critical rise times, relays may be used. Where higher speeds are needed, along with fast rise times, electronic relays or photon coupled isolators may be used. The ideal placement of this isolation capability is within the same area as the COMSEC equipment. The installation design must assure that the isolation mechanism cannot he bypassed.

5.4.6 Special considerations.

5.4.6.1 Patch and test facilities (PTFs). All facilities will incorporate some method to trouble-shoot defective equipment on a circuit. This may be as simple as a single jack field in a common equipment rack of a small facility to multiple patch racks with automated test and monitor capability in a large facility.

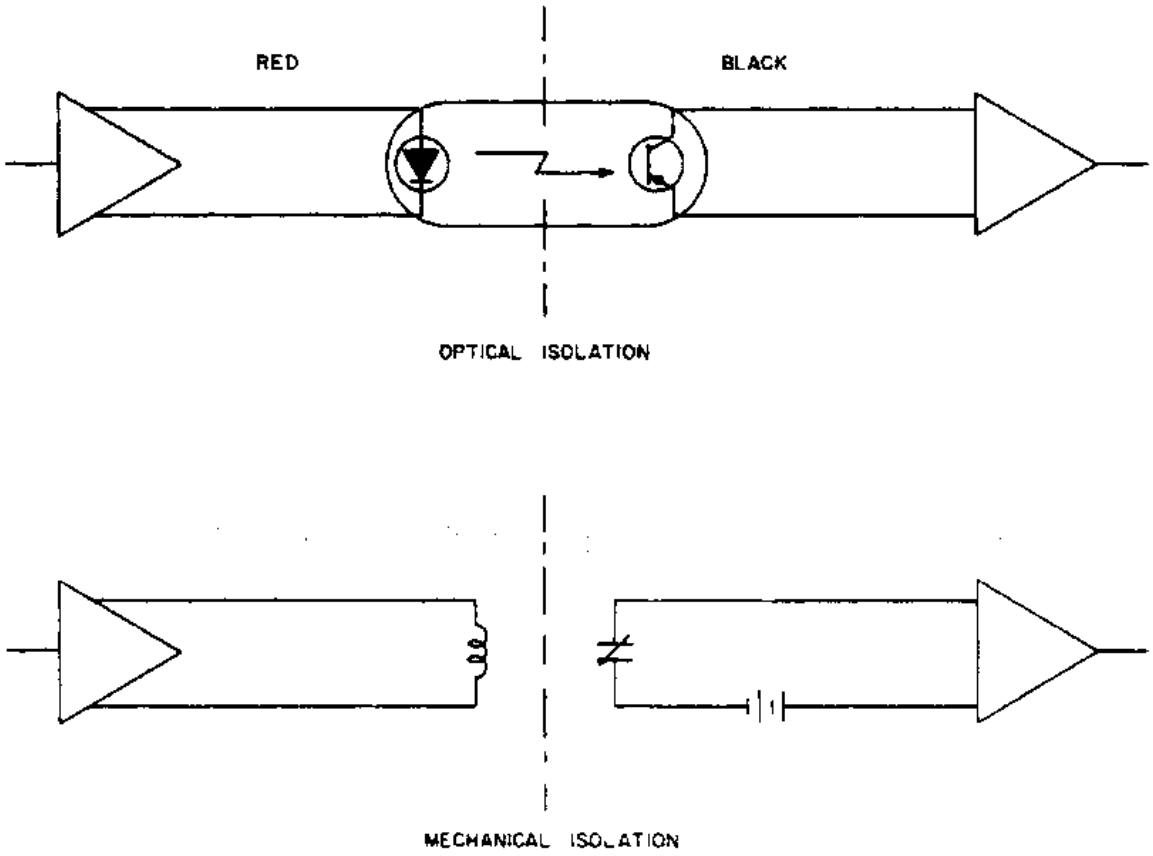


FIGURE 42. Isolator techniques.

5.4.6.1.1 General. The prime purpose of a PTF is the restoration and rerouting of circuits. The cardinal rule is continuity of the operations. The patching must include a provision for every wire on a circuit to be switched to another circuit. There must be no means of patching directly from the RED side to the BLACK side, or among different RED compartmented patches. In order to accomplish this restriction, four schemes may be used: physical separation, dissimilar patching, dissimilar wiring, and dedicated switching.

5.4.6.1.1.1 Physical separation. In larger facilities, identical patching equipment may be used for RED compartmented and noncompartmented digital signals and BLACK digital signals, provided each group is separated from the other by a distance greater than the longest available patch cord. Traditionally, manufacturers have not made cords greater than 6 feet (1.8 m) in length (see figure 31). The design should not include interbay trunking between compartmented and noncompartmented bays.

5.4.6.1.1.2 Dissimilar patches. It may not be possible to provide adequate separation in a facility. In this situation, dissimilar patches should be used to prevent patching into other communities (see figure 32).

5.4.6.1.1.3 Dissimilar wiring. If physical separation cannot be achieved, and dissimilar patches cannot be used, then each community should be wired to the patches in a unique manner. When designing the dissimilar wiring scheme, the goal is to cause the equipment to become inoperative should a mispatch occur. For instance, if a clock line and COMSEC control line were reversed, such as sync-initiate, a mispatch would put the clock on the control line, causing the COMSEC to continually attempt to resynchronize. Without the clock, the COMSEC could not operate (see figure 33). If multiple communities exist in a facility, dissimilar wiring may become too cumbersome to be practical.

5.4.6.1.1.4 Dedicated switching. Single channel facilities should not use patches at all, but should use A-B switches and x-switches to swap equipment (see figures 34 and 35).

5.4.6.1.2 Troubleshooting. Troubleshooting capability in a PTF may be as simple as plugging test equipment into a line or monitor jack, or as sophisticated as remote switching of test equipment into a line. Test equipment may include oscilloscopes, distortion analyzers, data scopes, bit error ratio testers, and pattern generators. If a switching matrix is used, separate matrices are required for RED and BLACK. Equipment used to trap and display data must not be capable of reintroducing that data into a circuit. If the equipment is to be used for both RED and BLACK testing, positive controls arc required to prevent crossing RED and BLACK signals. It may be necessary to certify this equipment using criteria for cryptographic equipment.

5.4.6.2 Local area networks (LANs). LANs are often described as privately owned optimized networks, offering reliable high-speed communications channels connecting information processing systems in limited geographic areas, such as offices, buildings, building complexes, posts, bases, camps, and stations with such services as word processing, data processing, electronic mail, and database management. LANs are becoming used increasingly because of the highly flexible nature of configurations and services which can be provided. LANs may be implemented using private automatic branch exchanges (PABX), broadband coaxial cable systems, and

baseband coaxial cable systems. FOC may be used in place of coaxial cable. Before a LAN is designed and installed, the responsible agency must ensure the host software is capable of supporting the levels of security required. Commercially available software typically does not support multiple security levels. Thus, all users must operate at the same security level. It may be possible with emerging technology to create a hierarchy of hosts and LANs connected by gateways which allow higher level users to access lower level hosts, but prohibit lower level users from accessing higher level hosts. DoD and service directives and regulations should be consulted to define the parameters and criteria for trusted software.

5.4.6.2.1 PABX LAN. LANs may be implemented via PABX where the nature of use is short-term connection, low-speed operation, and low-volume data transfer. The PABX may serve a particular area, building or complex, or it may be the base central office. Data rates up to 9.6 kbps may be supported. With the advent of digital branch exchanges, speeds up to 56 kbps may be achieved. When a PABX is used to implement a LAN, a secure network can be designed by including approved encryption devices and techniques in the system. A PABX-based LAN consist,, of on-call point-to-point links. This allows a terminal to establish a link to only one other point at a time. When a link is thus established, it can be secured for the duration of the connection. Terminals and hosts can then be designed using the techniques of this handbook with clear RED/BLACK boundaries. When such features as electronic mail are part of the system, it is assumed the receiver is responsible for accessing his mail box to retrieve messages or obtain other information. Thus, the design would exclude autodial capability by the host and autoanswer capability by the user.

5.4.6.2.2 Broadband LAN. Broadband LANs use frequency-division multiplexing on a coaxial cable to establish a communications network. The technology is similar to that developed for cable television. Typically, the bandwidth of a broadband system is 300 to 400 MHz. Such LANs are intended to support low-speed data, video and voice on a single physical medium. Bands of frequencies are established for each type of service. For instance, a band might be established between 10 to 25 MHz. This band could be further divided into 4000-Hz subchannels. Broadband, then, should he viewed as any other transmission medium if each subchannel is used by only one user. Transmission between the host and user would be encrypted and modulated, thus the medium is transparent to both. If multiple users share a subchannel, then the entire system must be RED if processing classified information.

5.4.6.2.3 Baseband LAN. Baseband LANs use baseband signaling on a single physical transmission medium. Data rates of 10 Mbps are achieved between nodes. Up to 1000 nodes may exist on a LAN. Some nodes may exist as terminal servers, each supporting multiple terminals. Such LANs also use multiple levels of protocol or function layers. At the present time, baseband LANs present significant challenges and risks in secure applications. All users have perpetual connection to all other users, The most significant problem, then, is how to establish privacy between any two users. Although development is underway, such a technique does not exist. Therefore, in order for a baseband LAN to be secure, it must he installed in a PDS. All users on the baseband LAN must operate at the same security level. Physical security measures must be quite stringent since no RED/BLACK barrier exists to protect the network. Baseband LANs should be kept as small as possible, and should not use gateways to other LANs.

5.4.7 Fiber optics. The use of FOC has been touted as the ultimate bonded medium for transmission of classified information because of its inherent property of neither radiating nor absorbing energy (RFI, EMI). While FOC is electrically immune, it does require physical protection. If FOC is used as a plain text medium between controlled access areas (CAAs) and crossing uncontrolled access areas (UAAs), the FOC must be installed in a PDS (see 5.7.3).

5.5 Filter and isolator requirements and installation.

5.5.1 Filters. Filters are used to pass signals or currents at certain frequencies to the load, while shunting unwanted frequencies either to ground or back to the source (see figure 43). Filters may be either passive or active. Passive filters are most commonly used for RFI/EMI control. Four types of passive filters may be used: lowpass, highpass, bandpass, or bandstop (see figure 44). Passive filters use an inductive impedance and a capacitive impedance to achieve the purpose. One impedance is in series with the load, while the other impedance is in parallel with the load. The parallel impedance shunts the undesired frequency. Filters are constructed in three network configurations: L or half-section, T, and Pi (see figure 45). The L network is the simplest, with the impedances connected as single components. The T network splits the series impedance in half, with half before and half after the shunt impedance. The Pi network splits the shunt impedance in half, with half before and half after the series impedance. The networks may be stacked to satisfy particular applications. Voice frequency (VF) and power filters can be purchased off the shelf, while filters for other applications are custom-made.

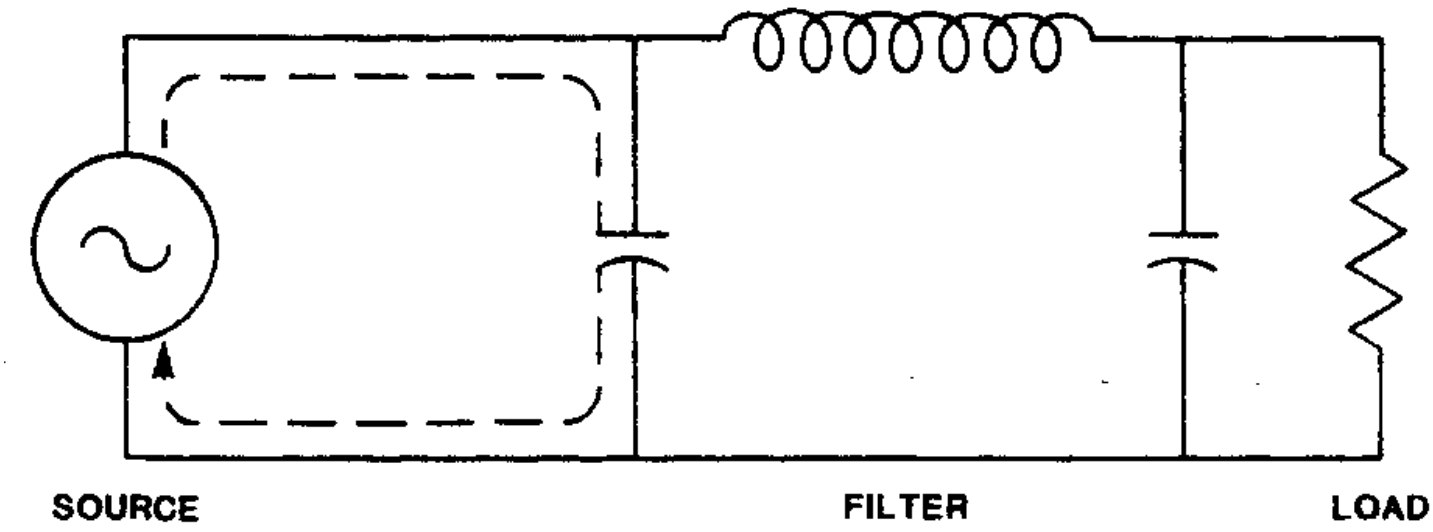


FIGURE 43. Typical filter operation.

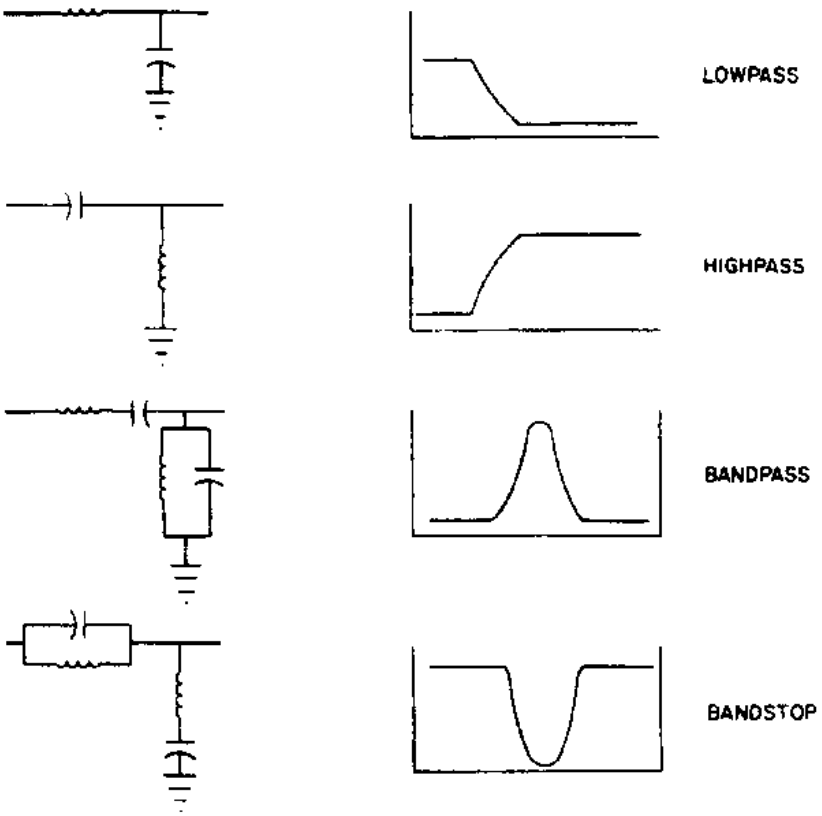


FIGURE 44. Filter action.

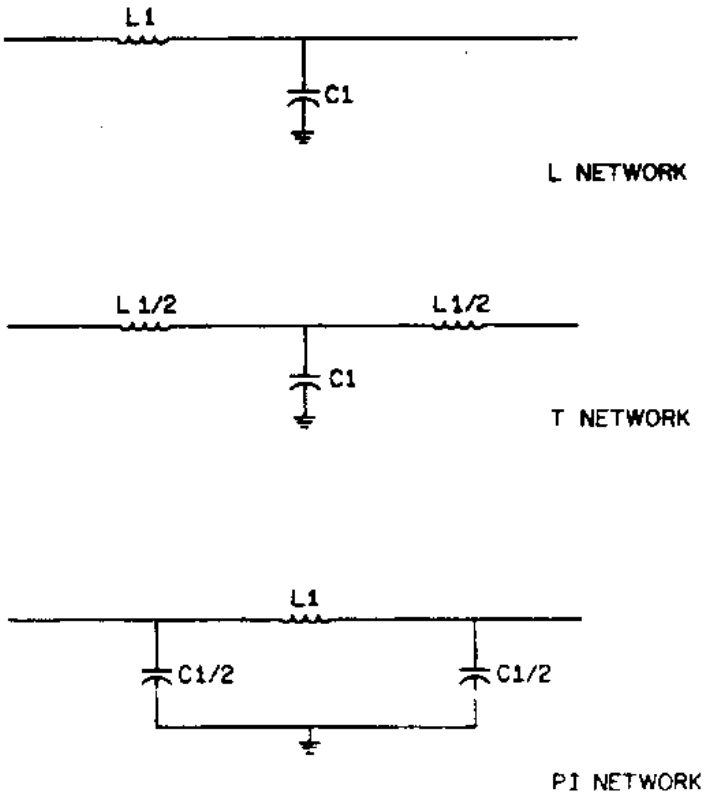


FIGURE 45. Filter construction.

5.5.1.1 Lowpass filters. Lowpass filters pass signals or currents below a specified cutoff frequency and attenuate frequencies above the cutoff. In lowpass filters, the series impedance is inductive, while the shunt impedance is capacitive. Lowpass filters are most commonly used as power-line filters and VF filters.

5.5.1.1.1 Power-line filters. Power-line filters are used to remove transient signals and RFI inducted on the lines from other sources, and to attenuate frequencies in the power system originating in the on-off cycling of motors. Power-line filters, if required, should be installed in the individual equipment rather than filtering the source of the power at the first service disconnect. This bulk filtering at the first service disconnect has distinct disadvantages in facilities, because the filter chosen by the designer must be selected based upon the maximum load on that service. Since the calculated load may be quite high, and the installed load may vary across the range of the ampacity of the filter, it is difficult to construct a filter that adequately attenuates the undesired frequencies. Further, the larger the ampacity of the filter, the more difficult is its physical construction. Filtering within the equipment results in reduced physical size and tailoring of the filter components to a relatively constant load. If RED equipment is used that is not TEMPEST approved, filtering may be needed. The preferred method is to install filters at the equipment, rather than bulk filter all such equipment (see figure 46). In no case should bulk filtering and individual filtering be used on the same equipment, since double filtering results in a composite filter of different characteristics which results in increased power consumption and reduced frequency cutoff (see figure 24). The waveform photographs (see figure 47) depict the effects of double filtering in a multiphase power system. The line side photos are the critical bus output of a rotating UPS. The load side photos are of one load center out of fourteen. The wave deformation at 90 degrees and 270 degrees is a synchronizing signal added by the UPS control circuitry. All equipment on this particular load center are TEMPEST approved devices using power-line filters within each equipment (see figure 48).

5.5.1.1.2 Voice frequency (VF) filters. VF filters, having a range of 300 to 4000 Hz, are used in facilities to filter audio signals for telephone lines and modems. These filters are used to prevent RFI from upsetting equipment and to contain RFI generated in a facility so that it is not carried outside the facility. VF filtering is normally accomplished at the point of egress from the LEA. The use of lowpass filters is satisfactory for voice band lines, but may not be satisfactory for quasi-analog modem lines. Modems using amplitude modulation or phase-shift keying should use bandpass filters with a center frequency equal to the carrier frequency of the modem. The rationale is that in the event a potentially compromising signal should be coupled into a line at VF, the lowpass filter would not attenuate that signal.

5.5.1.2 Highpass filters. Highpass filters are characterized by a high impedance below a cutoff frequency, passing all signals above that frequency. These filters may be used to remove signals induced by power lines from signal lines. While this filter is not normally used for TEMPEST purposes, the facility designer may find it necessary to use it for EMI purposes.

5.5.1.3 Bandpass filters. Bandpass filters are characterized by a low impedance at a specified band of frequencies with a high impedance at frequencies below and above that band. Such filters are typically used in equipment that use frequency-division multiplexing, such as voice frequency telegraph terminals, to breakout individual channels.

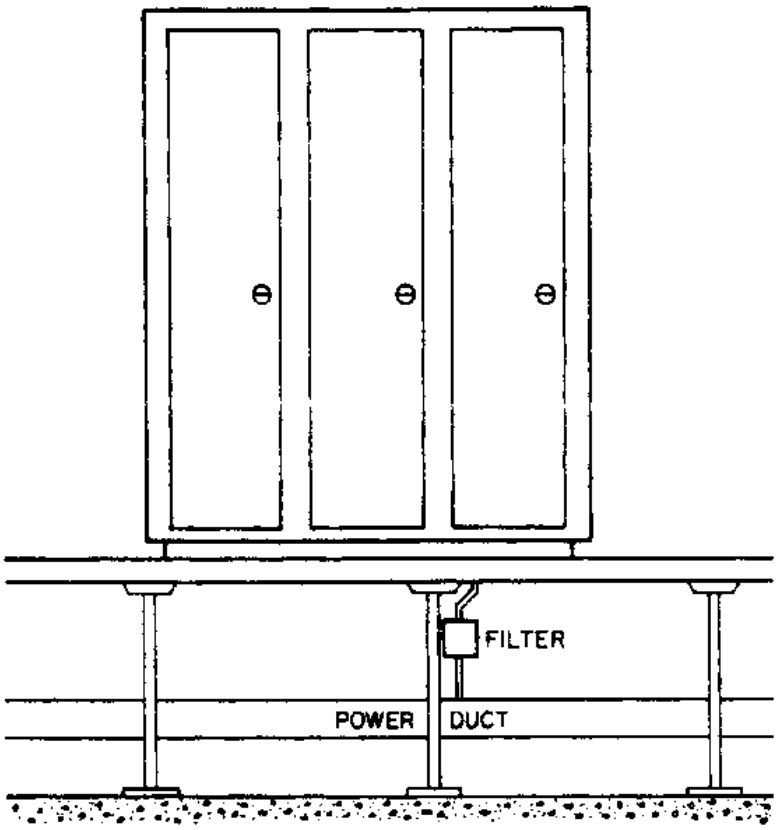


FIGURE 46. Equipment filtering, preferred method.

