NCS TIB 80-3

NATIONAL COMMUNICATIONS SYSTEM

TECHNICAL INFORMATION BULLETIN
80 - 3
EMP VULNERABILITIES OF TELECOMMUNICATIONS FACILITIES AND THEIR RELEVANCE TO EMP PROTECTION STANDARDS

APPROVED FOR PUBLIC RELEASE;
DISTRIBUTION UNLIMITED

JUNE 1980

NCS TECHNICAL INFORMATION BULLETIN 80-3

EMP VULNERABILITIES OF TELECOMMUNICATIONS FACILITIES AND THEIR RELEVANCE TO EMP PROTECTION STANDARDS

JUNE 1980

PREPARED BY:

CHAD STANSBERRY
(DEF COMM ENGR CENTER)
For
Office of NCS Technology
and Standards

APPROVED FOR PUBLICATION:

Marshall L. Cain
MARSHALL L. CAIN
Assistant Manager
Office of NCS Technology
and Standards

FOREWORD

The Manager NCS, under a recent statement of national security telecommunications policy, is responsible for the development of standards and practices to improve the survivability and utility of Federal telecommunication resources during national emergencies. Accordingly the NCS has just completed a three phase study effort leading to the identification of specific EMP protection standards which should be developed to provide a reasonable degree of protection of government owned and leased telecommunication facilities against disabling dameage from EMP. The Phase I results are depicted in NCS Technical Information Bulletin (TIB) 78-1. The Phase II results, identifying and categorizing the reasons for EMP vulnerability of attended and unattended terrestrial communication facilities, are presented in this document. The Phase III results, identifying the categories of standards requiring development to decrease EMP vulnerabilities, are presented in NCS TIB 80-4. Comments concerning this TIB are welcomed, and should be addressed to:

Office of the Manager
National Communications System
ATTN: NCS-TS
Washington, D.C. 20305
(202) 692-2124

Executive Summary

This report identifies and categorizes the reasons for High Altitude Electromagnetic Pulse (HEMP) vulnerability of terrestrial communication equipment and systems for leased and government owned stations in both manned and unmanned categories.

The reasons for this vulnerability fall into six categories: three relating to damage and three to upset. Damage is defined as destruction of a component such that its repair or replacement is required, and upset was defined as a change in the functional/operational state of the equipment that is either self correcting or resettable/restorable by operating personnel.

Equipment lists for generic categories of leased and government owned telecommunication facilities are presented for manned and unmanned stations, and correlated with available HEMP vulnerability data to provide lists of vulnerability reasons.

The most frequently occurring cause for HEMP vulnerability was inadequate electrical isolation of equipment cables from power lines, groundwires, waveguide, and other building penetrators. The second most frequent was improper or inadequate inter-equipment cable shields and cable shield terminations. The third most frequent was inadequate (low) failure thresholds for components used in the equipment design.

It was concluded that vulnerability distinctions do not exist between leased or government owned systems. Manned and unmanned vulnerability differences exist, but only in their degree of vulnerability. Essentially, the causes remain identical.

Recommendations are made to develop Federal EMP protection standards specifying standard techniques for alleviating the HEMP vulnerability of telecommunication facilities through (1) more effective electrical isolation of facility penetrators (2) more effective electrical shielding of the facility, its internal wiring and installed equipment and (3) improved damage thresholds for equipment critical to uninterrupted operation of the facility.

1.0 Introduction

This report identifies the electromagnetic pulse (EMP) vulnerabilities of both leased and government owned telecommunication facilities in two categories: manned and unmanned stations. The major task was to identify specific components/equipment/facility design practices that accounted for the vulnerabilities and determine the reasons for any difference among the categories.

The information presented was extracted and summarized from unclassified government reports and data files.

The primary purpose of this effort was to identify potential design practices or design practice programs that could lead to the development of federal standards for the design, installation and maintenance of telecommunication facilities.

1.1 Background

High-altitude EMP (HEMP) vulnerabilities and effects have been investigated by the research community for over a decade. Two programs have suitable and sufficient details for organizing the vulnerability of telecommunications into preliminary cause-and-effect groupings for the purpose of this report. The two programs are the Safeguard and the PREMPT (Program for EMP Testing). Both programs primarily studied the leased manned telecommunication stations employed by the common carriers. Only a small sampling of government owned equipment has been evaluated. This drawback is not serious. The vulnerability reasons were separated into six categories, and these categories are directly applicable to government owned equipment. The six categories are technically consistant and represent the maximum delineation possible under the constraints of data availability, data accuracy, and the state-of-the-art in EMP technology.

1.2 Report Organization

The report initially defines six vulnerability categories, their technical rationale, and describes the specific reasons for vulnerability that are assigned to each category. Three categories relate to equipment damage and three to equipment upset. For the purpose of this report, damage is defined as destruction of a component such that its repair or replacement is required, and upset is defined as a change in the functional/operational state of the equipment that is either self correcting or resettable/restorable by operating personnel.

Data on the common carrier leased station vulnerabilities is the most voluminous and consequently is discussed first. It in itself is essentially sufficient for the report purpose. This is followed by the government owned station vulnerabilities. Two different categories of unmanned stations are defined for convenience; unmanned repeater stations and unmanned user stations. Unmanned in this context means that technical personnel are not available for restoring service if damage or manual intervention for reset or restart is required. Power equipment vulnerabilities were deemed important enough to warrant a separate section. The technical presentation is followed by a discussion of the commonalities and differences found in the causes of vulnerability. It was clear that there are vulnerability characteristics that span the categories and lend themselves to cure by systematic standardizations. The conclusions section details those vulnerability areas that are suitable for a design practice development program that could lead to the development of Federal EMP Standards.

In general, it is assumed that the reader is acquainted with the telecommunications industry vocabulary. However, functional descriptions and charts are provided to guide the uninitiated through the transmission/switching equipment from one communications user to the next. Additionally, the report provides a set of charts that summarize the typical equipment complements at each manned/unmanned station, and the reasons for vulnerability.

2.0 Facility and Equipment Vulnerabilities

Data Base. Figures 2.1 to 2.6 represent the facility and equipment data base used for this report to characterize EMP vulnerabilities of leased and Government owned communication systems for both manned and unmanned stations. Two unmanned categories have been defined; the transmission repeater and the user stations.

This EMP data base is largely incomplete, since there are many equipment types that have not been examined or listed. It is, however, sufficiently broad to clearly indicate and categorize the specific reasons for vulnerabilities. These reasons fall into six categories, that led to the definitions and classification rules listed below for interpreting the data base. In general, these classification rules require only two items from this data base in order to identify the equipment vulnerability category. The first is whether the equipment was damaged or upset, while the second item is the value of EMP current at which damage or upset occurred. The rules are based on observations made in telecommunication facilities while under simulated HEMP illumination and on equipment subjected to HEMP like transients in the laboratory. The upper bound current found on interbay leads was 130 Amperes peak to peak (Ap-p). This peak is achieved via coupling from conductors which enter (penetrate) the facility from the exterior. A maximum of 20 Ap-p was observed when equipment was buffered from these penetrator conductors. The rationale behind the causal vulnerability rules is discussed in more detail after the rules are presented. The rules are:

Causal Vulnerability Classification Rules for Damage

Damage Rule 1: Equipment damage that occurs when EMP currents on intrasite cables exceed 20 Ap-p is caused by inadequate electrical isolation of the constituent component parts from conductors or metallic structures that penetrate the facility building. These penetrators include equipment groundwires, signal and power cables, antenna structures, waveguides and fuel/water lines. A corollary is that equipment is immune to EMP damage if no failure occurs when the EMP induced equipment cable currents exceed 130 Ap-p.