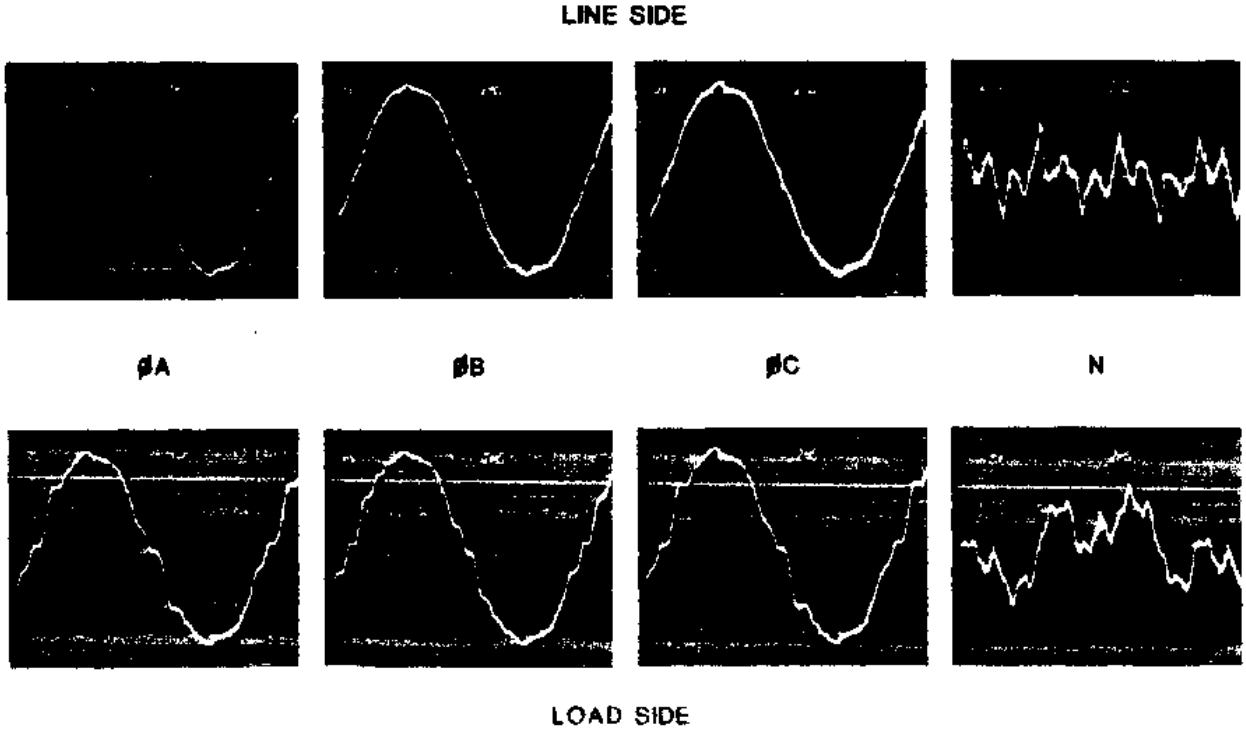


FIGURE 47. Double filtered waveform distortion.

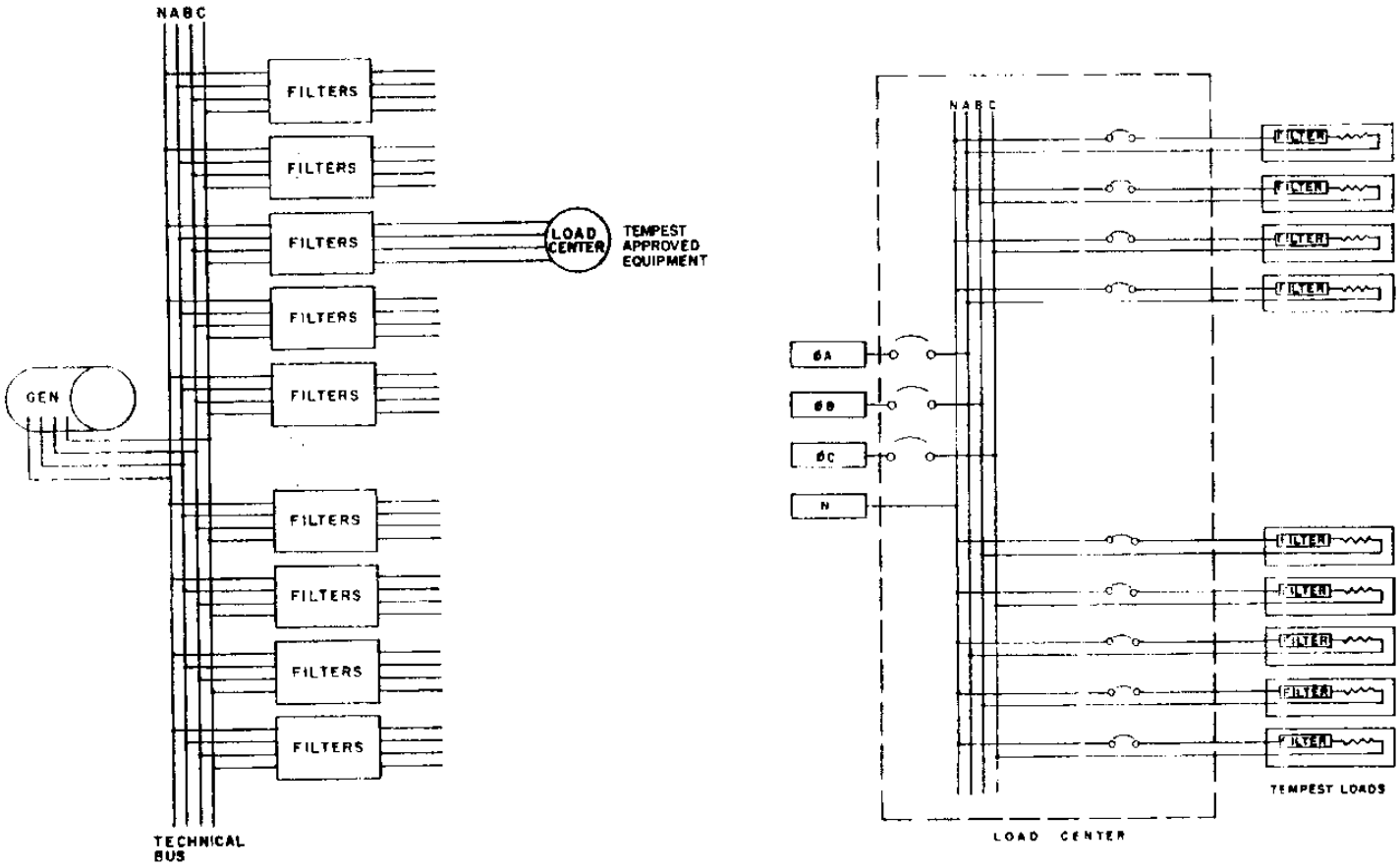


FIGURE 48. Power system double filtered.

5.5.1.4 Bandstop Filters. Bandstop filters operate opposite to bandpass filters in that a high impedance is present over the specified band of frequencies, while a low impedance is offered above and below that band. Bandstop filters may be used to block selected frequencies for EMI.

5.5.1.5 Filter parameters. Regardless of the type of passive, filter used, the facility designer must consider certain characteristics in selecting filters. The ideal situation would be to design and procure filters for each application. However, time and cost normally dictate the use of general purpose, readily available filters. Parameters to consider are: insertion loss, voltage drop, overcurrent rating, and maximum temperature rise at rated current. For power lines and VF signal lines, the following values are typical:

Insertion loss	Not less than 100 dB, 14 kHz to I GHz
Voltage drop	Not greater than 1% at full load
Over current	140% for 15 minutes
Temperature rise	Not greater than 25 deg. C above ambient at 100 A (proportionally lower for less current)
Leakage	Not greater than 0.5 mA between the case and ungrounded conductors

For highpass, bandpass, and bandstop filters the designer should select filters with an insertion loss of 100 dB for unwanted frequencies. All other parameters apply as stated.

5.5.1.6 Filter installation. Filtering at the point of egress is accomplished in the EM vault (if the facility is so equipped), or on the facility entrance plate. The filters are circumferentially bonded to the plate. Within the facility, filter cases for signal lines are bonded directly to the equipotential ground plane. Power-line filters are bonded to the equipment chassis and the FPSS.

5.5.1.7 Neutral filtering. The need to filter a neutral conductor in a facility may be dependent upon the adequacy of its ground system and the physical plant of that facility. A decision to filter the neutral conductor should be delayed until the facility is installed in order to evaluate the ground system. Measurements of neutral voltage to ground should be made at different points between the source and the load. If a difference of potential of less than 1 volt is consistently found, then neutral filtering may not be indicated. If a greater potential exists and cannot be corrected, then neutral filtering may be indicated. Strict compliance with the criteria in MIL-STD-188-124 and the guidance in MIL-HDBK-419 should eliminate the neutral filter requirements. This handbook assumes such compliance and assumes dedicated source power as described in paragraph 5.2.1.3.1 (i.e., that the power service transformer and first service disconnect are totally within the CS and that appropriate physical security has been applied to the CS). Small facilities that are installed in existing structures (e.g., wire rooms in embassies, consulates, etc.) cannot be expected to meet the above assumptions. In these cases, neutral filtering is indicated. When neutrals of polyphase systems are filtered, the neutral filter must be capable of passing the third harmonic of the combined frequencies of the phases (e.g., 450 Hz for 3-ph 50 Hz, 540 Hz for 3-ph 60 Hz).

5.5.1.8 Active filters. Active filters use operational amplifiers with externally applied resistances and capacitances to achieve filtering without the physical bulk and ferromagnetic effects of LC passive filters. Active filters exhibit high input impedance, low output impedance, and high gain over the useful bandwidth. The designer may elect to use active filters when space prohibits the use of bulky passive filters.

5.5.2 Isolators. Isolators differ from filters in that isolators appear as open circuits beyond the cutoff frequency. Isolators may he as simple as a relay or as complex as fiber optic systems.

5.5.2.1 Relay isolation. Low-speed signaling may use simple relays to provide isolation. The signal from the terminal device provides the voltage that alternately opens and closes the relay. The output contacts may alternate between open and ground, may provide a path for a voltage to ground, or may switch between two polarities. While high isolation can be achieved, the mechanical nature of relays limits speed. The possible arcing of contacts may produce undesired signals or may distort the intended signal. Relays may prove effective in he facility design for control signal lines originating in the RED areas that must be distributed to the BLACK areas. Specially constructed electronic relays are commercially available that operate at speeds compatible with 2400 bps transmission, and with 100 megohm isolation between input and output.

5.5.2.2 Optical isolation. Optical isolators use a light source and a light detector to transmit a signal across a space. The driver circuits typically are designed to ignore voltage levels above or below a voltage of interest. This ability to ignore unwanted voltages provides the blocking of signals coupled to the desired signal. Optical isolators may be constructed with the source and the detector aligned and separated by a fixed space, or may use an FOC to connect the two devices. The, FOC scheme is often found at the point of egress of the LEA. Isolators are commercially available to handle data rates to the megabit range. Isolators that use FOC are preferred for shielded facilities with the FOC passing through the shield through waveguides-beyond-cutoff. Where a shield does not exist, isolators using fixed space separation of the source and detector may be used.

5.6 Grounding, bonding, and shielding (GBS). It is essential that appropriate GBS practices be followed to provide adequate TEMPEST protection.

5.6.1 Grounding. Grounding is the measure taken to provide the electrical connection to earth through an EESS. The facility ground system consists of the EESS, the signal reference subsystem, the FPSS, and the lightning protection subsystem designed using MIL-STD-188-124 and MIL-HDBK-419. Figure 16 depicts a facility grounded for TEMPEST and EMP.

5.6.1.1 Earth electrode subsystem (EESS). The EESS consists of a bare No. 1/0 AWG 7-strand copper wire buried a minimum of 1.5 feet (0.45 m) below the earth surface and not less than 2 feet (0.6 m) nor more than 6 feet (1.8 m) from the building drip line. Copper-clad steel ground rods measuring 0.75 inch (19 mm) by 10 feet (3 m) are to be installed not more than 20 feet (6 m) apart. The rods are bonded to the copper wire by welding or brazing. The EESS is a closed loop which surrounds the facility. The design objective for the ground resistance of the EESS should not exceed 10 ohms. For additional design considerations, see MIL-STD-188-124 and MIL-HDBK-419. Local electrical codes in overseas areas should also be considered.

5.6.1.2 Signal reference subsystem. The principle function of the signal reference subsystem in a facility is to provide a common ground reference throughout the facility which is the same for all equipment. Secondary functions are to provide a path to earth for induced static and noise. and to serve as a ground plane for high-frequency signals between equipment. These functions are best provided by an equipotential ground plane which is installed under, over, or beside all of the equipment in the technical area. A horizontal plane is much more effective than a vertical plane in capacitively coupling high-frequency signals to earth. The plane should be bonded (welded or brazed) to the main steel structure of the building and to the EESS at multiple points.

5.6.1.2.1 Construction of the equipotential plane. Several methods are commonly used to construct an equipotential plane, including solid copper sheeting and grids of copper wire. A sheet of copper can be placed under floor tile or carpet. A grid of wire can be installed overhead in an existing installation, or embedded in floors, walls, or ceilings in new construction. Commercially available copper grids with silver-soldered, brazed, or welded joints may be used so long as the aperture is not more than 4 inches (100 mm) and the wire size is at least No. 6 AWG. An overhead grid may be fabricated on site using No. 1/0 AWG stranded copper wire for wall members and No. 2 AWG stranded wire for cross members. The cross members should be installed in a 4 by 4 inch (100 mm by 100 mm) aperture cross-hatch pattern. The cross members are bonded to each crossover point and at the ends to the wall members.

5.6.1.2.2 Connections to the equipotential plane. All equipment signal grounds are bonded to the plane using the shortest practicable runs of No. 6 AWG stranded wire. All connections to the plane should be welded or brazed; where this is not feasible, adequate cable clamps may be used. The plane is bonded to all adjacent structural steel and is connected to the EESS at multiple points around the perimeter of the facility using No. 1/0 AWG stranded wires. All equipment racks, cabinets, and cases will be grounded to the plane using short No. 6 AWG stranded copper wires bonded to the plane and bolted to grounding studs which are welded to each rack or cabinet. Equipment cases are grounded through the rack/cabinet ground, or are equipped with individual grounding conductors to the plane. If a case ground is not provided, a ground terminal should be installed as near the power entrance point as possible. Cable shields arc circumferentially bonded at both ends to case grounds or ground buses which are connected to the plane. Cable ladders and ducts are grounded at each junction. When cable ladders are installed, a No. 6 AWG copper wire is installed on the underside of the ladder, and all rack/cabinet grounds are bonded to the wire using pressure-type connectors. The ladder should be bonded to the equipotential ground plane at the point where the bonding conductor is the shortest. Cable ducts carrying de power or signal/control lines will be grounded by the same method. Cable ducts carrying ac power will be grounded to the ac protective ground bus in the power panel. Practical techniques for equipotential planes in new and existing facilities are available in FIPS PUB 94. Other grounding and bonding requirements are contained in Article 250, NEC.

5.6.1.3 Fault protection subsystem (FPSS). All equipment will be equipped with a conductor serving as the FPSS. (See NEC and MIL-STD-188-124.) The FPSS terminates on the power ground terminal of the equipment and the ground bus in the power panel. If the equipment does not have a ground terminal, one should be added to the equipment case ac, near the power entrance point of the equipment as possible. Extreme caution must be exercised to ensure the phase, neutral, and FPSS conductors are not reversed. The neutral and FPSS

conductors are bonded together at the first service disconnect or service transformer, and further bonded to the EESS. This is the only intentional grounding of the neutral conductor that is permitted by MIL-STDs or local codes. In shielded facilities, the FPSS conductor does not penetrate the shield. At the shield, the conductor will he bonded to the shield on the inside and outside. No aperture is made for the conductor.

NOTE: This handbook, in consonance with MIL-STD-188-124, emphasizes that the FPSS and power neutral conductors will be tied together only at the first service disconnect. Some equipment has been designed with the equipment chassis as a neutral return. Since the FPSS is also bonded to the chassis, currents in the FPSS are possible.

5.6.1.4 Lightning protection subsystem. Where lightning protection is required, it shall be designed using MIL-STD-188-124, MIL-HDBK-419, and the National Fire Protection Code No. 78.

5.6.1.5 Building structural members. All steel structural members of tile facility will be bonded together and grounded to the EESS.

5.6.2 Bonding. Bonding is the electrical connection between two metallic surfaces established to provide a low impedance path between those surfaces. This may be between two or more items of equipment, equipment and the equipotential plane, or the equipotential plane and the EESS. The preferred method of bonding is welding or brazing. This provides a strong bond which should not be affected by intense heat created by lightning or EMP/HEMP. Bonding may be accomplished through the use of pressure connectors (see figure 49). Pressure connectors should be inspected frequently to ensure adequacy of bonding. Ground conductors may be soldered if there is little risk from surges which may cause the solder to melt. Soldering should only be used if other methods are not feasible. Soldering is never used in the FPSS or lightning subsystem. Ail structural steel members of the building should be bonded together. This is done by welding all seams and joints. The members may be bonded by installing a jumper wire constructed of No. 1/0 AWG wire and crimp-type connectors. The connectors should be welded to the members. However, the connectors can be bolted or riveted if welding is not feasible. If pressure connectors or rivets are used, it is important that connections are tight, providing a strong mechanical bond. Further, such mechanical bonds should be accessible for periodic inspection. The steel members are connected to the EESS by using No. 1/0 AWG stranded copper wire. The cases of all power-line filters are bonded to the facility entrance plate. This is accomplished by circumferentially welding the case of all filters that penetrate the facility entrance plate, and connecting a No. 1/0 AWG stranded copper wire between the filter case and facility entrance plate if wall-mounted filters (generally power) are used. In addition to NEC bonding requirements for building metallic networks, where the equipotential plane is installed, all other metallic networks penetrating the plane (air-conditioning ducts, power conduits, structural beams, etc.) or adjacent to the plane should be bonded to the plane. Where dissimilar metals are to be bonded, consult MIL-HDBK-419 for additional protective measures.

5.6.3 Shielding. Shielding consists of those actions taken to reduce the coupling of electrical or magnetic fields into or out of circuits through the use of EM barriers. The methods of shielding may vary depending upon the type of equipment used, physical construction of the facility, and any requirement for HEMP hardening. Cable which has a nonferrous circumferential shield should be used for RED signal and control lines and is also recommended for BLACK lines. The shield of all cables used within an REA,

BEA, LEA, or CAA should be grounded at both ends. Cables for equipment or systems designed to operate in the high-level mode will be installed using ferrous-type conduit with compression or threaded fittings or ferrous-type cable duct. All RED signal and control lines, RED power, BLACK signal and control lines, BLACK power, arid all lines which are not a part of the communication system (door bells, administrative telephones, fire alarms, etc.) should be encased in separate conduits or ducts. Physical separation of all elements should be in accordance with table II. All conduits or ducts that are in close proximity should be parallel. When crossovers are necessary, all conduits or ducts should cross at right angles and with appropriate physical separation. All junction or terminal boxes which are part of a PDS used for TEMPEST control should be equipped with an RFI-gasketed cover and must have all apertures closed by conduit or ferrous-type aperture covers. All ducts should be grounded as indicated in paragraph 5.6.1.2. Conduits, if properly installed with appropriate coupling devices, will provide an adequate shield. All conduits and ducts should be marked every 3 to 5 feet (0.9 to 1.5 m) to distinguish between RED and BLACK runs. Normally, the less prevalent runs should be marked Wire lines that are not a physical element of the information mission system will be identified, BLACK. This includes utilities such as smoke detectors, thermostats, etc. TEMPEST approved equipment which uses low-level balanced voltage digital signaling, shielded cable, and has adequate built-in power and signal/control line filters, may not require use of conduit or duct. As a minimum, however, nonferrous shielded cable should be used. Use of conduit or duct is dependent upon TEMPEST tests and local environment.

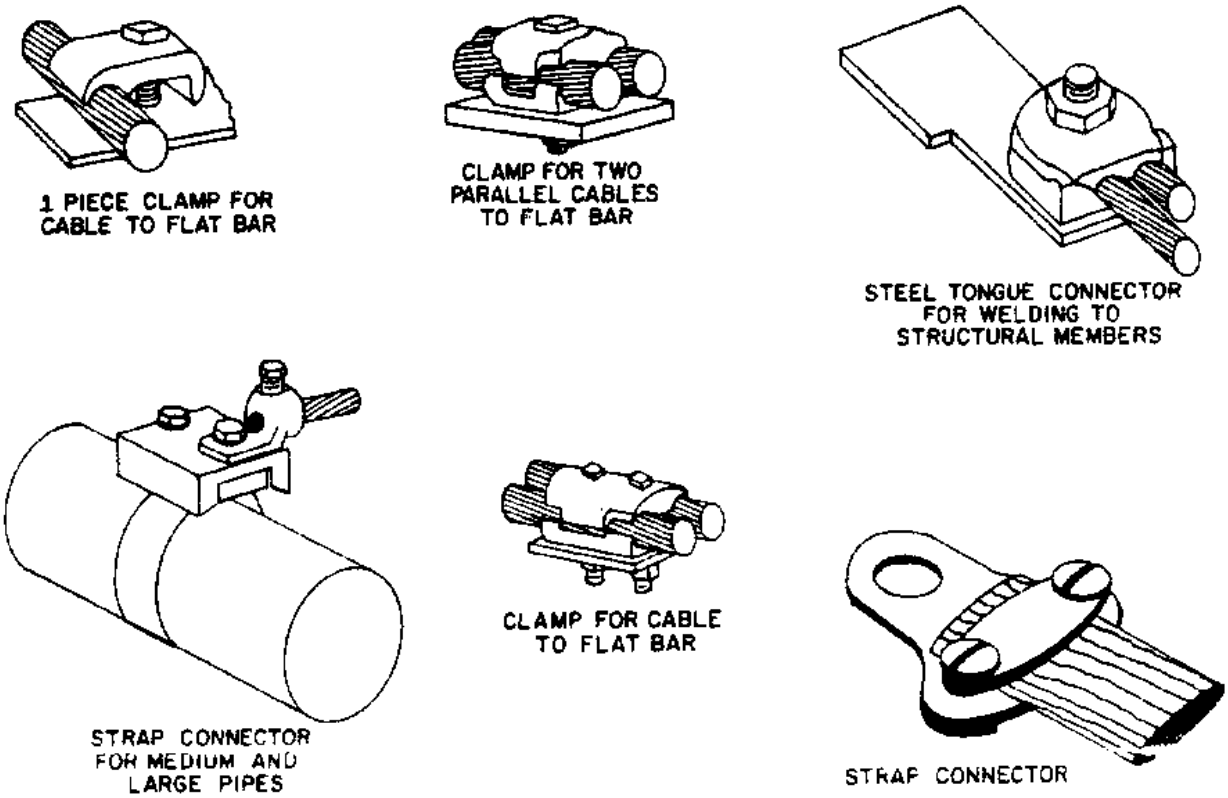


FIGURE 49. Pressure bonding techniques.

5.6.3.1 Facility shielding. Certain facilities, under certain conditions (see NACSI 5004), may require a global shield to contain free space radiation or suppress the EM environment at that location. To determine the amount of shielding, an EMC survey and analysis should be performed. This analysis should consider power density predictions or measurements, and equipment susceptibility/radiation evaluations. Once the need for shielding has been established, the shield should be constructed using guidance in MIL-HDBK-419 and specifications of NACSEM 5204. Most such shields will be six-sided.

5.6.3.2 Two-sided shields. In some facilities, a two-sided shielding concept may be used. This would occur when TEMPEST approved equipment is used exclusively. In reality, the shield is global, while the facility construction is only two-sided. The facility entrance plate and the equipotential ground plane comprise the two sides. Equipment cases, racks, cabinets, conduits, and ducts comprise the remainder of the shield. If such a configuration is used, the designer and installer must pay close attention to good engineering and installation practices. These include:

a. Positive electrical integrity of all cases, cabinets, racks, conduits, and wire ways through vigorous grounding and bonding.

b. Shield integrity and preservation by treatment or elimination of apertures.

c. Ensuring all panels, covers, and doors are properly installed and in place.

5.6.3.3 Utilities. All metal service pipes (e.g., water, steam, gas, sewer, fuel, air) (see figure 50) will be bonded to the EESS prior to entrance into the facility. This can be accomplished by attaching a No. 1/0 AWG stranded copper wire to the pipe with an adequate clamp (see 5.6.2), and then connecting the wire to the EESS. Where a facility entrance plate is used, these pipes should be routed through the plate and circumferentially bonded to it.

5.7 Security. Any facility which processes, transmits, stores, handles, or otherwise manipulates classified information must be afforded security commensurate with the level of classification of such material. The general principles of the security for areas containing classified material are contained in DoD, service, and agency directives and regulations. The guidance contained herein establishes a common facility baseline for facilities electronically processing information relative to the RED/BLACK concept to provide the security to protect against signals intelligence (SIGINT) and images intelligence (IMINT) exploitation. Some of this guidance further decreases exploitation by human intelligence (HUMINT).

5.7.1 Physical security. A facility is divided into spaces and areas where varying degrees of security are established and wherein specific operations are permitted to exist (see figures 14 and 15). The concept may be visualized as a pyramid, where each level of the pyramid takes classified information further away from access by uncleared or unauthorized agents. Each level then is a barrier to the next. These levels from bottom to top represent the uncontrolled access area (UAA), the controlled space (CS), the limited exclusion area (LEA), the BLACK equipment area (BEA), and the RED equipment area (REA).

5.7.1.1 Uncontrolled access area (UAA). The UAA is that area external or internal to a facility to which no controls for access are applied. Typically, it refers to the general area outside a facility perimeter to

which the local population has access, whether that be parking lots, wheat fields, or corridors. It is representative of the ground on which the pyramid sits.

5.7.1.2 Controlled space, (CS). The CS is the three-dimensional space surrounding facilities that process classified information within which unauthorized or uncleared personnel are (a) denied unrestricted access, (b) escorted by authorized personnel, or (c) under continual physical or electronic surveillance. (CS was previously known as the physical control zone.) Typically, it is established by a physical perimeter barrier, such as a fence or wall, around a facility. It should be established so that the entire space is under constant surveillance. For facilities occupying a small area within an existing building or a ship, the CS may end at the walls of the room or space, unless the local authority can establish control on the rooms and spaces surrounding tile area. It Is represented as the entire pyramid.

5.7.1.3 Limited exclusion area (LEA). The LEA is that room or area to which security controls have been applied to provide protection to RED information processing systems, equipment, and wire lines equivalent to that required for the information contained therein. In such areas, access by unauthorized or uncleared personnel is stringently denied. Within an LEA is a BEA and an REA. The LEA is represented by all the space within the pyramid.

5.7.1.4 BLACK equipment area (BEA). The BEA is that portion of a facility which contains equipment that interfaces the information mission equipment to an external transmission media after appropriate encryption safeguards have been applied. This area normally contains patch and test equipment and communications equipment. It is represented as the lower portion of the pyramid.

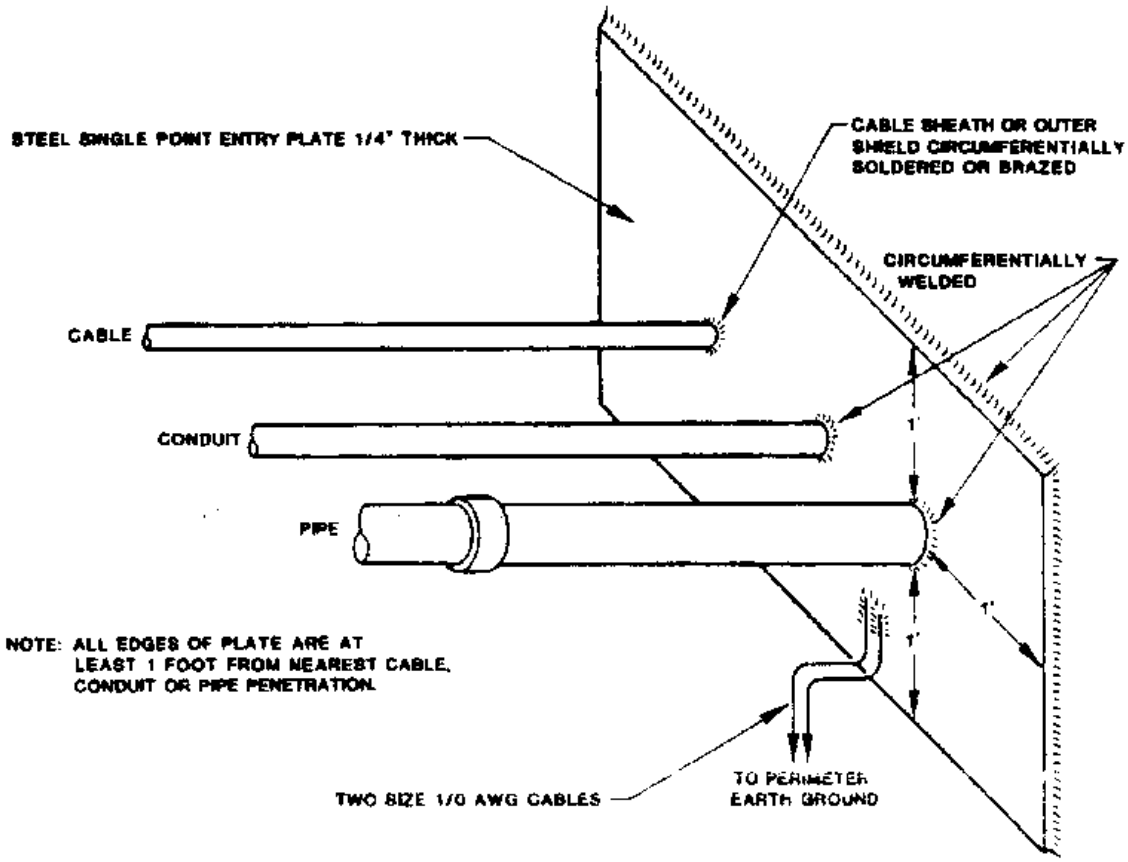


FIGURE 50. Facility entrance plate.

5.7.1.5 RED equipment area (REA). The REA is that space within the LEA designated for the installation of communications and information processing equipment that is intended to process plain text classified information. It is represented as the upper portion of the pyramid.

5.7.1.6 Other areas and considerations. In addition to the above spaces and areas, two subclasses exist which may dictate the size of a space, or may identify a need to apply protection to a space as a precaution. These are equipment radiation TEMPEST zones (ERTZs) and controlled BLACK equipment areas (CBEAs).

5.7.1.6.1 Equipment radiation TEMPEST zone (ERTZ). The ERTZ is that area or zone established as a result of determined or known equipment radiation TEMPEST characteristics. The zone includes all space within which a successful hostile intercept of compromising emanations is considered possible. An ERTZ normally would be associated with equipment in an REA.

5.7.1.6.2 Controlled BLACK equipment area (CBEA). A CBEA is a BEA, not within an LEA, which is afforded entry control at a security level commensurate with operational requirements. Examples of CBEAs are technical control facilities and radio relay sites supporting LEAS. Such facilities are typically afforded such protection to prevent HUMINT exploitation, equipment destruction, or network sabotage.

5.7.1.7 Design. When a new facility is designed, close coordination between the system engineer and physical plant engineer in conjunction with the operational planners, is needed to assure all required physical security measurers can be included in the design. An increase in real estate may negate the need and expense of shielding or encapsulation of equipment to contain emanations and prevent exploitation. Appendix B discusses the principles of physical security in facility design. It is intended to give the designer an overview of physical security and is not meant to override DoD, service, or agency directives, regulations, or policies.

5.7.2 Emissions security. Emissions security, as discussed here, are those measures taken in the design and installation of a facility. These measures:

a. Contain compromising emanations to the extent possible.

b. Reduce those emanations.

c. Prevent exploitation of those emanations.

d. Prevent the introduction of clandestine devices and fortuitous probes into a facility.

Emissions security also encompasses principles of EMC.

5.7.2.1 Emanations containment. Where indicated by NACSI 5004, the designer should utilize equipment which has been TEMPEST approved. Such equipment has been designed and certified as either totally containing its emanations, or having emanations of such low magnitudes as to be virtually nonexploitable. With proper attention to good engineering practices, RED/BLACK separation, and good installation practices, a high level of confidence and a very low level of risk can be achieved. Where nonTEMPEST equipment must be used, the engineer should research instrumentation sweeps of facilities using similar

equipment. Such sweeps should provide information to establish the ERTZ of that equipment. Where the ERTZ is unknown or of uncontrollable size, countermeasures to reduce or contain those emanations are indicated. Such methods may include encapsulation of the equipment, use of racks and cabinets, placing of equipment in screen rooms, or shielding of the facility. NACSI 5004 and NACSI 5005 should be consulted to determine the anticipated threat. That threat defines the level of required protection.

5.7.2.1.1 Encapsulation. Encapsulation of equipment to contain emanations involves surrounding the equipment with a stand alone RFI enclosure. Such encapsulation must include provision for the entrance of signal and power cables and provide adequate ventilation. Total encapsulation may not be practical if operators must have ready access to controls and indicators.

5.7.2.1.2 Cabinets. Equipment which is rack mountable should be mounted in cabinets. This method is effective if the front panels of equipment, when properly mounted, provide an adequate degree of RFI attenuation, Equipment should make bare-metal contact with the cabinet. All unused front rack space should be closed by blank panels. Closed-door operation of the cabinet provides further protection. Adequate warning is required that a TEMPEST hazard may exist when the door is open or panels are removed.

5.7.2.1.3 Screen rooms. Where a quantity of equipment requires ready operator access to controls and indicators, such equipment may be placed in a screen room within the REA. Screen rooms are commercially available to provide attenuation and containment of emanations and provide proper treatment of signal and power cables required to operate the equipment.

5.7.2.1.4 Shielded facilities. An entire facility may be shielded to contain emanations. While this method reduces or eliminates numerous problems in designing a facility, it may be quite expensive and may not be necessary. As pointed out in paragraph 5.7.1.7, the size of the CS may be such that by using other methods, shielding may not be required. The decision to shield must be made after careful study of the equipment being used, the adequacy of other methods, the physical plant, and the potential threat, coupled with cognizant agency regulations and policies. Shielding is easier to accomplish and has better protective capability when done concurrently with new construction. Shielding in new construction typically attains 100-dB or better attenuation, while retrofitting typically achieves about 60-dB attenuation. Additional measures may then be required. Facilities designed and hardened to HEMP threats are shielded to prevent damage to equipment. That shielding also provides TEMPEST protection to the facility.

5.7.2.2 Other exploitation prevention. The use of TEMPEST equipment and protective measures for nonTEMPEST equipment may be offset by emanations from interconnecting cables. Signals may be induced on cables passing through an ERTZ. These cables may egress the facility. To reduce this hazard, proper attention to cable protection is required. The use of shielded cables and metallic wire ways provides such protection by providing an EM barrier between the cable and the radiated signals.

5.7.2.2.1 Shielded cable. All signal cables in a facility should have at least one overall shield. The use of individually shielded pairs within a cable should be considered if signal characteristics of clock and data lines and supportive tests indicate a high likelihood of crosstalk. From a

protection viewpoint, individually shielded pairs may not offer sufficient increase of protection for the cost involved. As a matter of engineering practice, cables should be sized to accommodate a single channel or a single interface group between equipment.

5.7.2.2.2 Metallic wire ways. Metallic wire ways and conduits provide shielding for cables contained therein. Separate wire ways and conduits are used for RED and BLACK cables. Where such wire ways must run parallel, separation should be as indicated in table I. Where RED and BLACK wire ways must cross, crossings should be perpendicular. Wire ways should be unpainted to provide electrical continuity, and all sections and covers firmly bonded, grounded, and in place. In the REA, cables between equipment may be double shielded if the volume makes wire ways impractical.

5.7.2.3 Fortuitous probes and other exploitation. Where emanations have been reduced to acceptable levels, other exploitation schemes must be used by hostile elements, such as taps or probes. Since probes may take on any form through any conducting media ingressing or egressing a facility, controls must be placed on all pipes, wire ways, conduits, and conductors.

5.7.2.3.1 Conductors. All signal and power lines ingressing and egressing a facility should do so through a single cable and power entrance vault, with access restricted. Further, an accounting of all conductors is necessary. Most facilities are installed with extra conductors to accommodate upgrades. All such conductors should be grounded at every DF. In no case should unused conductors be crossconnected to conductors going to subsequent DFs. Spare pairs which are in place between BEA and a CBEA to reroute circuits should be grounded when not in use. This grounding provision can be provided in the patch panels.

5.7.2.3.2 Pipes, conduits, and wire ways. In unshielded facilities, all pipes, conduits, and wire ways should be equipped with a nonconductive section at the point of egress of the LEA. The section internal to the LEA should be bonded to the facility EESS. The section external to the LEA should also be bonded to the EESS. In shielded facilities, all pipes, conduits, and wire ways are circumferentially bonded to the facility entrance plate. (NOTE: Ducting and piping for heating, ventilating, and air-conditioning equipment receive the same treatment.)

5.7.2.3.3 Surveillance. All wire ways and conduits should be installed so as to be in constant view except as follows:

a. When passing through walls, floors, or ceilings in the CAA.

b. When permanently installed within the walls, under the floors, or above the ceiling provided that:

   (1) The condition of the installation is monitored. Accessibility is only from within the CAA or LEA.

   (2) Accessibility is only from within the CAA or LEA.

   (3) Requirements for a PDS are met.

   (4) Alarmed barriers to prevent undetected human penetrations are provided.

5.7.3 Protected distribution systems (PDS). Situations exist which require RED cable distribution to exit one LEA, traverse one or more lower levels of security, and ingress another LEA. In such cases, additional security measures are required to protect the information being distributed. Guidance is contained in NACSI 4009. Such protection must make penetration into the distribution media so difficult that it discourages the penetrator, or makes discovery and apprehension a certainty, The amount of protection depends upon the level of classification of the information, the level of security in the area(s) crossed, and the responsiveness of the security force. The PDS should be exposed to surveillance. All joints and covers should be welded, Pull boxes and accesses must be kept to a minimum. Where access to pull boxes must be retained, covers should be equipped with approved locks and intrusion detection devices. Cables contained within the PDS should have wire supervision which alerts security personnel should a successful penetration occur. Surveillance may also require lighting the entire run and monitoring it with closed circuit TV. To design a PDS, one must consider the geographic location, political environment, zone of control, size and complexity of the PDS, available surveillance, accessibility, and degree of vulnerability. The designer must work closely with the local security and intelligence agencies to define the threat to which the PDS must be designed. For instance, some locations may require less protection, while other locations may require stringent protection, or may not allow the use of a PDS due to a highly hostile local environment. Where intrusion detection systems (IDS) are used for the facility, such systems should be extended for additional monitoring of the PDS.

5.8 Telephone systems. Telephone systems are an integral part of the communications community. This type of service may range from a single telephone line to a fully expanded electronic private automatic branch exchange (EPABX). An EPABX may consist of secure or nonsecure voice, facsimile or data, with additional capability of voice conferencing, redline service, off-hook (hot line) service, dial intercom, or public address system access. Due to the probable extension of these systems beyond the CS, stringent TEMPEST control measures are mandated.

5.8.1 Administrative nonsecure telephone systems. Current technology and tariff/industry deregulation have produced a myriad of equipment and systems which may be interconnected by the public switched network. Service to a facility may be Government owned and operated, or may be provided by the common carrier or a third-party vendor. The variety and complexity of commercial telephone systems make the task of providing specific installation guidance difficult. Every installation must be examined in light of the particular environment involved. There are, however, basic steps which should be followed to provide security against a technical penetration of any telephone system. The more complex a system is, the more difficult it is to prevent a penetration. The best way of eliminating the problem would be to exclude telephones from areas in which classified information is discussed and/or processed. This approach is unrealistic in the majority of situations encountered. Although it is usually possible, and recommended, to exclude telephones from secure conference rooms, a working area is a different matter. Communications must be provided. Restricting the number of telephones to an absolute minimum is essential.

5.8.2 Risks. Telephones in areas where classified information is discussed or processed constitute exploitable vulnerability. Three distinct risks are involved: wiretapping, compromising emanations, and mircophonic coupling.

5.8.2.1 Wiretapping. All telephone conversations are potentially subject to interception. The path followed by telephone lines often presents several terminations where conventional wiretapping is possible. Also, the increased use of microwave links readily provides a means for hostile agents to intercept telephone conversations without detection. A conventional wiretap approach is virtually undetectable without physically examining the entire wire path, an impossibility in today's environment. Due to the high probability of intercept, classified discussions are prohibited over telephone systems which are not protected by authorized encryption techniques. This restriction applies also to the discussion of classified information over telecommunications systems where such systems are integrated into the facility's telephone equipment, even if all stations are within the secure perimeter.

5.8.2.2 Compromising emanations. Telephone lines may carry machine emanations from nearby equipment that processes classified information to uncontrolled areas. Appropriate countermeasures to address this threat fall within the purview of the TEMPEST program.

5.8.2.3 Microphonic coupling. Telephones may be used as part of a clandestine eavesdropping system even while on-hook (hung-up). Telephones in the on-book condition are found to frequently pass room conversations occurring in the vicinity of the instrument to unprotected areas. This may be the result of accidental or intended modification, or because of a design characteristic of the telephone instrument or its associated equipment.

5.8.3 Installation criteria. The installation of telephones within sensitive discussion areas should be in accordance with the following criteria (see figure 51) for cable/wire control, isolation, handsets, and signal.

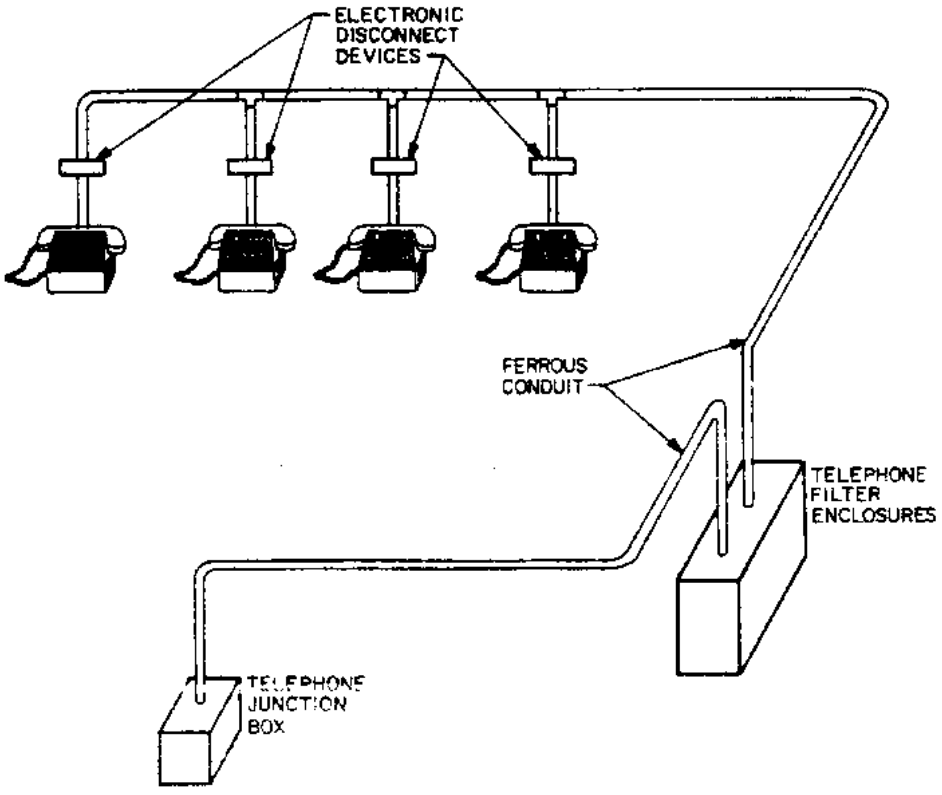


FIGURE 51. Administrative telephone installation.

5.8.3.1 Cable/wire control. Protection schemes for administrative telephone systems begin with control of all wire and cable.

5.8.3.1.1 Cable/wire entrance. All telephone wires should enter the facility at one point. Each conductor should be accounted for accurately at the point of entry. The accountability will identify, through labeling or log/journal entries, the existing use of every conductor. This accountability also applies to excess conductors that should be terminated at the point of entry and connected to appropriate connector blocks. In facilities that process classified information, lines may require filtering or optical isolation.

5.8.3.1.2 Multiline service. When multiline telephone service is used within sensitive, discussion areas, the associated key service unit (KSU) should he installed within the area or in an adjacent area that has equal security protection, This simple step will enhance security by reducing the number of conductors that enter a facility. For example, in a facility having four incoming lines, only the conductors connecting the KSU to the local telephone office will penetrate the controller area. If 6-button telephone sets are used, 12-pair cable is required from the KSU to the set. The reduction of penetration points is obvious.

5.8.3.1.3 Distribution. Within an LEA, telephone lines should be, routed from the entrance connector blocks in conduit and should be shielded cable. Telephone signal lines are not distributed in ducts with other signal cables. Where possible, telephone cable should be installed in conduit from the facility wire closet, or the KSU, to a point as close to the telephone set as is operationally

5.8.3.2 Isolation. Telephone instruments should be isolated from all incoming lines when not in use, i.e., in the on-hook condition. The recommended methods of achieving isolation are manual or automatic disconnect.

5.8.3.2.1 Manual disconnect The simplest and most economical means of isolating a telephone instrument from outside lines Is to fit each instrument with a plug and jack arrangement so the telephone can be disconnected manually at all times when not in use. This method is also the most effective one, but only if the user remembers to pull the plug. Such plug and jack installations should be arranged so they are convenient to use and incorporate an audible alarm to warn users to remove the plug upon completion of calls. The internal ringer of the telephone is permanently disconnected. An external buzzer or other audible device is used in place of the ringer. Figure 52 is a diagram of the recommended method. When multiline service is required. the plug and jack can be incorporated by using a single-line instrument and a separate key strip with a plug and jack installed between the instrument and key strip (see figure 53).

5.8.3.2.2 Automatic disconnect. The Western Electric Company model 270 automatic telephone disconnect device (ATDD) is designed to provide automatic disconnection of single- or two-line telephone instruments and is available only to Government agencies. Although it is more expense than a plug and jack arrangement, the model 270 is user transparent. It requires no action by the user to initiate or terminate a telephone call. The model 270 disconnect switch is also compatible with key telephone systems when installed between a key strip and a single-line instrument in the same manner described for the manual plug and jack arrangement in paragraph 5.8.3.2.1. This will require the installation of a model 270 switch for each telephone instrument.