Damage Rule 2: Equipment component damage that occurs when EMP currents on equipment cables exceed 2.0 Ap-p and are less than 20 Ap-p is caused by improper cable routing, inadequate cable shielding, or inadequate circuit design failure thresholds for EMP transients.

Damage Rule 3: Equipment component damage that occurs when EMP currents on equipment cables is less that 2.0 Ap-p is caused by inadequate circuit design failure thresholds, and are likely to fail due to power and lightning transients as well.

Causal Vulnerability Classification Rules for Upset

Upset Rule 1: Equipment that upsets when EMP currents on its cables exceeds 20 Ap-p and are less than 130 Ap-p is caused by inadequate isolation from penetrators.

Upset Rule 2: Equipment that upsets when EMP currents on its cables exceeds 2.0 Ap-p but are less than 20 Ap-p is caused by improper cable routing, inadequate shielding, and improper shield terminations.

Upset Rule 3: Equipment that upset when EMP currents on its cables is less than 2.0 Ap-p is caused by inadequate circuit design upset failure thresholds.

Note: If upsets occur below 13 Ap-p, damage rule 1 applies based on the empirical assumption that damage thresholds are 10 times the upset threshold.

Rationale for Vulnerability Classifications

Experiments and worst case analyses have shown that the maximum likely equipment induced currents do not exceed 20 Ap-p. Note: 2.0 Ap-p is the maximum likely value for shielded buildings. These EMP current values do not include the contributions due to EMP coupling from building penetrators which raises the maximums to about 112 Ap-p and 130 Ap-p respectively for the shielded and unshielded building. Other experiments have shown that EMP source impedances range from 5 ohms to 400 ohms with a reasonable average being 100 ohms. Other data indicates that properly shielded cable reduces EMP currents by about 20 db for the interior conductors.

Using these data, failures must be attributed to penetration effects if a failure occurs above 20 Ap-p, but the equipment is immune if failure occurs above 130 Ap-p. This corresponds to about a 2 KV to 13 KV voltage threshold for failure. At these levels it is clearly a better practice to isolate the penetrators rather than raise the components failure thresholds. Hence, penetration standards are mandatory for reducing penetration current effects in telecommunications facilities.

Continuing this reasoning, failure between 2.0 and 20 Ap-p (200 volts to 2000 volts) can be attributed to poor equipment cable shielding or routing, and shield termination defects. This is reasonable since the vast majority of circuit designs can usually pass a 200 volt transient specification.

LEASED TRANSIMSSION SYSTEMS

MULTIPLEX EQUIPMENT
FDM/ANALOG CHANNELS
1. A4, A5 - Channel Banks
2. LMX - Group Banks
3. MMX - Master Group Banks
4. PFS - Primary Frequency STD
DIGITAL - TDM
1. D3 Multiplexer
2. D4 Multiplexer

TECHNICAL CONTROL
1. No Data

TRANSMITTING/RECEIVING EQUIPMENT
FDM/ANALOG CHANNELS
1. Microwave Transmitters/Receivers TD2, TD3, TH, TJ, TL, TM
2. FM Transmitters/Receivers J68336, 3A, 3B, 4A
3. Wire Line Entrance Links J68833, 3A, 3B
4. FM Protection Switches FMAS, 200A
5. IF Protection Switches TDAS, THAS, 100A, 400A
FDM/ANALOG CHANNELS - COAXIAL CABLE
1. L1, L3, L4, L5, Auto Line Switch
2. L1, L3, L4, L5, Terminal Line Repeater
3. L1, L3. L4, L5, Power Separation Filter
4. L1, L3, L4, L5, Repeater Power Supplies
DIGITAL CHANNELS - TDM
1. T-1 Pulse Code Modulation

SIGNAL/SUPERVISORY PROCESSING EQUIPMENT
1. Voice Repeaters - 24V4, 44V4
2. Equalizers & Pads - LC-1
3. ECHO Suppressors - 931 GTE
4. 2/4 Wire Line Adapters
5. Supervisory/Signaling - SFSU 927 GTE