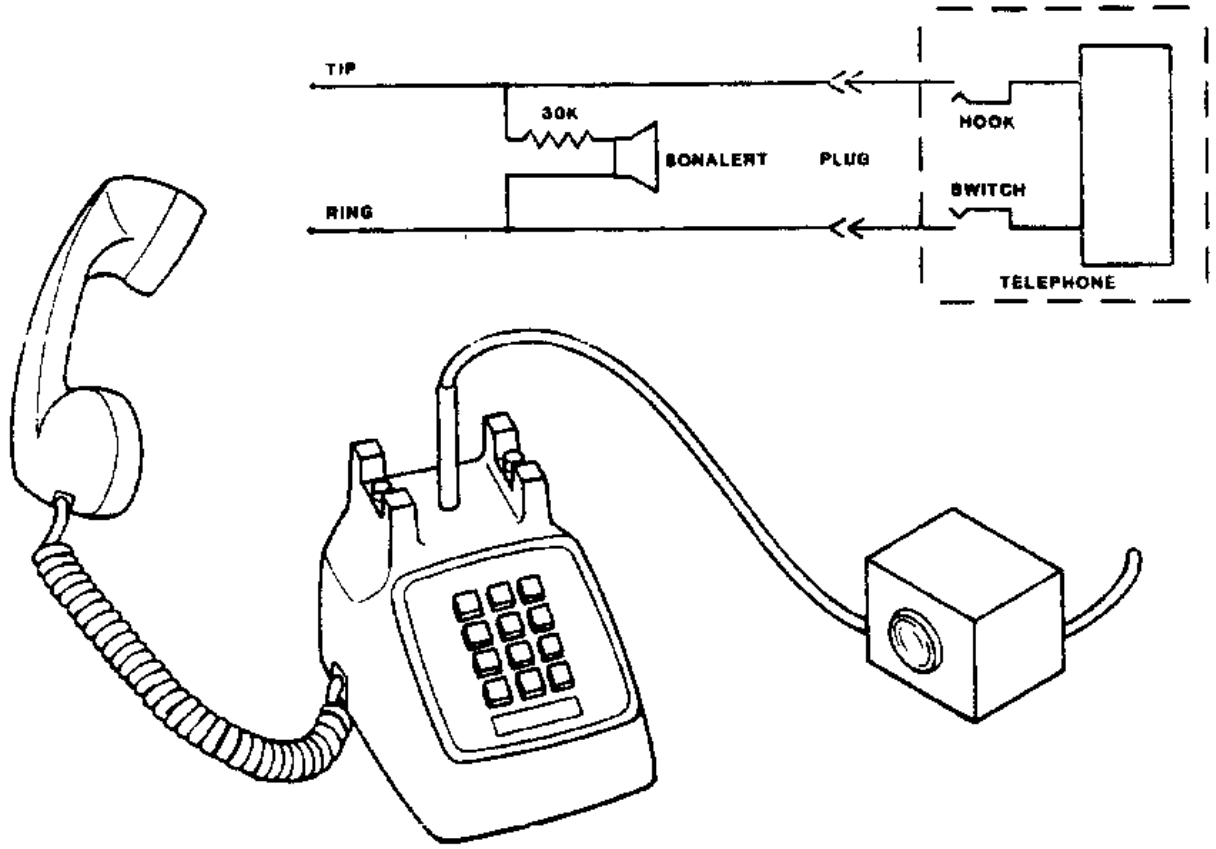


FIGURE 52. Manual disconnect method.

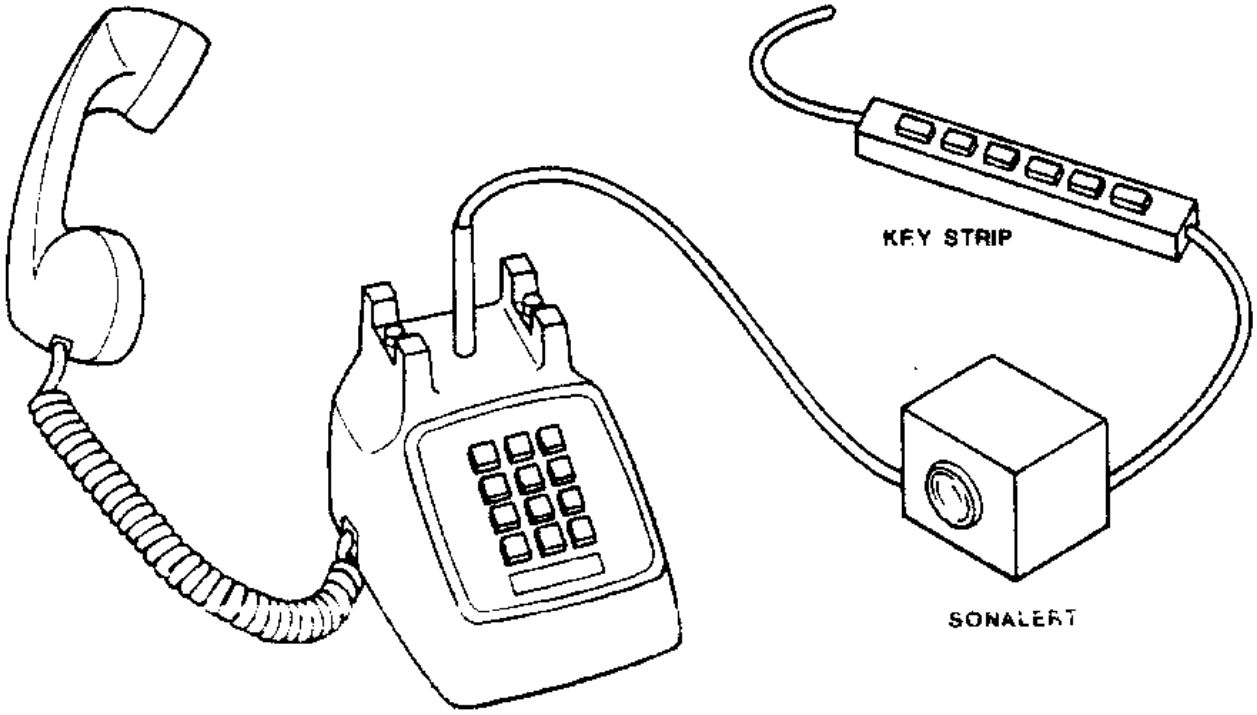


FIGURE 53. Key system manual disconnect.

5.8.3.3 Handsets. In cases where a hold feature is provided, either through the use of a multiline telephone set or a separate line selector key strip, no special handset is necessary. When a hold feature is not available, a security handset such as the WECO G-10A, G-10B, G-10F, or equivalent, is essential for audio protection in those situations where the instrument is left off-hook and unattended for short periods of time while the user obtains information, files, etc.

5.8.3.4 Signal. Since most standard telephone ringers have microphonic characteristics, the signaling of incoming calls within sensitive discussion areas should be accomplished in accordance with one of the following options:

a. In facilities where the KSU is installed within the secure perimeter, no special signaling apparatus is required if the KSU includes a local ring generator and is wired for common audible signaling. Any ringer or buzzer may be used. This type of installation requires a backup power source if telephone service is required during commercial power outages.

b. In facilities where KSUs are not used or are not installed in the secure area, the ringer or buzzer should be modified with an approved isolator kit.

5.8.4 Single-line service. The trend within DoD is to provide single-line service. With this type of service, each user or subscriber is provided a dedicated line and instrument. Service may include special functions such as call forwarding, call transfer, and conferencing. When such systems are utilized within a CAA, it is recommended that any special function capability be limited to that area, since extension of service may be detrimental to the TEMPEST integrity of the facility. All considerations are to be made in light of operational impact.

5.8.5 Electronic private automatic branch exchange (EPABX). The EPABX is emerging as the telephone system of the future. An EPABX may be designed to serve as few as 50 subscribers or may function as a dial central office serving a specific community of interest with trunking capability to other exchanges or local offices. The Telephone Security Panel, in a report to the community, "Computerized Telephone Systems", 30 June 1983 (see appendix D), issued instructions and standards for implementing computerized branch exchanges in areas where classified discussions take place. Those standards, coupled with good RED/BLACK engineering practices, assure a low-risk installation. It is imperative that systems/devices used in an area requiring RED/BLACK consideration are provided adequate filtering and isolation from other equipment or systems.

5.8.6 Key distribution systems. A key distribution system permits a greater number of users to share limited line capacity. An example of this is an office with 20 employees and 4 telephone lines. Each employee may have access to all lines, plus intercom capability. It is recommended that all instruments coupled to a key distribution system be limited to areas within the CAA. Installation criteria are as follows:

a. The KSU must be of U.S. manufacture and installed in accordance with paragraph 5.7.3.

b. The KSU should use high-security key telephone unit (KTU) line cards.
c. All instruments served by the KSU must be within the LEA.

d. The equipment must be installed and maintained by cleared U.S.

5.8.7 Intercommunication systems. Intercommunication systems installed within LEAs present audio security hazards similar to those related to telephone systems. Unless necessary for efficient operation, intercommunication systems should not be installed in LEAS. The design of many intercommunication systems allows audio in the vicinity of any station to be intercepted at any point along the connecting cable run. The speakers in public address systems may also function as microphonic transmitters. If determined to be essential, all components of the system, including connection cables, should remain within the established secure perimeter. Under no circumstances should intercommunication systems that use ac power lines or rf energy as the transmission medium be used. Intercommunication systems must be tested to ensure the components do not generate rf emissions which may be intercepted and exploited.

5.8.8 Specialized telephone equipment. The installation of specialized telephone equipment, such as telephone answering devices and speaker phones, is discouraged within LEAS. Such systems add to system complexity and increase the potential for undetected exploitation. In cases where operational need overrides the security ramifications, specialized telephone equipment should be installed using the provisions of paragraph 5.8.3.

5.8.9 Approved equipment. With the rapidly changing technology in the telephone industry, the designer should consult DIAM 50-3, the local cognizant TEMPEST authority, or the cognizant security authority for current approved telephone equipment and procedures.

6. NOTES

6.1 Intended use. The purpose of this handbook is to provide basic guidance to engineers and installers of military departments and agencies in the design and installation of systems and facilities which accept, store, retrieve, manipulate, graph, archives integrate, and communicate classified information. When selectively applied, its principles support RED/BLACK and TEMPEST programs of the military departments to reduce the risk of clandestine exploitation of classified defense information. Its principles may also be applied to lesser degrees to systems processing unclassified information which may be sensitive due to provisions of public law.

6.2 Subject term (key word listing).

Electronic security

Grounding, bonding, and shielding

Physical security

Power

RED/BLACK concept

TEMPEST

6.3 Changes from previous issue. This revision correlates to the previous issue in concept only. The content has been subjected to extensive change and reorganization to reflect emerging technology. Of particular note, however, is the change in philosophy for grounding systems. The previous issue used a single-point grounding scheme that was adequate for the technology that existed. That scheme is no longer appropriate. For those situations where the user must interface to an existing single-point ground system, consult the guidance in MIL-HDBK-419, Grounding, Bonding, and Shielding for Electronic Equipments and Facilities.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. TRANSPORTABLE FACILITIES

10. General. This appendix provides minimum guidance on the installation of transportable information processing facilities. Although many concepts are similar to those of fixed installations, there are some unique requirements for transportable systems. The guidance provided will apply to all transportable systems requiring RED/BLACK consideration and protection, and should be complied with except when additional treatment is recommended as a result of TEMPEST testing. Such additional treatment will be determined by the cognizant TEMPEST authority on a case-by-case basis. See figure A-1 for a typical transportable information processing system.

20. Power sources. Power for transportable systems may be provided by generators, base power, or commercial sources. Unlike base or commercial power, generators dedicated to one operational system provide adequate isolation from other systems. However, generators may be used to provide power for more than one shelter and for various types of equipment and systems. In this case, the use of isolation devices may be needed. The recommended method of accomplishing this is to use appropriate filters.

20.1 Three-phase generators. These commonly used generators supply 120/208 Vac 3-phase 4-wire power. A ground terminal is provided on the chassis or frame of the generator. To ground the neutral conductor and provide the fault protection subsystem (FPSS), this terminal should be connected to the earth electrode subsystem (EESS) and the ground terminal of the shelter using a No. 2 AWG stranded copper wire. The conductor connected to the shelter should be spirally wrapped around the power cable in the same direction and with the same spiral spacing as the phase and neutral conductors. When polyphase equipment is used, it is important to ensure that each phase conductor is properly terminated at the generator and power panel (see figure A-2).

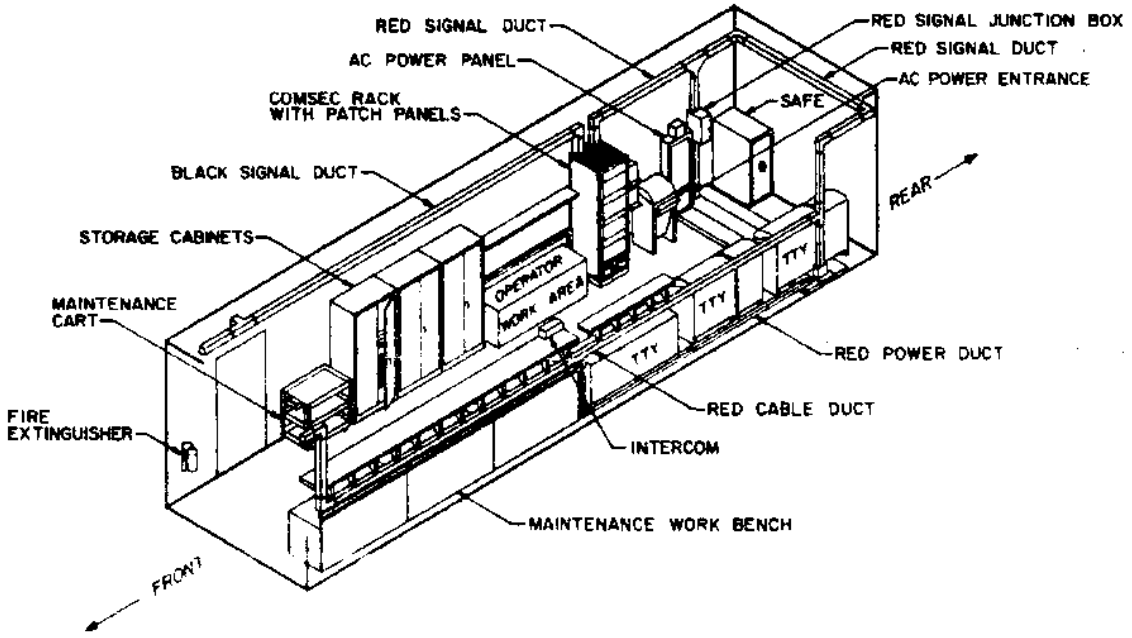
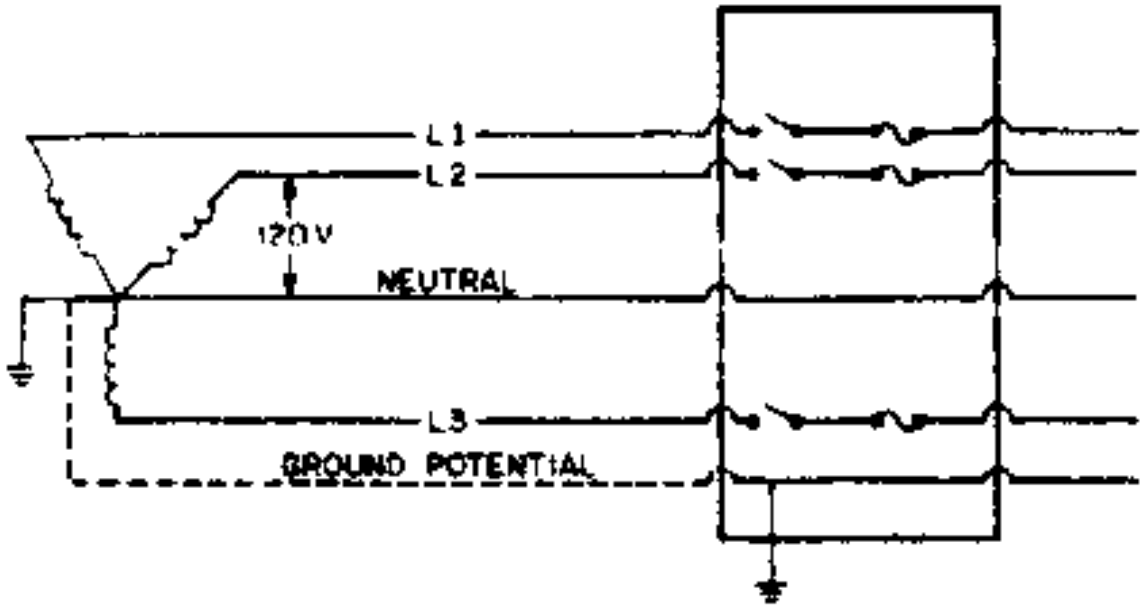
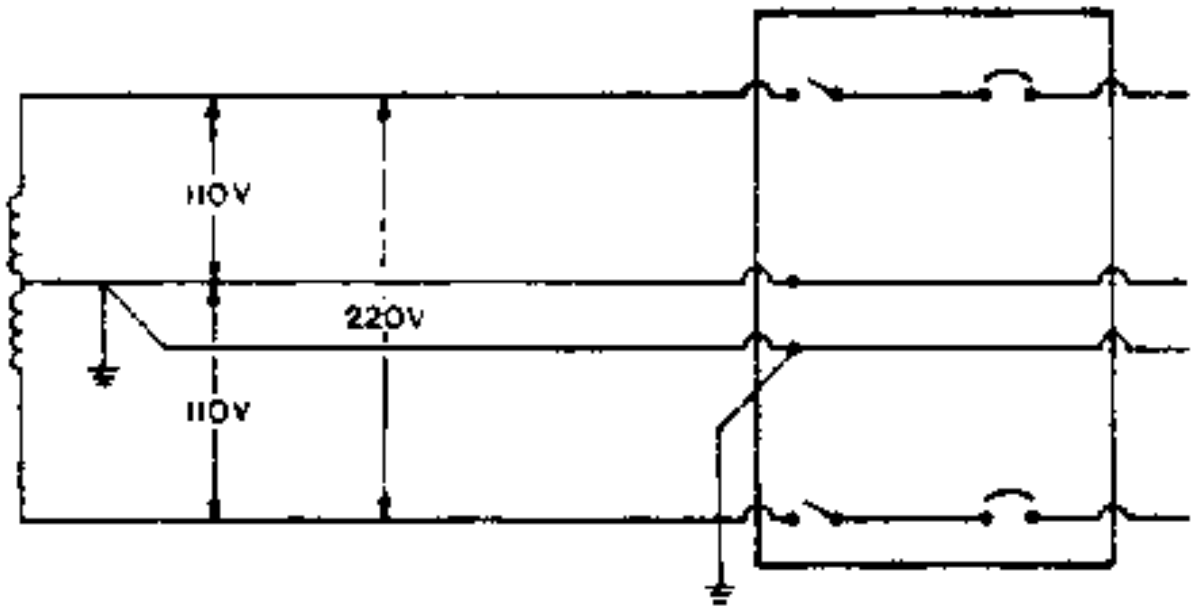


FIGURE A-1. Typical transportable communications system.



THREE PHASE



SINGLE PHASE

FIGURE A-2. Power source configurations.

20.2 Single-phase generators. This type of generator provides 115/230 Vac single-phase power and will normally provide the FPSS conductor in the cable. In addition, the ground terminals of the shelter and the generator should be connected to the shelter's EESS.

20.3 Base or commercial power. When base or commercial power is used, additional treatment of the subsystem becomes necessary, such as installation of power-line isolation devices. (See 50.1 for filtering and isolation.) The FPSS conductor might be provided by the power source, but it may not be below 25 ohms resistance. The ground terminal of the shelter should be connected to the shelter EESS to provide an earth resistance of 10 ohms or less. This ensures that a difference in potential does not exist between the FPSS and the equipment rack, cabinet, and case ground. Power lines should be kept as short as possible to reduce vulnerability to lightning or electromagnetic pulse (EMP)/high-altitude electromagnetic pulse (HEMP).

30. RED equipment installation. TEMPEST approved RED equipment for transportable communications systems provides the lowest level of risk. However, TEMPEST approved equipment may not be available or may not meet the operational needs. When nonTEMPEST approved equipment is used, special treatment, such as installation of power- and signal-line filters or isolators, is required. The need for additional protective measures should be determined by the cognizant TEMPEST authority.

30.1 Equipment separation. When a shelter includes RED and BLACK equipment, physical separation must be provided, but placement of equipment depends on the design of the shelter. Ideally RED equipment should be separated from BLACK equipment and other electronic devices by at least 3 feet (0.9-m). If situations exist which will not permit a 3-foot (0-9-m) separation, then maximum possible separation should be provided. When installed in tents or buildings, RED equipment should be a minimum of 3 feet (0.9 m) from outer walls and windows or doors. Personal electronic devices (radios, tape players, computers, etc.) should not be permitted in areas where RED equipment is installed and operated.

30.2 Terminal devices. Terminal devices may be installed in various design configurations and may be operated in shelters, vehicles, buildings, or tents. Since it is not practical to install conduit in the field, or in temporary locations, other protective measures should be taken. Terminal devices should be installed so that access is controlled. It may become necessary to screen equipment in order to prevent it from being viewed by personnel who are not properly cleared. Encryption devices should be installed at the terminal location to provide secure communication. Cable with an overall nonferrous shield should be used for signal and control lines. The shield should be grounded at both ends. Cables should be kept within the controlled space (CS) and should be checked frequently for tampering. Encrypted signal lines may extend beyond the boundaries of the CS. These cables should be clearly visible while traversing tile uncontrolled space.

30.3 Voice terminals. Ideally, only secure voice terminals would be used for classified telephone traffic. However, nonsecure voice terminals may be installed as a local network for discussion of classified information if the network is approved by the cognizant security manager. When nonsecure voice terminals are used in the configuration, all wire lines must be kept within the CS. Network design should prevent direct off-net calling from nonsecure terminals. Calling outside the network should be possible only through manual intervention on the switch. User education about the capabilities and limitations of nonsecure terminals is critical when using this type of network.

40. Signal distribution. Cables with an overall nonferrous shield should be used for all signal and control lines for transportable systems. The shields should be grounded at both ends to provide adequate shielding inside and outside the shelter. When unshielded cable must be used outside the shelter, it should be used for BLACK signal lines only and should be separated from RED lines by a minimum of 6 feet (1.8-m) if operating conditions permit. If a 6-foot (1.8-m) separation is not possible, maximum possible distance should be provided.

40.1 RED and BLACK patch panel isolation. Although space may be limited, RED and BLACK patch panels should be installed with adequate isolation between them. TheN, should be installed with enough separation so that it is not possible to patch from one to the other with a standard length patch cord. RED and BLACK panels should be installed in separate equipment cabinets and separated by at least 3 feet (0.9 m).

40.2 Isolation of RED/BLACK signal and control lines. RED and BLACK signal and control lines should be separated by at least 3 feet (0.9 m). If this is not feasible, separate them as far as possible. RED and BLACK signal and control lines should be contained in separate cables which have an overall nonferrous shield and should be installed overhead when conditions permit. This can be done by installing them on poles, in trees, or by constructing

"A" frames for support. Some systems have been designed to use multipair

overall shielded cable containing both RED and BLACK lines. Avoid this practice whenever possible. If RED and BLACK lines are contained in the same cable inside the shelter, filters or isolators should be installed at the point of egress from the shelter.

40.3 Digital and analog cables connected to patch panels. Digital and analog cables should enter the patch panel cabinet by using methods that would prevent the cables from running adjacent to or crossing each other. This is effective in reducing the possibility of crosstalk.

40.4 Sensitive Compartmented Information (SCI) and non-Sensitive Compartmented Information (non-SCI). Shelters which are certified for SCI and non-SCI traffic should have patch panels which are isolated by communities. Panels should be clearly identified to indicate the community. Panels that employ a different wiring configuration and have unique patch cords should be used in order to eliminate inadvertent patching from one to the other.

40.5 Filters and isolators. External filters or isolators may be required on RED and BLACK signal lines which are contained in the same multipair cable. All signal and control lines should terminate inside the shelter. Signal lines which penetrate the shelter skin should do so through filters or isolators installed at the point of penetration. Filters installed in series with built-in filters ma,v result in changing the operating characteristics of the filler and could modify the bandpass frequency, reducing the desired signal rejection. If equipment contains filters, optic isolators are recommended at the point of egress.

40.6 External RED and BLACK signal and control lines. Some transportable systems are designed to have RED signal and control lines which are external to the shelter. Separate RED and BLACK cables with an overall nonferrous shield should be used for signal and control lines with separate connectors at the facility entrance plate. RED signal lines external to the shelter should be kept at least 6 feet (1.8 m) from BLACK signal lines and all power cables.

50. Power- and signal-line isolation. Power- and signal-line isolation for transportable systems is dependent on the type of equipment used and the shelter design.

50.1 Power-line, isolation. Most transportable shelters are not equipped with separate power distribution panels for RED and BLACK equipment. Devices that use the high-level mode of operation without adequate filter devices should have power-line filters installed as near to the power distribution panel as possible. Equipment that is TEMPEST approved, uses low-level signaling, and has adequate power-line filters should not have external filters installed. When external filters are used, RED and BLACK power lines should be separated by at least 3 feet (0.9 m). Conduits, cable ducts, or cable race ways should be used when possible to provide further isolation.

50.2 Signal-line isolation. RED and BLACK signal lines should not be included in the same multipair cable. RED and BLACK lines should be separated by at least 3 feet (0.9 m) throughout the shelter. Equipment that operates in the high-level mode, and does not have adequate signal-line filters should have external filters installed. Equipment that is TEMPEST approved, operates in the low-level mode, and has adequate filters installed should not require external filters or isolation devices.

60. Grounding, bonding, and shielding (GBS). Grounding of transportable facilities is dependent on the type of operation and the terrain. Short-term operation and rapid deployment or frequent relocations may require the use of a single earth electrode. Operation in one area for more than 1 or 2 hours, however, would permit the use of a more extensive and effective ground system. All transportable shelters should have at least two ground terminals at diagonal corners of the shelter. Systems operated in the same geographic area should have an EESS and should be connected to the EESS of other shelters so long as the length of the interconnecting ground conductor is 12 feet (3.6 m) or less. Longer conductors should not be used as this would increase the vulnerability to lightning or EMP/HEMP. Various ground systems may be used for transportable systems.

60.1 Metal shelters. Shelters constructed of metal material should use the inner and outer skin as an equipotential ground plane. This requires all seams to be continuously welded so that the resistance of the seam is not more than the resistance of the conductive panel. This will create a circumferential, low impedance, conductive path to ground. Multiple ground terminals should be welded to the outer skin so that multiple ground conductors may be connected between the shelter and the EESS. When installing the ground terminals, all paint or other protective substances should be removed prior to installation to provide a good mechanical and electrical bond. Welds should be circumferential to assure proper and effective bonding. Internal grounds should consist of threaded terminals of 1 inch (25 mm) by 0.25 inch (6 mm) copper ground bus, welded or brazed to the skin. Prior to installation, the skin should be free of any insulating materials that may increase resistance in the ground network. Then, the ground terminal should be circumferentially welded. The inner and outer skins should be bonded to the shelter frame at multiple points to provide electrical continuity. All welds should he treated with a conductive, protective coating to prevent corrosion and deterioration. The skin of the shelter should be bonded to the transporting frame (if the shelter is permanently affixed to the frame) by welding ground conductors (solid strap with a stress bend) to the skin and frame at multiple points to assure that a difference in potential does not exist.

60.2 Nonconductive shelters. Shelters constructed of nonconductive material should have a copper mesh screen installed between the inner and outer skin to form an equipotential ground plane. The screen should be installed in the floor, ceiling, and all walls of the shelter and should cover all surfaces except apertures for air-conditioners and cable entrance plates. Air-conditioner mounts and cases should be bonded to the screen. Cable entrance plates should be circumferentially welded to the screen and connected to the EESS using a No. 2 AWG stranded copper wire. Since the -screen in the door must be detached from the rest of the screen to permit the door to open and close, multiple flexible conductors should be bonded to-the door and main screens.

60.3 Earth electrode subsystem (EESS). An effective method of providing the earth ground is to use a circumferential EESS that consists of multiple copper-clad steel rods installed around the shelter. The rods should be 5 feet (1.5 m) long and 0.75 inch (19 mm) in diameter. At least two ground rods should be installed at diagonal corners of the shelter. Additional rods may be installed if the shelter size permits. It is important, however, that a minimum distance of one rod length and a maximum distance of two rod lengths is maintained between rods (see figure A-3). For shelters which are too small to permit proper spacing when using rods at each corner, one rod will be installed at the front corner and another rod at the diagonal rear corner. The purpose of using multiple rods is to provide more than one

AWG stranded copper wire must be installed between the outer skin or frame of the shelter and each ground rod. All rods should be bonded together using No. 2 AWG stranded copper wire and appropriate pressure connectors. The EESS resistance should be 10 ohms or less.

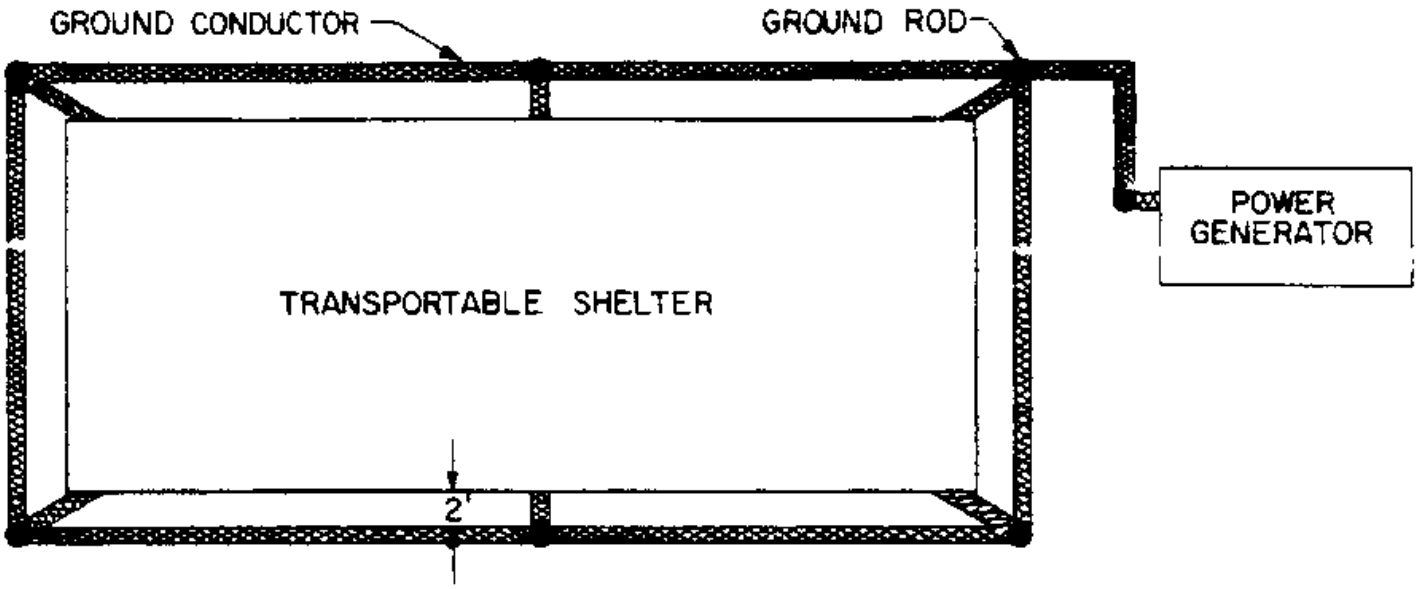


FIGURE A-3. Preferred transportable grounding method.

60.4 Alterative grounding. Another way to provide ground is to use a star ground which consists of seven ground rods. One rod should be installed as the center with the remaining six rods installed around it at 1.5 times the rod length from the center and from each adjacent rod in the star. All rods should be interconnected using No. 2 AWG stranded copper wire and pressure connectors. The shelter should be connected to the EESS by connecting multiple ground conductors between the shelter and the outer rods. If only one ground terminal is provided of) the shelter, the ground conductor should be connected to the center ground rod. When more than-one shelter is used in the same area, all shelters may be connected to the star ground. If the distance makes this impractical, each shelter should have its own EESS (see figures A-4 and A-5).

60.5 Grounding under adverse conditions. Adverse conditions may exist which would prevent use of conventional grounding methods for transportable systems on granite, coral, rocky areas, desert areas, or coastal regions. To compensate for this, a copper mesh screen, not less than 10 feet square (3 meters square), is laid on the earth surface (see figure A-6). The screen should be constructed of No. 12 AWG stranded copper wire with apertures of not more than 4 inches square (100 millimeters square). All crossover points should be brazed to provide effective low-resistance bonds over the surface of the screen. Installation in granite, coral, rock, or hard-packed desert

areas is accomplished by drilling holes 10 to 12 inches (250 to 300 mm) deep using a 0.675 inch (17 mm) star drill. The holes should be spaced 2.5 feet (0.75 m) apart around the perimeter of the screen. Fluted drive pins that are 12 to 14 inches (300 to 350 mm) long and 0.688 inch (17.5 mm) in diameter should be driven into the holes and bonded to the screen with pressure connectors (see figure A-7). After installing the screen, the ground should be covered with at least 1 inch (25 mm) of sand and should be treated with a thin layer of magnesium sulphate (epsom salts) and water. It may not be possible to remove the drive pins once they have been installed. When installing the screen in sandy soil or in coastal regions, drive pins should not be used. The screen should be buried approximately 6 inches (150 mm) below the earth's surface and covered with sand. It should be periodically treated with magnesium sulphate to ensure an effective ground. All ground conductors should be bonded to the screen using appropriate pressure connectors. When drive pins are used and the operation is completed, the pins should be driven into the ground after the screen is removed.

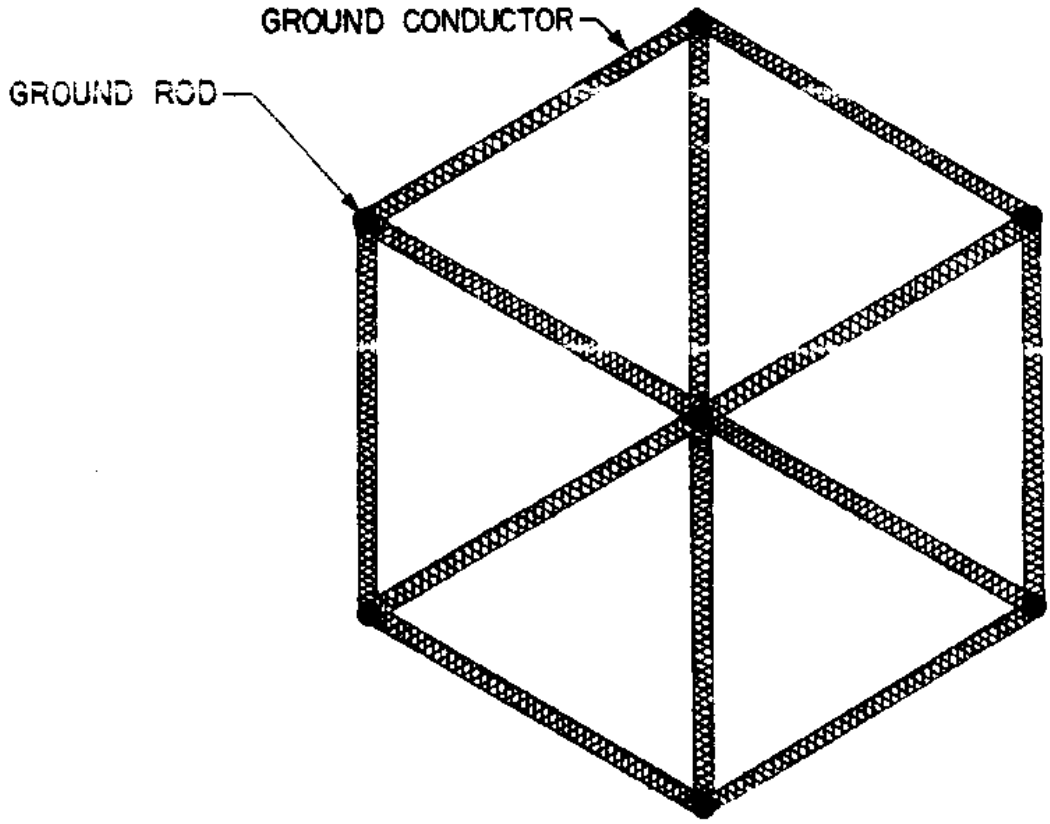


FIGURE A-4. Typical star ground.

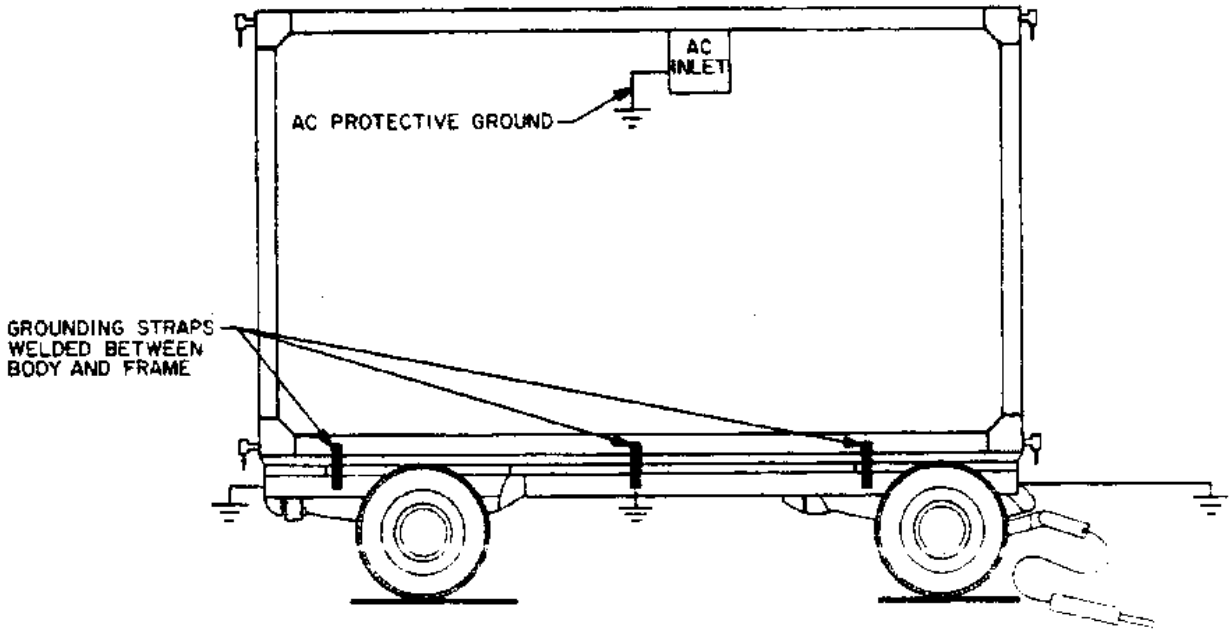


FIGURE A-5. Preferred method of grounding shelters to transporting frames.

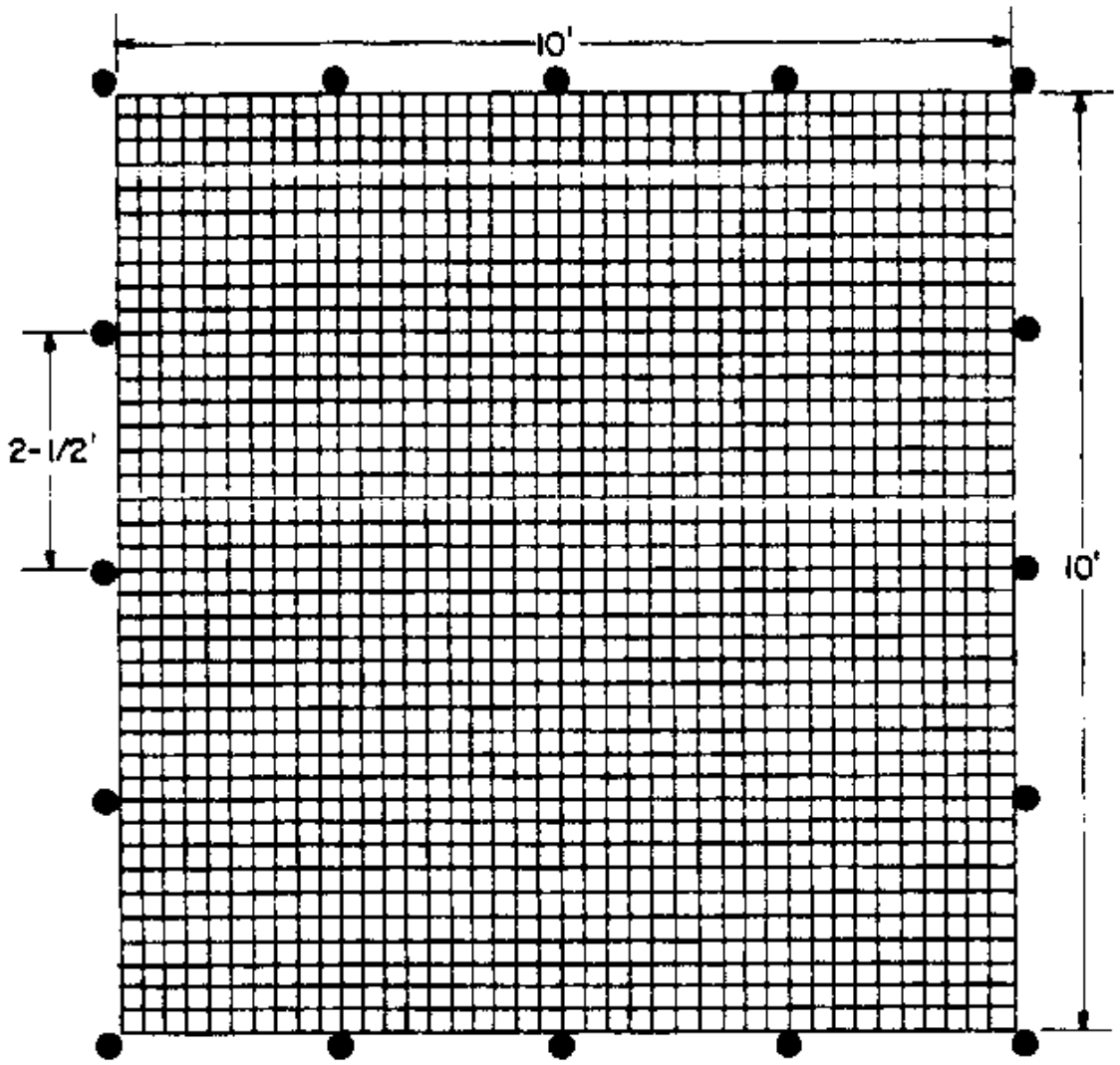


FIGURE A-6. Mesh screen and drive-pin positioning for grounding under adverse conditions.

60.6 Treatment of apertures for EMP/HEMP. All apertures must be treated to ensure a complete shield. All doors should be coupled to the skin by installing jumpers. At least three jumpers should be used. They should be welded to the door and wall skin. Air-conditioners should have metal mesh screens installed inside all panels which have filter apertures in them and in the duct into the shelter. Screens should be cut, installed, and circumferentially welded as depicted in figures A-8 and A-9. Only metal mesh filters should be used and should not be removed except for cleaning. The facility entrance plate should be metal and should be circumferentially welded to the skin of the shelter. All connectors which penetrate the entrance plate should be metal and should be circumferentially welded to the plate. All connectors should be equipped with metal-threaded caps screwed onto the connectors when not in use.

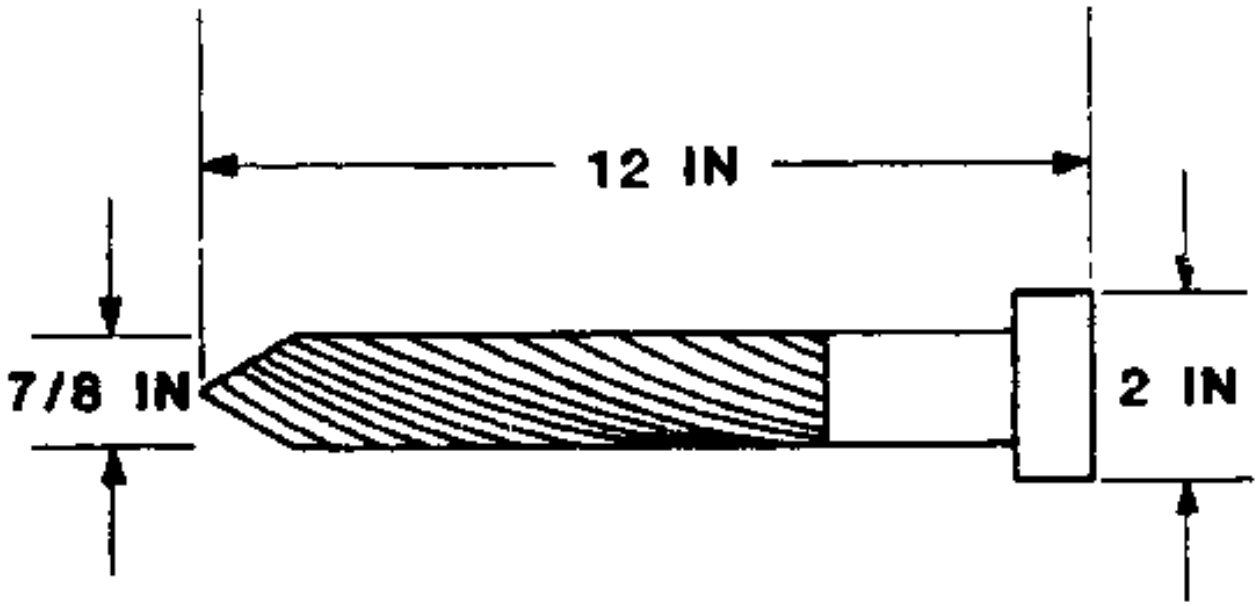


FIGURE A-7. Fluted drive pin for anchoring mesh screen.

60.7 Grounding for EMP/HEMP. Power fault grounding is critical for lightning and EMP/HEMP protection. Only the circumferential EESS described in paragraph 60.3 should be used. Multiple ground conductors should be installed between the shelter and the EESS to provide more than one path for ground currents.

60.8 Use of air terminals. In areas that have many electrical storms, it may be necessary to install air terminals (lightning rods). Air terminals should be constructed of solid copper, bronze, or aluminum rods to prevent them from exploding, igniting, or otherwise being destroyed. Solid copper or bronze rods should be at least 0.5 inch (12.5 mm) in diameter and solid aluminum rods 0.675 inch (17 mm) in diameter. Air terminals should be installed by welding threaded mounting plates at each corner of the roof of the shelter. The rods should be threaded to make the installation and removal easier. Air terminals should extend at least 10 inches (250 mm) above the highest point of the shelter. They should be interconnected by installing a No. 2 AWG stranded copper wire around the perimeter of the roof of the shelter and connecting it to each terminal with a pressure connector. A No. 2 AWG stranded copper wire should be connected between each air terminal and the EESS (see figures A-10 and A-11). When antennas are used, or when shelters are not equipped with air terminals, one can he provided by installing an air terminal on a pole which is higher than all conductive metals and connected to the EESS using a No. 2 AWG stranded copper wire.