CIRCUIT SWITCHING SYSTEMS
1. ESS-1 Circuit Switch
2. AECo Circuit Switch
MESSAGE SWITCHING SYSTEMS
1. No Data

MANNED STATION - EQUIPMENT TYPES VS. FUNCTIONAL CLASSES

Figure 2-1

LEASED TRANSMISSION SYSTEMS

TRANSMITTING/RECEIVING RADIO REPEATERS
FDM/ANALOG CHANNELS
1. Microwave Transmitters/Receivers TD2, TD3, TH, TJ, TL, TM
TDM/DIGITAL CHANNELS
1. No Data

CABLE REPEATERS - FDM/ANALOG
1. L1, L3, L4, L5, Basic Repeaters
2. L1, L3, L4, L5, Requlating Repeaters
3. L1, L3, L4, L5, Equalizing Repeaters
CABLE REPEATERS - DIGITAL/TDM
1. T-1 Pulse Code Modulation Repeaters

SIGNAL CONDITIONING
1. Loading Coils
2. Build Out Capacitors
3. Voice Repeaters

UNMANNED STATION - EQUIPMENT TYPES VS FUNCTIONAL CLASSES

Figure 2-2

LEASED USER/TERMINATION SYSTEMS

SUBSCRIBER SWITCHING
1. PBX/PABX

SIGNAL/SUPERVISORY PROCESSING EQUIPMENT
1. Telephones - Touch Tone/Dial
2. Data Sets - 203/303, Teletype, CRT
3. Supervisory/Signaling - SFSU - 927 GTE
4. Voice Repeaters - 24V4, 44V4
5. Equalizers & Pads - 931 GTE
6. Line Adapters 2W/4W

TRANSMISSION SYSTEMS
1. Microwave Transmitters/Receivers
2. T-1 Pulse Code Modulation
3. N,O,K, Carriers

UNMANNED STATION - EQUIPMENT TYPES VS. FUNCTIONAL CLASSES

Figure 2-3

GOVERNMENT OWNED TRANSMISSION SYSTEMS

MULTIPLEX EQUIPMENT
DIGITAL TDM CHANNELS
1. TD1198 1st Level Mux
2. TD 2nd Level Mux
FDM/ANALOG CHANNELS
1. No Data

TECHNICAL CONTROL
1. Emergency Action Centers

TRANSMITTING/RECEIVING EQUIPMENT
DIGITAL CHANNELS - TDM
1. Microwave Transmitters/Receivers FRC 163
FDM/ANALOG CHANNELS
1. No Data
FDM ANALOG CHANNELS - COAXIAL CABLE
1. No Data

MESSAGE SWITCHING SYSTEMS
1. AUTODIN
CIRCUIT SWITCHING SYSTEMS
1. AECO
2. 4W5

SIGNAL/SUPERVISORY PROCESSING EQUIPMENT
1. Voice Repeaters - No Data
2. Equalizers/Pads - No Data
3. 2W/4W Line Adapters - No Data
4. Echo Suppressors - No Data
5. Supervisory/Signaling - No Data
6. Secure Voice - No Data

MANNED STATION EQUIPMENT TYPES VS FUNCTIONAL CLASSES

Figure 2.4

GOVERNMENT OWNED TRANSMISSION SYSTEMS

TRANSMITTING/RECEIVING RADIO REPEATERS
FDM DIGITAL CHANNELS
1. FRC - 163
FDM ANALOG CHANNELS
1. No Data

CABLE REPEATERS TDM/ANALOG
1. No Data
CABLE REPEATERS FDM/ANALOG
1. No Data

SIGNAL CONDITIONING
1. Loading Coils 2. Build Out Capacitors 3. Voice Repeaters

UNMANNED STATION EQUIPMENT TYPES VS FUNCTIONAL CLASSES

Figure 2.5

GOVERNMENT OWNED USER TERMINATION SYSTEMS

SUBSCRIBER SWITCHING
1. PBX, PABX, - No Data

SIGNAL/SUPERVISORY PROCESSING EQUIPMENT
1. Telephones - Touch Tone/Dial
2. Data Sets, Teletype - No Data
3. Supervisory/Signaling - No Data
4. Voice Repeaters - No Data
5. Equalizers/Pads - No Data
6. Line Adapters 2W/4W - No Data
7. Secure Voice

TRANSMISSION SYSTEMS

UNMANNED STATION - EQUIPMENT TYPES VS FUNCTIONAL CLASSES

Figure 2.6

Alternatively, the shielded building can or could substitute for the lack of shielded cable. Standards for shielding are therefore mandatory to avoid penalizing circuit designs.

Lastly, failure below 2.0 Ap-p (200 volts) is entirely due to inadequate circuit design damage thresholds. In fact engineering judgment would dictate that failure at these levels is excellent evidence that the circuits might well fail from normal line transients.

These rules and categories are arbitrary, but reasonable, and assist greatly in defining the standards necessary for EMP protection without defaulting to a technical posture that forces development of standards and specifications for every equipment component used in industrial designs. Such a posture has to be avoided since EMP failures are related to cable configuration/lengths which vary from facility to facility. It is easy to imagine the economic penalty of specifying a 2000 volt failure threshold for a $1.00 transistor or relay used and produced in quantities of millions.

The results of applying these rules to the data base is summarized in Tables 2.1 through 2.6. One chart each for the leased, government owned, manned and the two unmanned station equipment complements. An overall summary, rank ordered by frequency of occurence for each cause, is provided in Section 4.0.

It will be noted that nearly every equipment listed will fall into the damage rule category (i.e. insufficient isolation from penetrators). This may seem severe and arbitrary considering that some equipments tested at 80 Ap-p and above showed no vulnerability. It is essential however to bear in mind that penetrators carry EMP currents from 1000 Ap-p to 20,000 Ap-p and reasonable assurance of immunity demands appropriate isolation, especially in physical small facility buildings. This approach seems even more practical when these current values are translated to their voltage values of perhaps 5 KV to 100 KV. These values are sufficient for arc-over, possible power follow-thru and even fires.

2.1.1 Manned Station Equipment Vulnerabilities

2.1.1.1 Multiplex Equipment Vulnerabilities

Figure 2.7 is a block diagram of these equipments and their type numbers which form a Frequency Division Multiplex (FDM) scheme that is widely used for Microwave and Cable transmission systems. The multiplex equipment combines individual voice and low speed data channels such that a large number can be transmitted on a single channel. These combined channels are called groups, supergroups, and mastergroups, and occupy a channel bandwidth that is proportional to the bandwidth of the individual voice/data channels. The primary frequency supplies provide the signals for the multiplex function. The outputs of the multiplex are fed to the FM transmitters/receivers via the Wireline Entrance Links as shown in Figure 2.8. Figure 2.9 illustrates the multiplex input required for coaxial cable systems. The following discussion presents the known vulnerabilities of the Multiplex equipment and their effect on the transmission plant. Table 2.1 lists the vulnerability reasons/causes for this equipment class.

* Penetrators are exterior cables, antenna structures and ground wires that enter the facility / Couple EMP currents to equipment wiring

LEASED MANNED STATION VULNERABILITIES

FUNCTION	EQUIPMENT NAME & TYPE	VULNERABILITY REASONS
Multiplex, FDM	Channel Banks	Inadequate Isolation from Penetrators*
	Group Banks	Inadequate Isolation from Penetrators*
	Master Groups	Inadequate Isolation from Penetrators*
	Primary Frequency, STD	Inadequate circuit Design Upset Failure Thresholds for EMP Transients
Transmitting/Receiving	Microwave Transmitters and Receivers	
	TD-2B	Inadequate Isolation from Penetrators
	TD-3	Inadequate Isolation from Penetrators
	TH-3	Inadequate Isolation from Penetrators
	TL-2/TM-1	Inadequate Isolation from Penetrators
	N3	Inadequate Isolation from Penetrators, Possible Inadequate Circuit Design Failure Thresholds