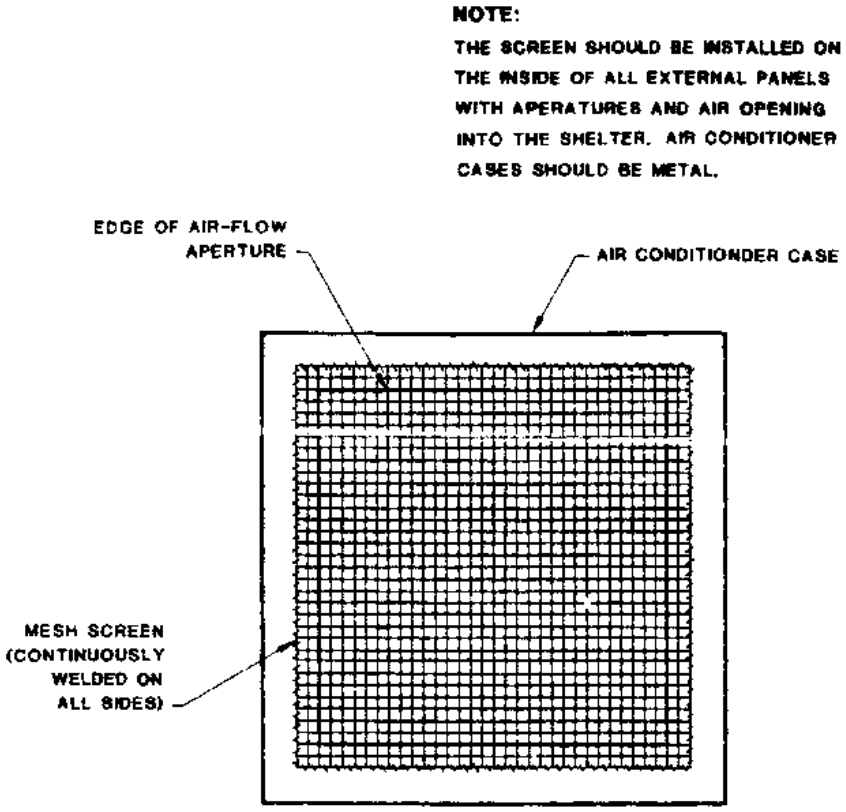
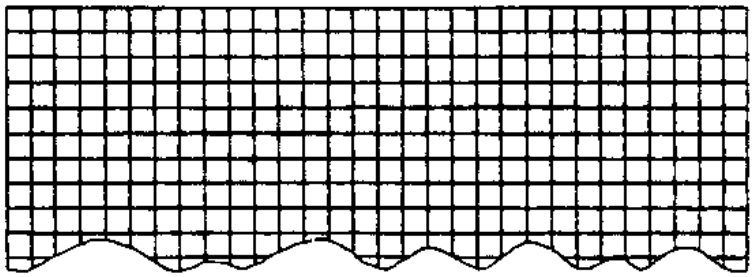
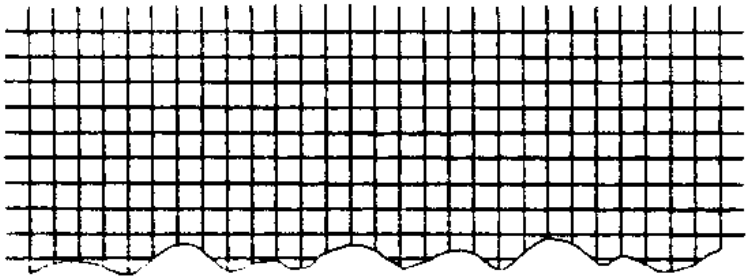


FIGURE A-8. EMP/HEMP protection screen for air-conditioner apertures.



PROPER METHOD OF CUTTING SCREEN



IMPROPER METHOD OF CUTTING SCREEN

FIGURE A-9. Method of cutting mesh screen.

60.9 Surge protectors. Surge protectors are needed to protect internal wiring and equipment from power surges created by lightning, EMP/HEMP, or power-line transients. They should be installed on all power, signal, and control lines that penetrate the shelter skin. There are various types of surge protectors available, such as metal oxide varistors (MOVs), gas filled spark gaps (gas tubes), zinc oxide nonlinear resistors (ZNRs), and unipolar and bipolar silicon-avalanche diode suppressors (SAS). Due to their rapid response time and durability, MOVs, ZNRs, or SAS should be used at the shelter entrance plate to shunt the initial surge to ground. Due to the current-carrying limitations of this type of device, gas tubes should also be installed near the shelter entrance plate. Although the response time for gas tubes is much slower than for other devices, the current-carrying capability is high and should effectively shunt peak surge currents to ground.

70. Physical security. Maximum physical protection should be provided for transportable systems whether they are operated in a field or garrison environment. This Is the responsibility of the cognizant security manager and the local command. As a minimum, CS should be established that provides adequate access control and effective radiation protection. The perimeter of the CS should be protected in such a way that access is limited to those who have an operational interest in the transportable system. Access to the shelter should be controlled by use of doors that are locked from the inside and equipped with one-way viewers.

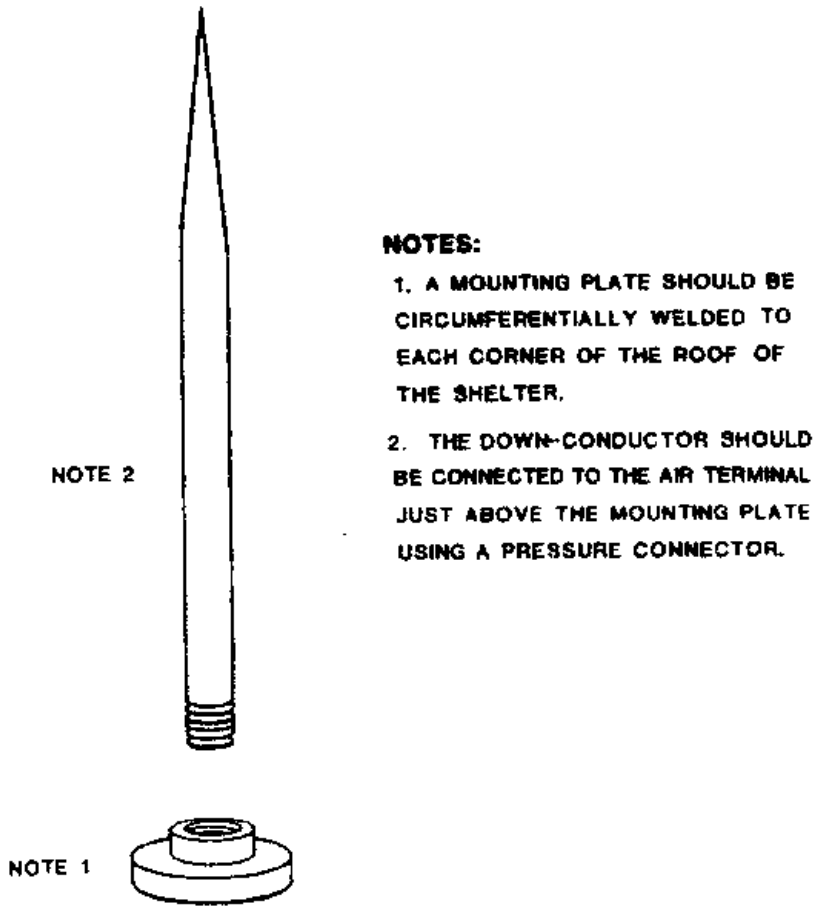


FIGURE A-10. Air terminal and mounting plate for transportable shelters.

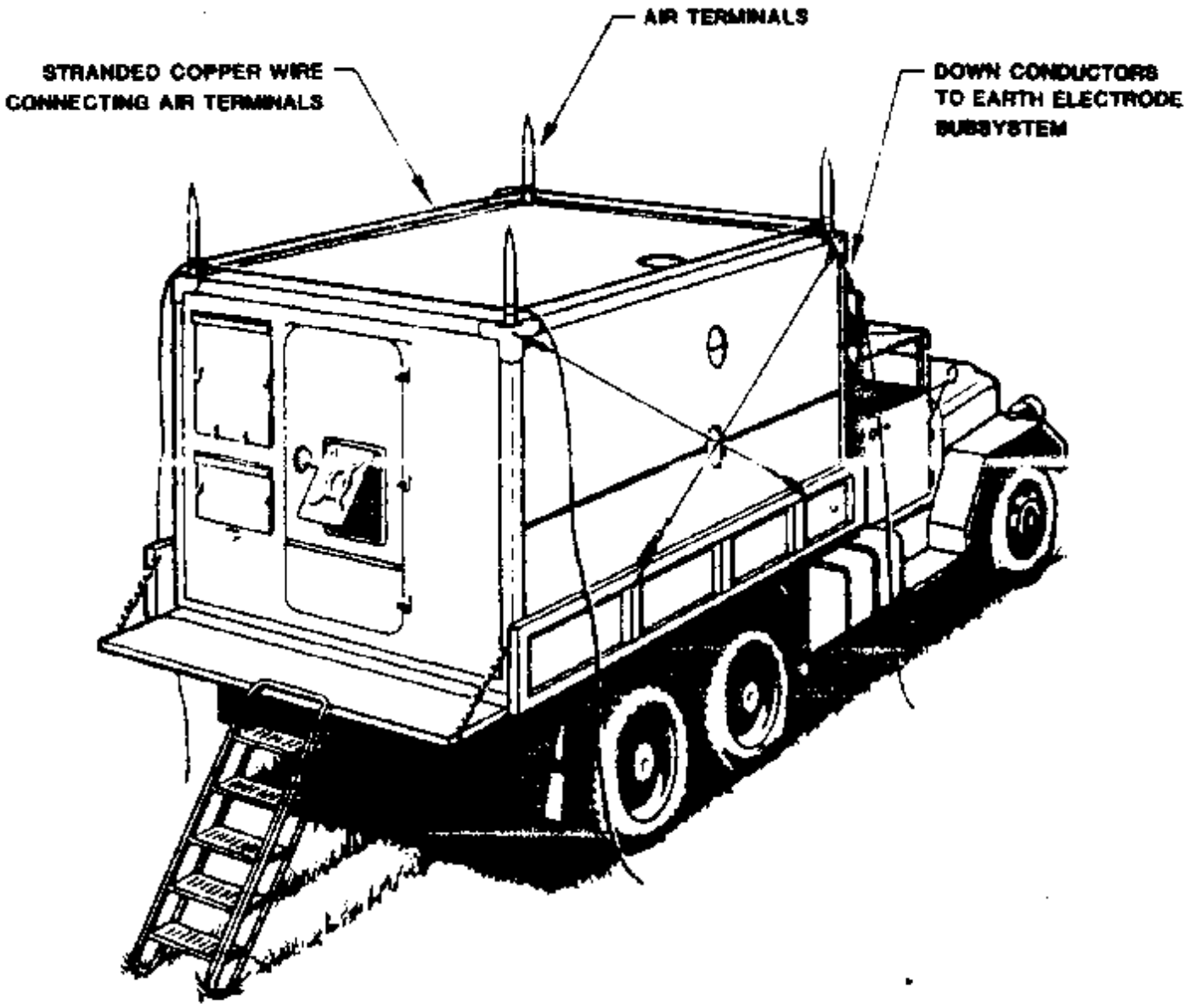


FIGURE A-11. Installation of transportable shelters.

80. Administrative telephones and intercom systems. Administrative telephones and intercom systems should be installed a minimum of 3 feet (0.9 m) from RED equipment. These systems should be tested to determine emanation characteristics and should be equipped with isolation devices that prevent electromagnetic (EM) coupling of RED signals to the administrative lines. Nonsecure telephones should be equipped with electronic disconnect devices or optic isolators and nonradiating ringers. Extreme caution must be exercised to ensure that acoustic coupling of classified information does not occur. Intercoms which operate between RED shelters should be interconnected with fiber optic cables (FOCS) when possible. If FOCs are not available, shielded cable should he used. The shields should be grounded at both ends. Filters should be installed in the line to prevent EM coupling of RED signals to the line.

90. Design and verification. Transportable shelters should be constructed in accordance with specifications provided by the design activity. The following procedures should be compiled with when designing a system.

90.1 Construction material. Shelters should he constructed of metal material with continuously welded scams to provide adequate bonding and shielding. If the shelter is permanently affixed to the transporting frame, the skin should be bonded to the frame at multiple points to provide effective ground continuity. This is accomplished by installing solid steel straps equipped with stress bends between the skin and the frame. These straps should be welded to ensure a strong bond. All apertures should be treated by installation of screens (see 60.6).

90.2 Cable race ways. Shelters should be equipped with separate ferrous-type closed cable race ways for RED signal and control, BLACK signal and control, RED power, and BLACK power cables. Race ways should be separated by at least 3 feet (0-9 m).

90.3 Doors. Doors should be made of metal material. They should be bonded to the skin of the shelter with flexible conductive straps and should incorporate RFI gasketing. Doors should be constructed so they can be locked from the inside. One-way, wide-angle, through-the-door viewers should be installed to provide a means of positive visual identification prior to opening the door.

90.4 Shelter grounding points. Multiple grounding points should be provided on external surfaces of the shelter to provide multiple ground current paths to earth. At least two ground terminals should be installed at diagonal corners of the shelter. All cable entrance plates should be equipped with ground terminals. The inner and outer skins of the shelter should be bonded together with multiple terminals provided on the inner skin.

90.5 Entrance panels. Power and signal entrance panels should be separated by the maximum allowable distance. When a shelter is designed to have RED and BLACK lines penetrating the shelter skin, separate RED and BLACK panels should be provided with at least 3 feet (0.9 m) of separation. The ideal configuration would be to have RED and BLACK panels on opposite sides of the shelter.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. PHYSICAL SECURITY

10. Physical security requirements and installation guidelines. A balanced security program must have a firm physical security foundation that is coupled with adequate electronic security measures to protect and secure classified information, processors, and facilities. It makes no sense to expend resources on electronic security if hostile intelligence service elements have physical access to the classified information/documents.

20. Physical security program design. A physical security program should be formulated and implemented using a total organization/facility approach. This approach is organized in-depth and contains mutually supporting elements of a physical and electronic nature. Coordination between physical security specialists, security managers, and facility engineers is necessary because it prevents security gaps or duplication of responsibilities and performance.

20.1 Total facility approach. A total organization/facility approach to physical security is based on:

a. Thoughtful and continuing analysis of existing protective measures.

b. Careful evaluation of the necessary and practical measures to maintain security at a viable level.

c. The security needs and local conditions of each facility.

d. The understanding that as physical security measures become more stringent, the operational capability may decrease.

20.2 Mutually supporting elements of physical security. Mutually supporting elements of physical security are those elements which augment the effectiveness of physical security measures. Mutually supporting elements of physical security include:

a. Perimeter physical barrier(s).

b. Clear zones.

c. Protective fighting.

d. Access control facilities.

e. Intrusion detection systems.

f. Perimeter defensive positions, if appropriate.

g. Armed guard forces.

h. Communications.

Selective integration of any or all of these elements can provide satisfactory facility security.

30. Facility design considerations. Available resources must he used in the most efficient manner possible to achieve adequate protection and security of a classified information processing facility and its contents. All security measures should be used to complement and supplement each other. A lack of integration of security measurers may result in a waste of money, equipment, and manpower. More importantly. the security of a facility may be jeopardized. Emphasis should be placed on the operational requirements of the facility to determine the type and extent of physical security measures needed. The following pertinent factors should be considered, in sequence, by the facility designer/planner:

a. The importance of the mission or assignment of the facility to the operating agency.

b. The area to be protected, including: the nature and arrangement of the activity; classification level of information, data, or activities within the facility; the number of personnel involved; monetary or strategic value of material and equipment located therein; and existing threats.

c. Integration of operating and maintenance requirements.

d. The political, legal, and economic environment.

e. Feasibility, effectiveness, and desirability of the various methods of providing adequate physical protection.

f. Costs of material and equipment to be installed, as well as the availability of funds to ensure adequate protection for all critical areas and activities.

40. Security threats. Security threats are acts or conditions that may result in the loss or compromise of classified information, loss or destruction of equipment or property, or disruption of the facility's mission/activities. Before an effective physical security program can be developed, the threat of interference with facility operations and the potential for compromise must be determined and evaluated. The recognition of all risks is essential if adequate security measures are to be designed to abate or eliminate the facility's vulnerability. The severity of security threats depends on such variables as the type of facility (SCIF, ADP, communications center, cryptofacility, etc.), physical layout of the facility, mission, and construction. In addition, the geographical location, the capability and possibility of hostile intelligence service exploitation, and the stability of law and order are also important factors to consider. Security threats can be categorized into two types - natural and human.

40.1 Natural security threats. Natural security threats are those threats that are:

a. Normally not perpetratable by human means.

b. Normally not preventable by physical security means.

c. Capable of affecting physical security operations adversely by negating existing physical security practices (i.e., collapsed perimeter fences/ walls, inoperable protective lighting, poor visibility, power outages, etc.).

Natural threats require unique interim protective measures like additional guard forces. Examples of natural threats are floods, storms, fog, high winds, earthquakes, snow and ice, rock or mud slides, and forest fires. Any facility prone to these natural threats requires preplanned measurers that will counteract the adverse impact of various natural threats.

40.2 Human security threats. Human threats to physical security are the result of a state of mind, attitude, weakness, or character inconsistency on the part of one person or a group of persons. Human threats include covert or overt acts of commission or omission. These threats are intended to disrupt, destroy, or compromise the mission or activities of a facility. Physical security measures are primarily designed to deter these threats. Examples of human threats are sabotage, espionage, terrorism, human intelligence (HUMINT), disaffection, disloyalty, and apathy of personnel.

50. Planning. Planning for the physical security of a facility must be constant, practical, flexible to the, mission, and responsive to the needs of the facility commander/director.

50.1 Objectives. Effective physical security planning must be concerned with, and be designed to, the probability that the most serious incident that could be perpetrated against the facility will be perpetrated given the critical nature of the information processed and stored there and the local threat. Planning must also take into account the personnel, material, and equipment available. Physical security measures should be implemented for the continuity of all security operations.

60. Controlling personnel movement. Perimeter barriers, intrusion detection devices, and protective lighting provide physical safeguards; however, these alone are not enough. A positive personnel movement control mechanism must be designed and established to facilitate and expedite authorized entry. It must preclude unauthorized entry by those who may try to circumvent the control mechanism. Planning and designing personnel access control points for controlling personnel movement through the various restricted areas is a concern of the facility engineer and physical security specialist during the facility design. Personnel security clearances and identification procedures are a concern once the facility is operational.

60.1 Restricted areas. In restricted areas, entry is subject to special control for security reasons. Restricted areas improve security by providing in-depth security measures. These special controls increase efficiency by providing degrees of security compatible with operational requirements. The use of restricted areas makes it possible to have security commensurate with operational requirements. Instead of establishing control measures for the facility as a whole, varying degrees of increasing security provisions can be provided by designating CONTROLLED, LIMITED, and EXCLUSION areas. As a result, interference with overall operations is reduced and operational efficiency can be maintained in a less-encumbered manner.

NOTE: The term RESTRICTED AREA is, in effect, a legal designation (Internal Security Act of 1950), whereas the terms CONTROLLED, LIMITED, and EXCLUSION are administrative subdivisions of the term that differentiate the degree of restriction or control required to prevent a compromise of classified information.

60.1.1 Types of restricted areas. The degree of security and control required for a facility depends on the nature, sensitivity, and importance of the security interest. Restricted areas are established to provide:

a. An effective application of necessary security measures, such as exclusion of unauthorized personnel.

b. Increased access controls over those areas requiring special protection.

c. Conditions for compartmentalizing classified information, critical material, or equipment with minimum impact on operations.

Restricted areas or portions of restricted areas, may be further administratively designated as controlled, limited, or exclusion areas, These designations allow varying degrees of access restriction, movement control, and protection to be applied, as needed.

60.1.2 Exclusion area. An exclusion area is defined as a restricted area that stores or processes classified information and material. Access or proximity to the area constitutes, for all practical purposes, access to the classified information and material. Access to exclusion areas should be restricted to personnel cleared to the level of the information being stored or processed and whose duties require access and a need-to-know.

60.1.3 Limited area. A limited area is defined as a restricted area that stores or processes classified information and material. it is an area to which only authorized (cleared) personnel should be permitted free access. Uncleared personnel may enter a limited area only if escorted by authorized personnel at all times.

60.1.4 Controlled area. A controlled area is one that usually surrounds an exclusion or limited area. It is normally established for administrative control, safety, or as a buffer zone to increase the security of exclusion or limited areas. The requirements for access to a controlled area are less restrictive than those of the limited and exclusion areas. Authorization for access to and movement within a controlled area may include personnel with official business or quasi-official business, such as concessionaires or building and grounds maintenance personnel.

60.1.5 Controlled space (CS). CS, for TEMPEST purposes, is defined as the three-dimensional space surrounding classified information processors that is intended to contain any compromising emanations radiated by the equipment. CS may be the physical confines of operational facilities, or if emanations exist beyond the, facility’s walls, floors, or ceilings, may include large areas of the building that houses the facility, or the installation on which the building is located. CS may be designated as an exclusion, limited, or controlled area. Personnel need not be cleared to the level of compromising emanations present to access a CS. For example, a sensitive compartmented information facility (SCIF) is designated as an exclusion area. The equipment contained in the SCIF may radiate outside the exclusion area into an area designated as a controlled area (i.e., a parking lot within a fenced area). It is not necessary to redesignate this CS as an exclusion area, because personnel cannot detect the presence of compromising emanations. The effectiveness of a CS is dependent upon the distance compromising emanations will travel in an exploitable form, and the distance from that point that a hostile agent would be forced to attempt an intercept operation. CS eliminates or reduces accessibility, which is one of the essential elements of TEMPEST vulnerability.

60.2 Physical safeguards for restricted areas. The physical safeguards applied to a facility are dictated by the sensitivity of the information processed. Safeguards may include: a range of guards, perimeter security fencing, gates, clear zones, window bars, secure doors, intrusion detection alarms, electronic surveillance devices, and other similar measures. Certain types of facilities (SCIFS, ADP, communications centers, cryptofacilities, etc.) have more restrictive requirements prescribed for physical security safeguards as an element of facility accreditation or approval.

70. Protective barriers. Protective barriers are normally used to define the practical physical limits of a restricted area and effectively control access to the area. Protective barriers are divided into two major categories - natural and structural. Natural protective barriers are mountains, deserts, rivers, gorges. or other similar terrain that is difficult to traverse. Structural protective barriers are man-made devices such as fences, walls, floors, roofs, grills, bars. roadblocks, or other types of construction that inhibit access to the restricted area. The use of barriers offers two important benefits to a physical security program. First, barriers create a psychological deterrent to those individuals who may contemplate unauthorized entry into restricted areas. Second, barriers have a direct impact on the number of security posts needed to secure a restricted area. The facility designer has little control over natural barriers. The guidance that follows concentrates on structural barriers.

70.1 Structural barriers. Structural barriers (such as fences or walls) are required for the entire perimeter of limited or exclusion areas and should be considered for all controlled areas. Specific types of facility barriers cannot be designated for all situations, but should incorporate structural perimeter barriers and provisions for access authorization verification at points of entry.

70.1.1 Fence design criteria. Four types of fencing are authorized for use in protecting restricted areas: chain link, barbed wire, concertina, and barbed tape. Choice of fence type depends primarily upon the degree of permanence of the facility, availability of materials, time available for construction, and requirements/specifications of the responsible department or agency. Generally, chain link fencing will be used to protect permanent limited and exclusion areas. All four fencing types may be used to augment or to increase the security of existing restricted area protective barriers.