Table 2.1

LEASED MANNED STATION VULNERABILITIES

FM TRANSMITTERS/RECIEVERS

Transmitting/Receiving Continued	J68336	Inadequate Isolation from Penetrators, Possible Inadequate Circuit Design Damage Thresholds
	3A, 4A	Inadequate Isolation from Penetrators
	WIRE LINE ENTRANCE LINKS	
	J68833	Inadequate Isolation from Penetrators
	3A	Inadequate Isolation from Penetrators
	FM & IF Protection Switches	
	(FM) FMAS	Inadequate Isolation from Penetrators, Possible Inadequate Circuit Design Damage Thresholds.
	(FM) 200A	Inadequate Isolation from Penetrators
	(IF) TDAS	Inadequate Isolation from Penetrators, Possible Inadequate Circuit Design Damage Thresholds.
	(IF) 100A	Susceptible to upsets from EMP, Power, or Lightning Transients due to Improper Wire Routing and Terminal/Shielding.
	400A	Inadequate Isolation from Penetrations

Table 2.1 (continued)

LEASED MANNED STATION VULNERABILITY

FUNCTION	EQUIPMENT NAME & TYPE	VULNERABILITY REASONS
FDM/Analog Channels, Coaxial Cable	L4, Terminal Equipment	Susceptible to upsets from EMP, Power, or Lightning Transients due to Improper Wire Routing and Terminal/ Shielding.
	L1, L3, L5 Terminal Equipment	No data available
Digital Channels TDM	T-1 PCM	Susceptible to upsets from EMP, Power, or Lightning Transients due to Improper Wire Routing and Terminal/ Shielding.
Circuit Switching Systems	ESS-1 Circuit Switch	Susceptible to upsets from EMP, Power, or Lightning Transients due to Improper Wire Routing and Terminal/ Shielding.
	AECo Circuit	Inadequate circuit design upset failure thresholds inadequate isolation from penetrators
Technical Control	No data	No data

Table 2.1 (continued)

LEASED MANNED STATION VULNERABILITIES

FUCTION	EQUIPMENT NAME	VULNERABILITY REASONS
Signal/Supervisory Processing Equipment	Voice Repeaters 2V44, 4V44	No Data available; Likely inadequate circuit design failure thresholds and inadequate isolation from penetrators
	Equalizers & Pads LC-1	" "
	Echo Suppressors GTE 931	" "
	2/4 Wire Line Adapters	No data available; Likely inadequate isolation from penetrators
	Supervisory/ Signaling GTE 927	" "

Table 2.1 (continued)

LEASED UNMANNED STATION VULNERABILITY

Fuction	Equipment Type & Name	Vulnerability Reasons
Transmitting/Receiving Radio Repeaters	TD-2, TD-3, TH, TJ, TL/TM	See Leased Manned Station Vulnerability Chart
Cable Repeaters L1, L3, L4, L5	L4, Basic Repeaters	Immune To Damage
	L4, Regulating Repeaters	Immune To Damage
	L4, Equalizing Repeaters	Susceptible to upsets from EMP, Power, or Lightning Transients due to Improper Wire Routing and Terminal/Shielding.
	L1, L3, L5	No Data
Signal Conditioning	Loading Coils	Limited Data, Likely to be Immune to Damage
	Build Out Capacitors	Limited Data, Likely to be Immune to Damage
	Voice Repeaters	See Leased Manned Station Vulnerability Chart

Table 2.2

LEASED USER TERMINATION SYSTEMS

FUNCTION	EQUIPMENT NAME & TYPE	VULNERABILITY REASONS
Subscriber Switching	PABX & PBX	No data
Signal/Supervisory Processing	Teletype	No data - likely immune to damage
	Touch Tone Telephone	Requires additional penetration isolation high probability of immunity in most installations
	Data Sets	Limited data, likely inadequate circuit design upset thresholds
	Voice Repeaters Equalizers, Pads Line Adapters	See Leased manned vulnerability chart
Transmission Systems	T-carrier N, O, K carrier	See Leased manned vulnerability chart

Table 2.3

GOVERNMENT OWNED MANNED STATION VULNERABILITY

FUNCTION	EQUIPMENT TYPE & NAME	VULNERABILITY REASONS
Transmitting/Receiving	Digital Transmitters & Receivers	Limited data suggests inadequate isolation frcm penetrators
Multiplexer	Analog Transmitters/Receivers	No data - Probably similiar to leased manned stations
	Digital Multiplexer	Limited data suggests inadequate isolation frcm penetrators
	Analog Multiplexer	Limited data suggests inadequate isolation from penetrators
Coaxial Cable	-	No Data
Message Switching Systems	AUTODIN I	Inadequate isolation from penetrators, Improper wire routing/termination/shielding to prevent upset
	AUTODIN II	Inadequate isolation from penetrators, Improper wire routing/termination/shielding to prevent upset
Circuit Switching	AECo	Inadequate isolation from penetrators, Inadequate circuit design upset thresholds for EMP transients
	4W5	No data possible, inadequate isolation from penetrators

Table 2.4

GOVERNMENT OWNED MANNED STATION VULNERABILITIES

FUNCTION	EQUIPMENT TYPE & NAME	VULNERABILITY REASONS
Signal/Supervisory Processing	No data	Functional identity to leased station suggests same reasons
Technical Control	Emergency Action Centers	Available data suggests inadequate isolation from penetrators

Table 2.4 (continued)

GOVERNMENT OWNED - UNMANNED REPEATER STATION VULNERABILITIES

FUNCTION	EQUIPMENT TYPE & NAME	VULNERABILITY REASONS
Transmitting/Receiving Radio Repeaters	Digital Radio	No Data
Cable Repeaters		No Data
Signal Conditioning	Voice Repeaters Loading Coils Build out Capacitors	No Data

Table 2.5

GOVERNMENT OWNED USER TERMINATION STATION VULNERABILITIES

FUNCTION	EQUIPMENT TYPE	VULNERABILITY REASONS
Transmission Systems	Satellite Terminals	Inadequate Circuit Design Damage Thresholds and Inadequate Isolation from Penetrators
Subscriber Switching	PABX, PBX	No Data
Signal/Supervisory Processing		No Data - See Leased User Termination Station Vulnerability Chart