70.1.2 Barrier wall design criteria. Barrier walls are those free standing walls that are not an integral structural component of a facility. Walls are seldom used as a perimeter barrier due to the cost of installation. When a masonry wall is deemed necessary as a positive barrier, tile minimum height must be 7 feet (2.1 m) and must have barbed wire top guard that is sloped outward at a 45-degree angle and carries at least 3 strands of barbed wire. The top guard should increase the vertical height of the total barrier by at least 1 foot (0.3 m).

70.1.3 Utility openings. Sewers, air and water intake and exhausts, and other utility openings of 10 inches (250 mm) or more in diameter that pass through perimeter barriers must have security equivalent to that of the barrier(s) penetrated. Interior manhole covers 10 inches (250 mm) or more in

diameter must be secured to prevent unauthorized opening. Unavoidable drainage ditches, culverts, vents, ducts, and other openings that have a cross-sectional area greater than 96 square inches (619 square centimeters) and with any cross-sectional dimension greater than 10 inches (250 mm) will be protected by securely fastened welded bar grills. As an alternative, drainage structures may be constructed of multiple pipes, each pipe having a diameter less than 10 inches (250 mm). Multiple pipes of this diameter may also be placed and secured in the inflow end of a drainage culvert to prevent access to the restricted area via the culvert.

40.1.4 Other positive barriers. Building walls and roofs, when serving as perimeter barriers, must be constructed and arranged to provide uniform protection equivalent to that provided by chain link fencing. If a building has less than two stories, a top guard must be used along the outside coping to deny access to the roof. Windows, inactive doors, and other openings must be protected by securely fastened bars, grills, or chain link screens.

70.1.5 Facility entrances. The number of active entrances to the facility and perimeter entrances should be limited to the minimum number required for safe and efficient operation of the facility. Active perimeter entrances should be designed so security forces can maintain full control without impeding vehicular or personnel movement. This involves having sufficient entrances to accommodate the peak flow of pedestrian and vehicular traffic, and adequate lighting for efficient inspection of access credentials. When exterior entrances are not manned during nonduty hours, a sturdy locking mechanism should be installed. These entrances should be illuminated during periods of darkness and should be monitored by closed-circuit TV cameras or be randomly inspected by roving patrols. This procedure also applies to doors and windows that form a part of the protective perimeter.

70.2 Perimeter roads and clear zones. When a facility’s positive perimeter barrier encloses a large area, an interior, all-weather, perimeter road should be provided for security patrol vehicles if these areas are not to be monitored by closed-circuit TV cameras. Clear zones should be maintained on both sides of the perimeter barrier to provide an unobstructed view of the barrier and the ground adjacent to it. Roads should be within the clear zone and as close to the perimeter barrier as practical without causing soil erosion, and should allow passage of a patrol vehicle.

70.2.1 Clear zones. A clear zone of 20 feet (6 m) or more should exist between the perimeter barrier and exterior structures, parking areas, and natural or man-made features. When possible, a clear zone of 50 feet (15 m) or more should exist between the perimeter barrier and the structures within the restricted area, unless greater distances are dictated by the presence of compromising emanations. These clear zone distances are obviated when a building wall constitutes the perimeter barrier. When it is impossible to have adequate clear zones because of property lines, natural or man-made features, it may be necessary to increase the height of the perimeter barrier (except for building walls), Increase security patrol coverage, provide more protective lighting, or install an intrusion detection system (IDS) along that portion of the perimeter barrier.

80. Protective lighting. Protective (or security) lighting provides a means of continuing, during periods of reduced visibility, a degree of protection close to that maintained during daylight hours. Protective lighting has considerable value as a deterrent to would-be thieves and vandals and makes the actions of a potential saboteur more difficult.

80.1 Protective lighting planning. Protective lighting is an essential element of an integrated physical security program. Its application at various facilities depends upon local conditions and the nature of areas to be protected. Each situation requires careful study to provide the visibility that is practical for security duties such as verification of access authorization credentials, prevention of illegal/unauthorized entry into restricted areas, and inspection of unusual suspicious circumstances. When protective lighting provisions arc impractical, additional security measures such as increased security patrols, additional sentries, or an alarm system will be necessary. To be effective, protective lighting should discourage or deter attempts at unauthorized entry by intruders and make detection certain if such entry is attempted. Proper illumination may lead a potential intruder to believe detection by security forces is inevitable.

80.2 Protective lighting design. In designing a protective lighting system, specific consideration should be given to the physical layout of the facility, other buildings of the installation, terrain, atmospheric and climatic conditions, and the additional protective requirements over and above those measures already in existence. All isolated limited and exclusion areas that are external to a large installation must have protective lighting on a permanent basis at perimeter and access control points. The lighting must be positioned to prevent glare that may impair the vision of security personnel and to avoid silhouetting or highlighting the guards. Protective lighting systems should be designed so that failure of one or more lights will not significantly reduce security effectiveness. High brightness contrast between intruder and background is another consideration. Predominately dark, dirty surfaces or camouflage-type painted surfaces need more light to produce the same brightness around buildings than do clean concrete, light brick, and grass. When the same amount of light falls on an object and its background, the observer must depend on contrasts in the amount of light reflected. The observer can more easily distinguish poor contrasts by increasing the level of illumination. When the intruder is darker than his background, the observer primarily sees the outline or silhouette. Intruders in this situation may be foiled if light-colored finishes on the lower parts of buildings and structures are used. Reflective stripes on building walls are also effective because they provide recognizable breaks in outlines or silhouettes. Two basic methods (or a combination of both) may be used to provide practical and effective protective lighting. One method is to light the boundaries and approaches. A second method is to light the area and structures within the boundaries of the restricted area. Facility engineers should consult physical security specialists to help determine the appropriate type and the degree of protective lighting system(s) that best serves the security needs of the facility being designed or reworked.

90. Intrusion detection system (IDS). An IDS is an integral element of an in-depth physical security program and plays a vital role in the protection of classified facilities, equipment, and material. For an area to be secure, an IDS must focus upon detecting unauthorized individuals at the entry point (gate, door, fence, etc.), area (building, field, room), or at a specific object (vault, file, safe). Remember, when selecting an IDS for a facility, any IDS is useless unless it is backed up by a prompt security force response when an IDS alarm is activated.

90.1 Purpose of IDS. An IDS is used for one or more of the following reasons:

a. Economy. An IDS permits more efficient and economical use of manpower. It cases the manpower intensiveness associated with security forces.

b. Substitution. An IDS can be used in place of other physical security measures which cannot be used because of safety regulations, operational requirements, appearance, layout, cost, or other reasons.

c. Augmentation. An IDS provides additional physical security controls at critical points or areas.

90.2 IDS planning considerations. The following factors need to be considered to determine the necessity and feasibility of installing an IDS:

a. Mission of the facility.

b. Criticality of the facility, or its information, to the mission of the organization.

c. Vulnerability and accessibility of the facility to human threat.

d. Geographical location of the facility and the location of the areas to be protected inside the facility.

e. Facility construction.

f. Hours of operation.

g. Existence and availability of other forms of protection.

h. Initial and recurring cost of the proposed IDS as compared to the cost (in money or security) of the possible loss of classified material and information.

i. Response time of supporting guard forces.

j. Savings in manpower and money over a period of time.

k. Intruder-detection time requirement.

90.3 Types of IDS. Many types of IDS exist and each is usually designed to meet a specific security problem. Point-of-entry, photoelectric, sound, vibration, motion, and beat detectors are but a few of the IDS components that can be used to secure a facility. The facility engineer, in cooperation with the physical security specialist, should determine which system, or combination of systems, best provides for the security of a planned/'existing facility.

100. Lock and key systems. The lock is the most widely used security device of the basic safeguards used to protect classified material and equipment. Regardless of the quality or cost, locks should be considered delay devices only and not positive barriers to entry. The facility engineer is responsible for determining the appropriate locks, latches, padlocks, and other locking mechanisms on doors, vaults, cabinets, and similar built-in items that are an integral part of a building or structure. Department or agency regulations may prescribe specific types of locks for specific types of facilities that store classified information.

APPENDIX C. ELECTROMAGNETIC PULSE (EMP)

10. General. A significant threat to the survivability of electronic systems used by the Department of Defense (DoD) is the effect of electromagnetic pulse (EMP). EMP is one of the destructive components of a nuclear detonation. Unlike the other destructive components (shook wave, thermal energy) whose effects are restricted to a region near the detonation, EMP, since it contains electrical and magnetic components, can be collected by conductors and transmitted great distances from the site of detonation. The EMP can disrupt communications, upset equipment operation, or cause equipment component destruction.

10.1 EMP generation. When a nuclear detonation occurs, gamma rays are produced which radiate outward from the burst at the speed of light (see figure C-1). As the gamma rays collide with air molecules, electrons are dislocated, creating Compton electrons. These electrons are affected by the magnetic fields of the earth, which create an electromagnetic (EM) wave that propagates toward the earth. To be effective. the burst must take place above the earth, at altitudes as low as 20 km. A burst 560 km above the geographic center of the continental United States would completely blanket the country.

10.2 EMP effects. The effects of EMP upon electronic equipment and components can be likened to the effects of lightning - stress by high currents and voltages. However, EMP produces higher currents and voltages, covers a greater frequency spectrum, and has a faster rise time (see figure C-2). Equipment may be subjected to state changes which cause improper operation (upset) or component failure (burnout). Upset is the introduction of spurious signals which temporarily disrupt normal operation or which may be misinterpreted by the equipment processor. Burnout is permanent damage to system components to the extent that the equipment is inoperative until replacement is effected.

20. Protection requirements. Certain DoD facilities, having time-urgent missions, mandate a high degree of assurance of immunity to EMP-induced upset or burnout. Other supporting missions may allow lesser degrees of protection, while accepting momentary upset. The objective then, of any EMP protection, is to ensure the currents and voltages induced by the EMP into electronic devices, or at other sensitive locations in a system, are smaller than a current or voltage which could reasonably be expected to produce damage or upset. The applied physical principles of EM compatibility may be used to develop such protection. Three fundamental approaches may be used:

a. The interfering signal source level may be reduced.

b. The receptor susceptibility may be reduced.

c. The attenuation of the path or paths over which interference is transmitted from the source to the receptor may be increased.

These approaches are implemented by increasing equipment robustness and isolating equipment from the EMP environment.

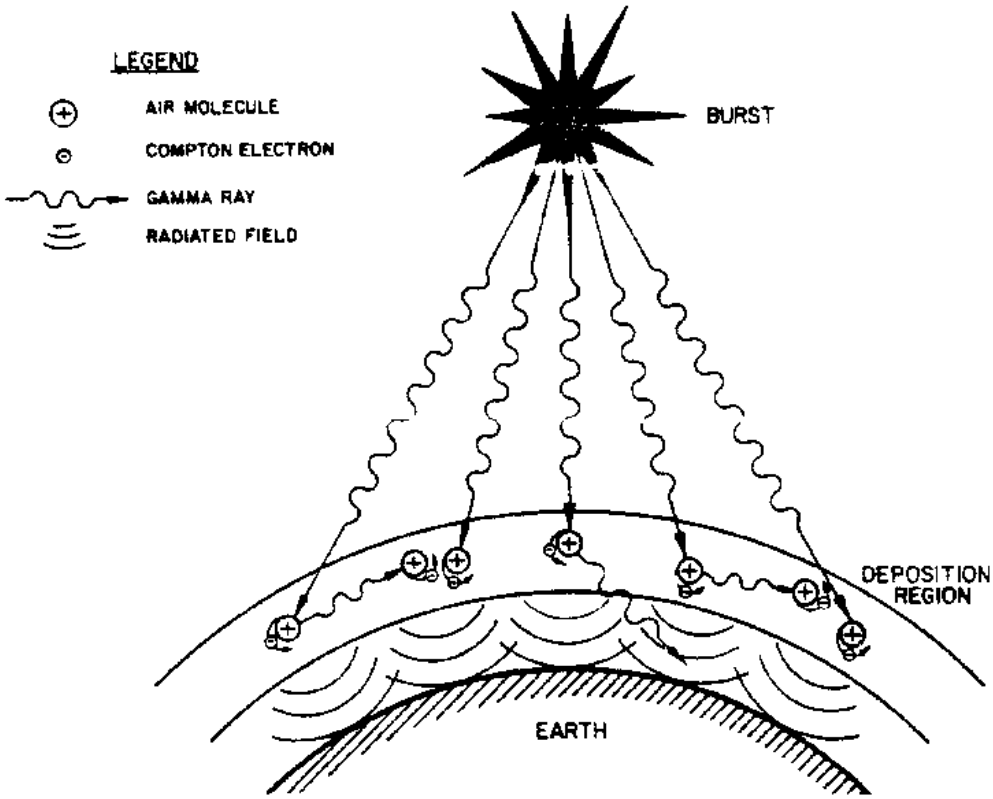


FIGURE C-1. EMP generator.

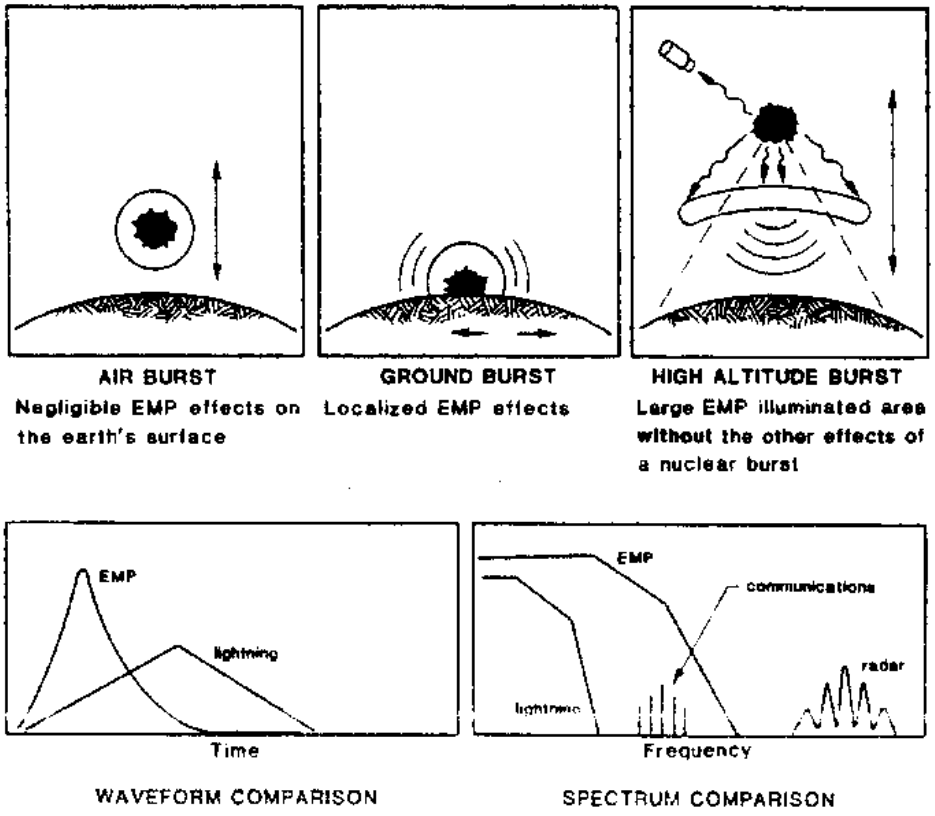


FIGURE C-2. EMP characteristics.

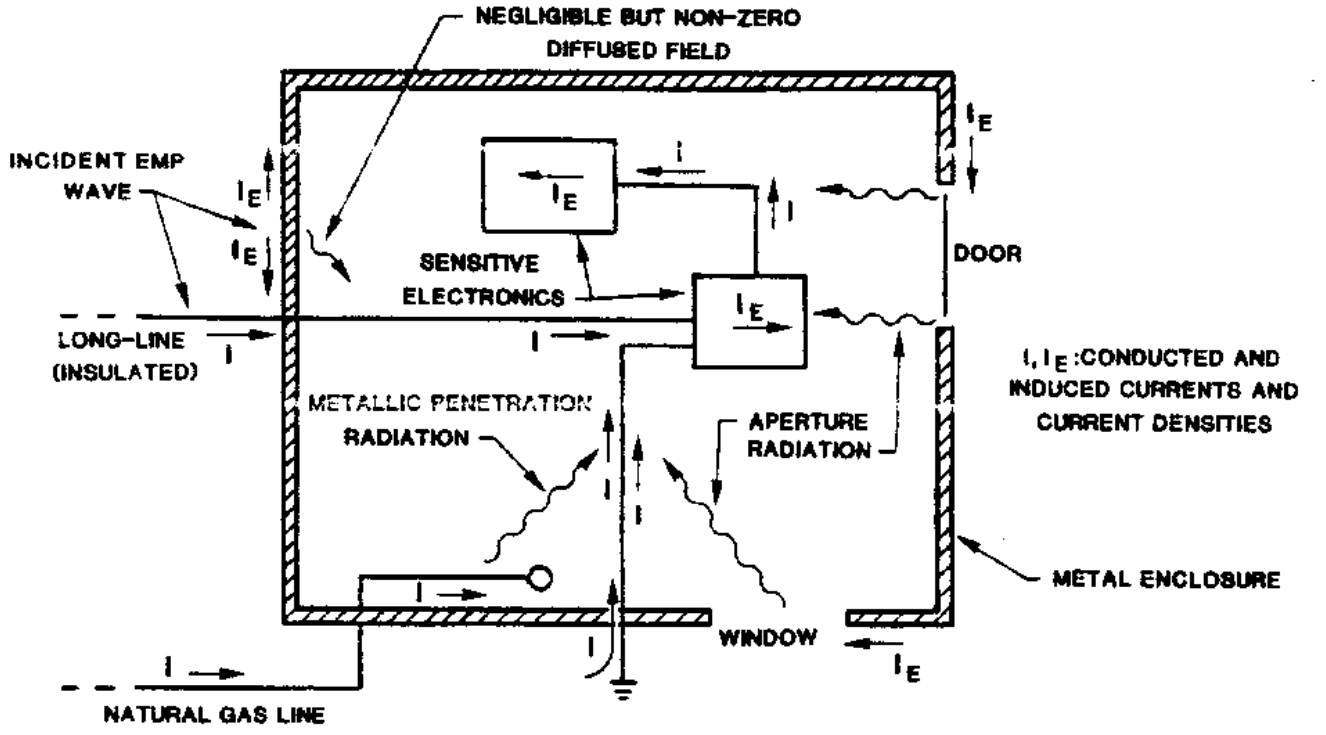
20.1 Isolation. To protect equipment, it is necessary to establish a barrier which is impervious to the EMP wave or greatly attenuates it (see figure C-3). A peripheral shield encapsulating the system can provide such protection. For any shield to be effective, it must be totally closed. However, because of penetrations for signal cables, power, heating, ventilating, and air-conditioning equipment, personnel entrances, etc., a totally closed shield is not attainable (see figures C-4 and C-5). Therefore, additional protection is provided by placing protective devices at the shield to electrically close any penetrations, treatment of apertures to prevent entry of EM radiation, and concentration of conducting penetrators in a single area to reduce current flow in the shield.

20.2 Shielding. An unbroken shield is quite effective against the EMP EM field. Less than a millimeter of copper, aluminum, or steel will reduce the field strength to near-ambient level. A two-level barrier approach is often used. A facility shield is installed to reduce the incident transient to less than that usually experienced by the contained equipment during normal operation. The equipment cabinets, cases, and racks then reduce the level of transients experienced on a routine basis to a level tolerable by the internal circuitry. This approach has the attractive feature that the internal barrier is continuously tested simply by operating the equipment in its normal environment of power surges, switching transients, and signal crosstalk. Shields installed and tested using MIL-STD-461 and MIL-STD-462 can reasonably suppress the magnitude of the radiated EMP.

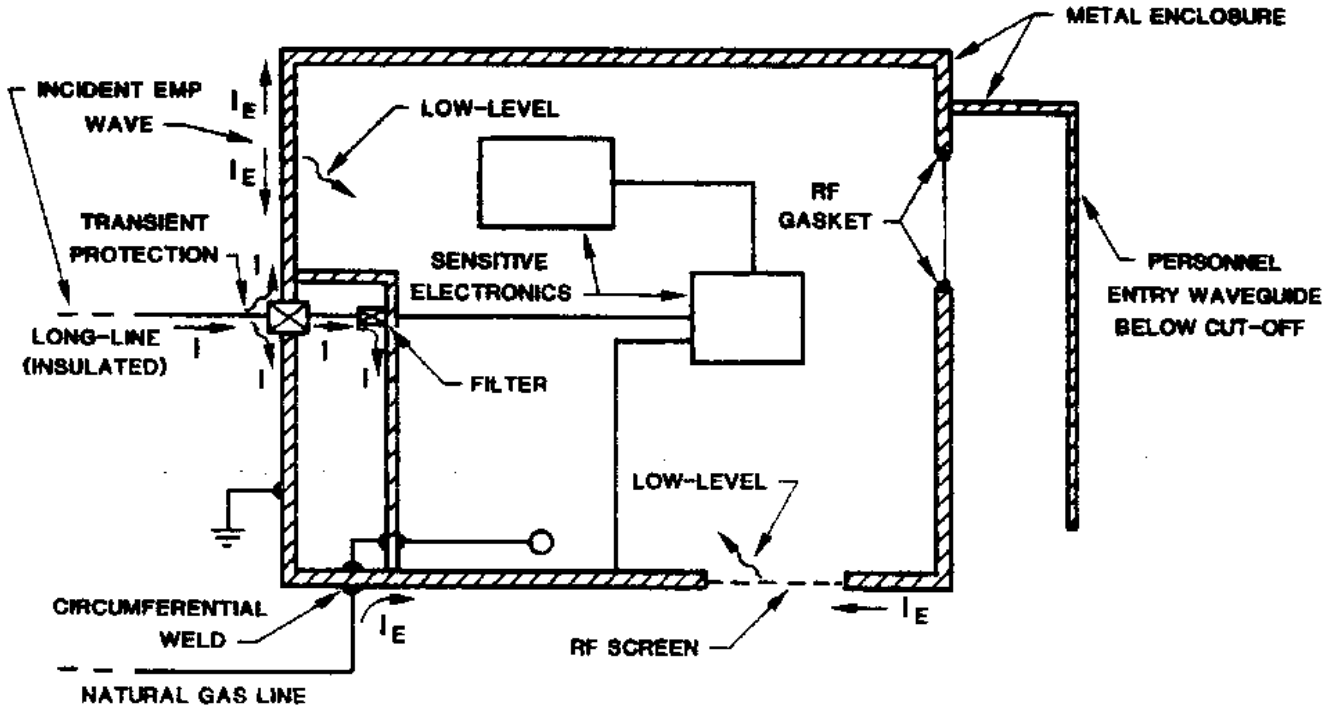
20.3 Apertures. The effectiveness of any shield is degraded by any apertures. Because of the broadband nature of the EMP, the number and size of allowable apertures is quite small. A single opening in a welded seam, for example, should not exceed 0.5 inch in its largest dimension. Multiple openings in the same area must be much smaller. Certain large apertures, like doors and windows, cannot be eliminated and must be treated in some way to strongly attenuate incident EM fields. Most apertures which cannot be eliminated can be treated with waveguide-beyond-cutoff techniques. A waveguide with a length five times its cross-sectional width provides approximately 100.dB attenuation of radiated EMP at frequencies below cutoff. The cutoff frequencies have wavelengths equal to twice the longest cross-sectional width. This treatment is well suited to personnel entries and conductor penetrations which cannot be filtered or otherwise treated. Apertures such as ventilating ducts can be effectively closed using honeycomb panels also conforming to the 5:1 length/width ratio. Windows may be treated with wire mesh embedded within the glass.

20.4 Penetrations. Conductors which penetrate the shield are far more serious than arc apertures in the shield. because the conductors carry the huge induced transients into the shielded facility. These conductors include not only signal and power cables and their shields, but also water and gas pipes, waveguides, etc. One general rule is that all conductors which can be grounded should be bonded circumferentially to the facility shield so that any induced current is shunted to earth by the shield. Another principle is that all penetrators, groundable or not, enter the facility through one localized region of the shield and are equipped with protective devices. Cable shields fall into the category of groundable conductors, but the enclosed conductors do not, and must be relieved of the EMP-induced transients before entering the facility. The recommended technique is to run all nongroundable conductors (power and signal) through the entry plate into an EMP vault. An EMP vault is a shielded enclosure within the facility shield, having the entry plate in common with the shield. Within the EMP vault, each conductor goes through a terminal protection device (spark gap, metal oxide varister, etc.) followed by a capacitor-input filter (lowpass or

bandpass) to remove any remaining transient components, as well as the "splatter" created by the action of the surge arrestor. Filters constructed with multiple PI sections are preferred over other filter constructions (see filter and isolator requirements and installation, MIL-HDBK-232A).

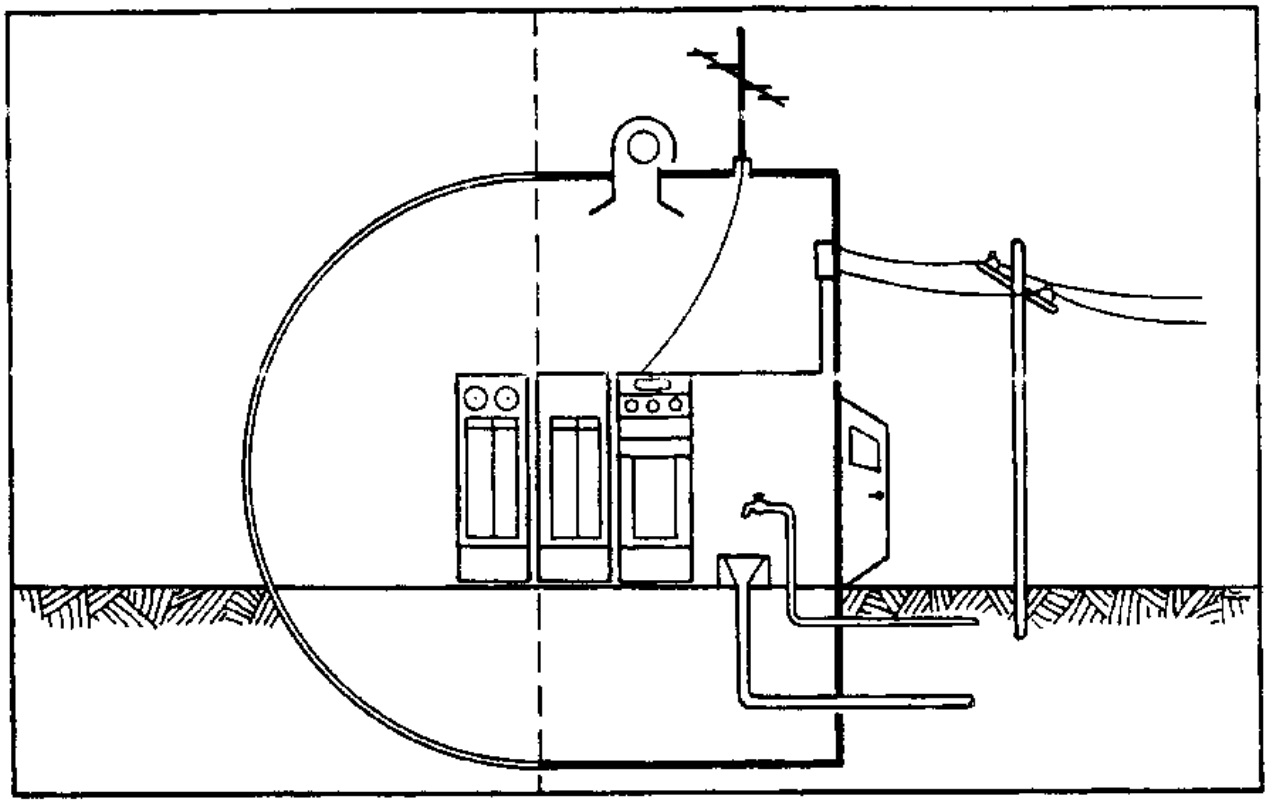


a) MULTIPLE INTERACTIONS WITH UNCONTROLLED "SHIELD"



b) APERTURE AND PENETRATION CONTROL

FIGURE C3. Unprotected and protected facilities.



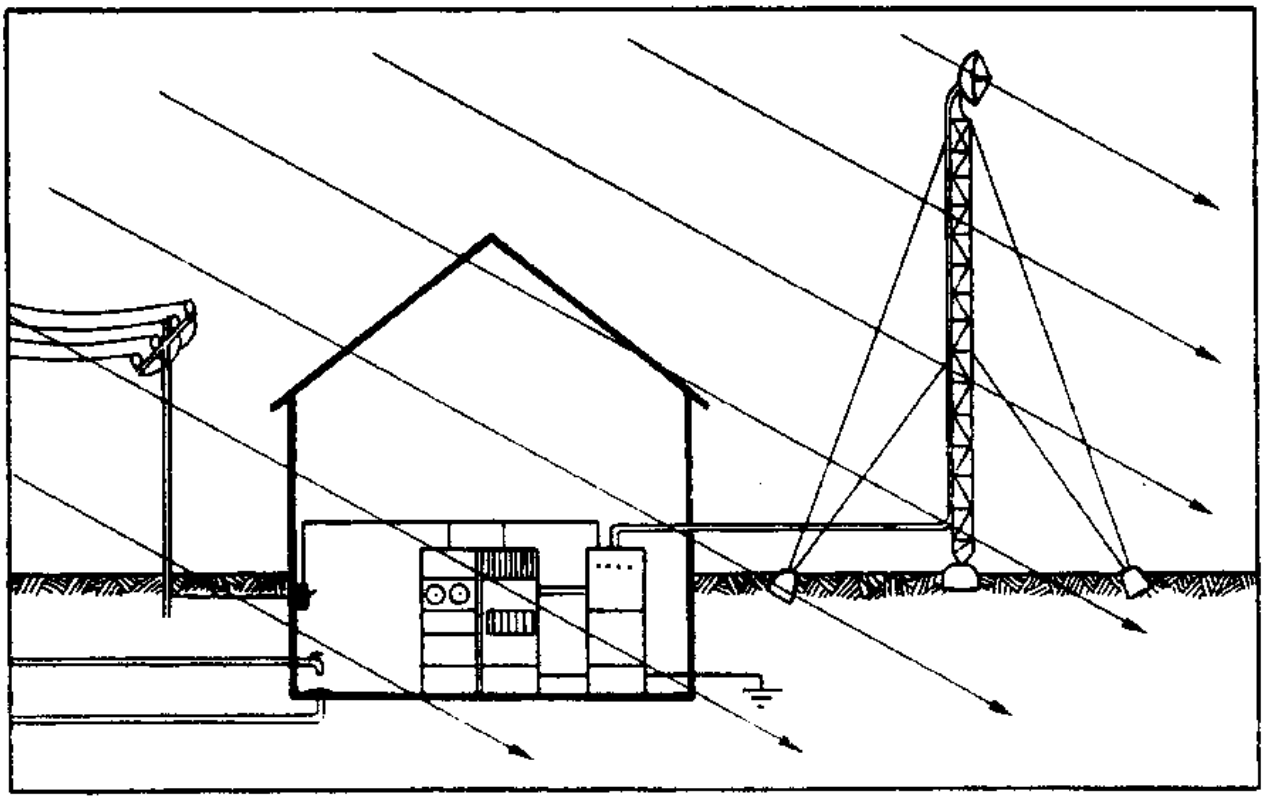


FIGURE C-4. Protection principles.

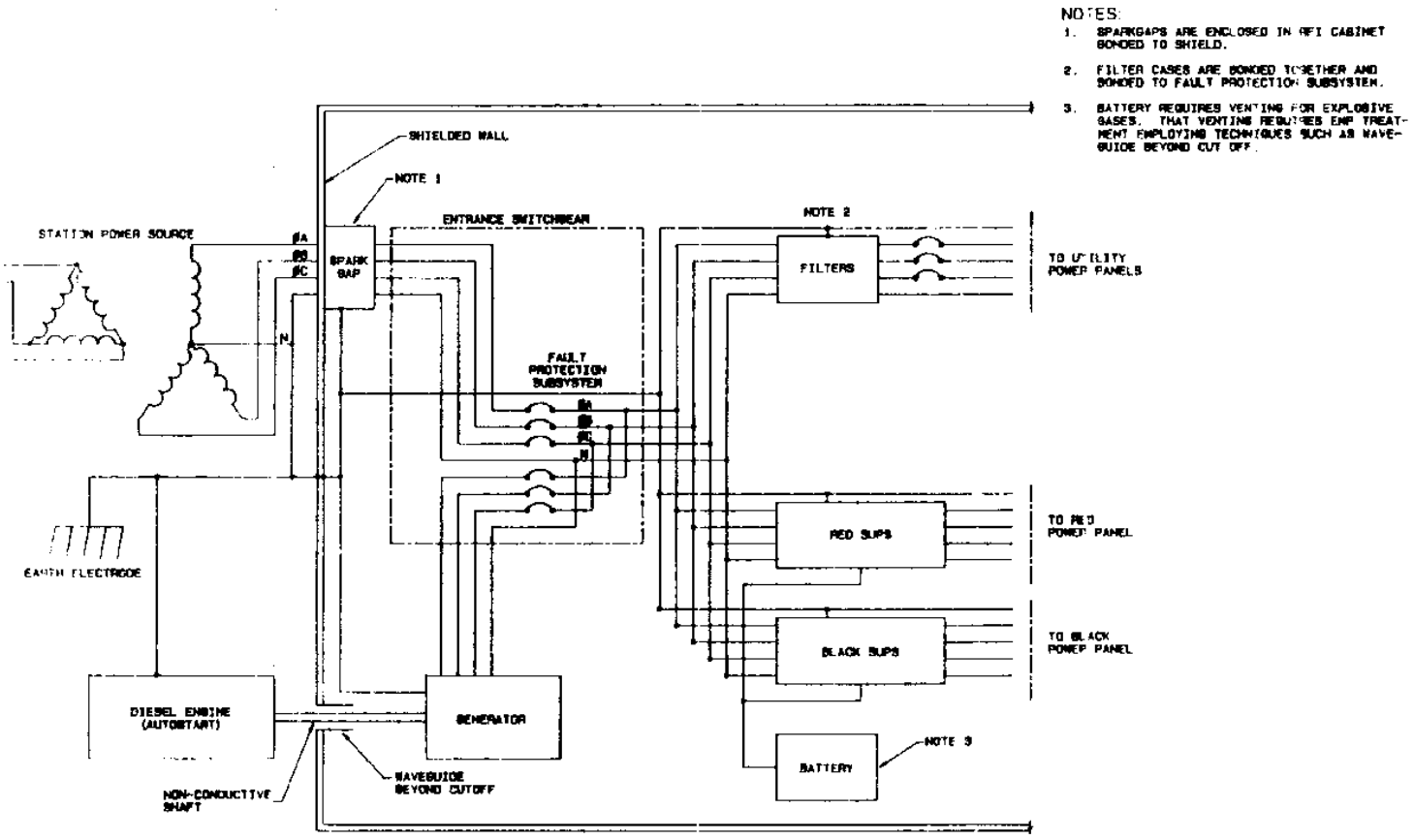


FIGURE C-5. TEMPEST/EMP treated power.

20.5 Grounding and bonding. The previously described principles arc of little or no consequence if proper grounding and bonding techniques have not been used. The goal of all grounding and bonding techniques is to redirect the EMP into the earth. Thus, an effective earth electrode subsystem (EESS) is required, with positive bonds to the shield, positive bonds between elements of the shield, and protective components coupled to the shields. Guidance for grounding and bonding is given in MIL-HDBK.419.

30. TEMPEST considerations. One might conclude that the guidelines for EMP and TEMPEST are the same. Where EMP protection has been applied, a benign TEMPEST environment external to a facility may exist. Within the facility, however, a hostile TEMPEST environment may exist if proper attention has not been given to TEMPEST principles. One may also be led to consider a TEMPEST facility to be immune from EMP. While the facility may be TEMPEST safe, it may be vulnerable to the magnitude of the EMP. The design of such facilities should account first for TEMPEST protection, then EMP protection. In this manner, those attributes which are mutually satisfactory may be successfully integrated. Where conflicts exist, tradeoff’s ran be identified, thus achieving the most cost effective design.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. COMPUTERIZED TELEPHONE SYSTEMS

This appendix contains the Report to the Community: Computerized Telephone Systems, June 30, 1983.

THIS PAGE INTENTIONALLY LEFT BLANK

TECHNICAL SURVEILLANCE COUNTERMEASURES SUBCOMMITTEE
AUDIO COUNTERMEASURES WORKING GROUP
TELEPHONE SECURITY PANEL
JUNE 30, 1983
REPORT TO THE COMMUNITY:
COMPUTERIZED TELEPHONE SYSTEMS

It is the policy of the U.S. Intelligence Community that all appropriate audio security measures are rigorously enforced for any telephone system which services an area where classified information is discussed. It has been a matter of concern that appropriate audio security measures for computer controlled private branch telephone exchanges have not been clearly defined; the installation and operating standards developed by the Telephone Security Panel, and provided in this report, are intended to remedy this deficiency.

A private branch exchange (PBX) operates, essentially, as a private telephone subnetwork. It ties together an internal group of subscribers into an independent network and provides external connections to the universal network by means of trunk lines to a telephone company central office exchange. A computer controlled private branch exchange (CBX) uses stored program computer technology to perform the necessary message switching functions. The resident computer in modern commercial CBX has made it possible to incorporate a multitude of attractive features for many diverse applications. There are many features which enhance the basic telephone service but the applications are not restricted to telephone service; modern CBX systems provide data processing, word processing, energy consumption control, communications traffic analysis, and other services in addition to processing telephone calls. CBX systems were introduced in the nineteen seventies. There are a great number of manufacturers from many countries producing them; to a large extent they are utilizing different technologies and approaches to achieve basically the same objectives. There has been from introduction, uncertainty as to how the inclusion of CBX systems at sensitive locations affects the security of those locations. This uncertainty developed because the CBX properties and features were unfamiliar and because computer software (rather than easily verifiable hardwire connections) is used to implement the features and to control the network switching functions.

It has been determined that the security-related concerns and considerations which must be accommodated with a CBX are essentially the same as for any type of telephone system. In fact, a great number of telephone company central offices use the same kind of stored-pro,-ram computer-controlled switching to provide multifeature CENTREX service.

All of the protective measures now accepted for central off ice service and manual PBX systems are fully as effective with CBX systems. These measures are designed to assure that on-hook audio signals (room conversations picked up by some microphonic function in a telephone, or other station equipment such as a console or data terminal, while it is on-line but not actually being used in a telephone call) cannot become available for clandestine, unauthorized, intercept. This is accomplished by requiring specified isolation or disconnect devices on the telephone lines, either on the lines connecting to the station equipment or on the lines leaving the physical control zone (PCZ). The isolation/disconnect devices are located within the PCZ. They prevent audio signals originating at the on-hook station equipment from being transmitted any further on the telephone lines, thus eliminating

all possibility that on-hook audio will be transmitted out of the PCZ on the telephone wires. Properly designed and constructed station equipment can be type-accepted by the community as intrinsically fulfilling the isolation/disconnect requirement without additional support.

CBX configurations incorporating the accepted isolation/disconnect measures need not be subject to any installation or operational restrictions unless consideration is being given to concerns other than on-hook audio.

Isolation of the station equipment from all uncontrolled lines forms the basis for the community's program to prevent an on-hook audio compromise of national security information. The use of specialized isolation/disconnect devices or station equipment to achieve this isolation, however, for large CBX installations often involves unmanageable economic, logistic, and/or operational burdens and becomes impractical.

The Telephone Security Panel has developed a set of installation standards, conformance to which will permit a CBX system to be used without the special isolation/disconnect or station equipment normally required, These standards, which are listed below, are predicated upon having located the CBX within the PCZ so that the CBX may be used as the means of isolation. The entire local telephone system is strictly organized to assure that no means is provided for on-hook audio to be present on any external lines. This approach also provides the opportunity to deny external access both to internal calls and to call detail information for the individual subscriber stations: benefits not available with CENTREX or uncontrolled CBX systems using conventional isolation methods.

TSP GUIDELINES FOR COMPUTERIZED TELEPHONE SYSTEMS

I. Minimum standards for CBX on-hook audio protection.

1. Physical security measures: A physical control zone (PCZ) with appropriate physical security is required over the entire area of concern.

1.1 The CBX is located in the PCZ. If the CBX supports station equipment located in a nonconterminous PCZ, then those stations are not protected by the isolation provided by the CBX installation and they must be provided with special isolation/disconnect devices or station equipment.

1.2 If the PBX supports any nonapproved or unprotected station equipment within the area of concern, all lines, intermediate wiring frames, and distributed CBX equipment modules (to include voice and data links) associated with these stations are contained within the PCZ.

1.3 All program media (tapes, disks, etc.) are provided positive physical protection against unauthorized alteration. A certifiably correct master program is always maintained under secure conditions to be available as a check of the operating program and a means of removing possible or identified software security deficiencies.

2. System configuration: The system configuration must effectively isolate the station equipment from all lines which leave the PCZ.

2.1 Two separate dedicated wiring frames (or sets of wiring frames) are are maintained inside the PCZ containing the CBX to support connections with facilities outside that PCZ. These are termed "external" wiring frames (in this paragraph) to distinguish them from frames used to connect the CBX to equipment located within the PCZ. One of the "external" frames is used to terminate all lines entering from outside the PCZ (C.O. trunks, tie trunks, telephone, etc.). It is located at the point of entry for these lines and is available for inspection. The second of the "external" frames provides the connections to the CBX. Cross-connections between the two "external" frames are limited to only those needed to extend active central-office lines to the CBX. The "external" wiring frames are separated by at least three feet from each other and from all internal wiring frames. No cross-connections are permitted between internal and "external" frames. CBX port circuit packs connected to "external" wiring frames are not installed in the same circuit carriers as those connected to Internal wiring frames. No two carriers share common cabling to the wiring frames. All cross-connect strapping pairs at the cross-connect fields are labeled as to identification and/or purpose. Each cross-connect label cites the appropriate paragraph or drawing of the installation document which prescribes the connection.

2.2 Each individual subscriber station has dedicated running wires to a specific, individual, port circuit of the CBX. Off-hook connections between port circuits are accomplished by metallic (or electronic) switching or by multiplex bus methods. The CBX keeps the running wires of every port circuit separate and unconnected from those of every other port except in the case of metallic switching, and then connections may only occur for ports actually engaged in an information interchange between off-hook subscriber stations (or between a station and a trunk). Audio coupling in either direction through a switch or between a port circuit and a multiplex bus only occurs when the associated station equipment or trunk is off-hook. (Off-hook here is intended to mean that a subscriber station or trunk connected to the CBX is initiating or actively engaged in communication either with the CBX itself or with some other subscriber station or trunk by means of a link established by the CBX.)

2.3 No port circuits or assigned station directory numbers are shared by extension stations inside the PCZ with extensions outside the PCZ. All extensions from the same port circuit or with the same station directory number are either wholly contained within the PCZ or wholly excluded from it.

2.4 Speakerphones are not permitted.

3. Prohibited functions: Some operational features that may be available with the CBX involve functions which are not consistent with good audio security practices. These functions are expressly prohibited and any CBX feature using them must be disabled.

3.1 The CBX must not be able to place or hold any subscriber station in an off-hook condition unless directed to do so by that subscriber station itself. The off-hook condition is completely controlled by

the station equipment.

3.2 There is no means for remote access to any CBX services.

3.3 Incoming calls (trunk or local) come to a console or telephone and are answered manually. There is no voice activated pickup, automatic pickup (e.g., by telephone answering units and ADP terminals), or other responses of any kind to incoming calls except annunciation (initiated by the CBX) to the called station.

4. Administrative security measures: Administrative procedures are needed to ensure that none of the protective measures are intentionally or inadvertently degraded as a result of hardware or software chances to the system. Some of the administrative procedures are described functionally as requirements to be achieved. Their implementation may be any combination of physical security, systems configuration (hardware, software, and layout), personnel security, and technical countermeasures appropriate to the particular CBX and installation in question.

4.1 An appropriate minimum level of security clearance is determined by the cognizant agency for personnel having access for any purpose (to include installation and maintenance) to the station equipment, CBX components, wiring, and distribution frames located within the PCZ. Persons not possessing the minimum clearance will not be permitted access to the system except outside the PCZ or under suitable administrative safeguards.

4.2 Positive barriers exist to prevent all system diagnostics and CBX software modifications except those from specific programming stations located within the PCZ.

4.3 Only specific designated individuals with appropriate security clearance have physical access to the programming stations and may change the system software or hardware configuration.

4.4 The integrity and efficacy of the protective measures are to be assured with a regular program of countermeasures inspections.

4.5 Frequently reload the operational program medium from the certifiably correct master to assure that no unauthorized changes have occurred.

4.6 All system documentation including instructions, manuals, installation and service practices, system configuration records, etc. arc to be kept with the CBX in the PCZ.

4.7 Dial access or barrier codes are not acceptable means for denying unauthorized persons access to any CBX features or control operations.

II. Other considerations: Most telephone installations of interest to the U.S. Intelligence Community involve other telephone security considerations in addition to the fundamental problem of on-hook audio. Application of the below listed supplementary measures will realize the full potential of the CBX to address those concerns: these measures are recommended by TSP wherever operationally feasible.

1. If the CBX provides any features which allow subscriber stations and attendant's consoles to monitor the audio or data at other stations (such as line or trunk verification or executive override), positive barriers are placed into the system to prevent implementing these features from outside the PCZ.

2. Central dictation features are disabled.

3. There is no CBX accessed central loudspeaker paging system.

4. All attendant's consoles are located within the PCZ.

5. Number of central answering positions is minimized.

6. Except for attendant's consoles, telephones are single line 2500 type.

7. The CBX does not maintain call detail recording information (beyond the temporary storage that is necessary to support the communications switching functions and auxiliary features) unless positive barriers exist to preclude access to this information from outside the PCZ.

8. The CBX does not maintain speed calling lists.

9. The CBX and all critical station equipment are powered from uninterruptible power supplies.

10. Service provided to facilities located outside the PCZ can be curtailed to provide priority service to internal communications.

11. All switching, maintenance, or operational conditions set up from subscriber stations can be selectively cancelled by an attendant's console located within the PCZ.

Custodians:
Army -- SC
Navy -- EC

Air force -- 90

Review activities:
Army - CR
Navy - EC, MC
Air Force - 17, 89
DoD - DC, NS, JT

Preparing activity:
Army -- SC

(Project SLHC-2322)