Table 2.6

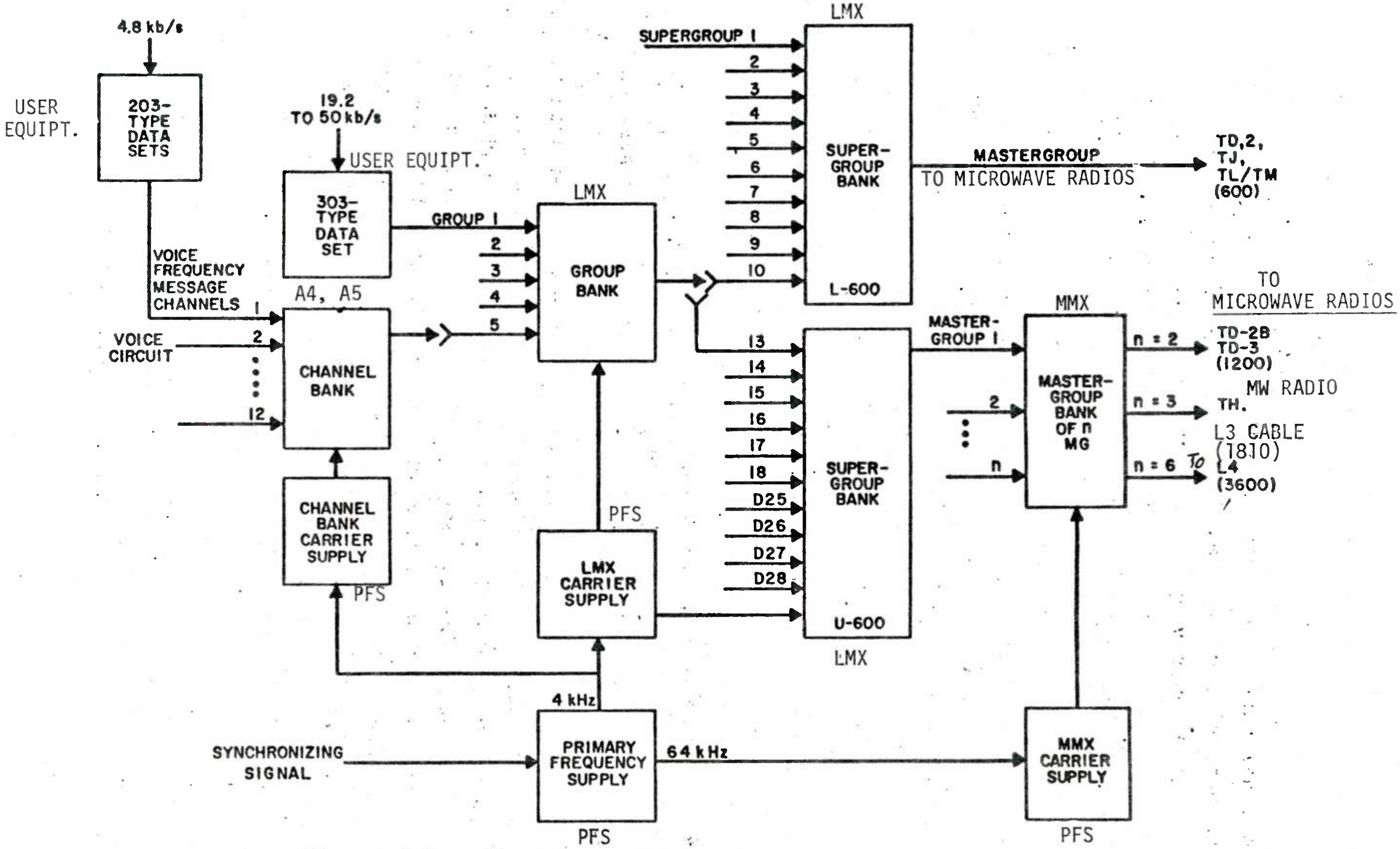


Figure 2.7. Structure of Long Haul Multiplex Equipment

Primary Frequency Supplies (PFS)

This equipment provides the carriers used to combine/insert each voice channel into a specific part of the frequency bandwidth. Damage could prevent communication in groups of either 12, 60, 600, 1200, 1800 or 3600 channels depending on what portion was affected. (See Figure 2.7.) Upset or malfunction temporarily shifts the various channels out of their respective frequency slots causing voice interruptions or data drop outs.

EMP tests were conducted on three PFS equipments; an early electromechanical design, (PFS-1), a solid state design (PFS-2A) and an updated version of this latter unit (PFS-2B) which had improved EMP upset immunity.

The test results indicated that the PFS-2A and PFS-2B were upset by EMP currents below 2.0 Ap-p for the former and less than 20 Ap-p for the latter. These failures place the PFS in upset categories 2 and 3. The vulnerability causes therefore are due to inadequate circuit design upset thresholds and improper cable routing/shielding or shield terminations as discussed in Section 2.0. The PFS-1 unit was electromechanical and was not upset. These units were not tested at the maximum likely EMP current transients. Assuming damage thresholds are a factor of 10 higher than upset thresholds, the circuits that upset would probably be damaged at the maximum levels. In that case damage rule 1 applies. Insufficient penetration isolation is targeted as the cause.

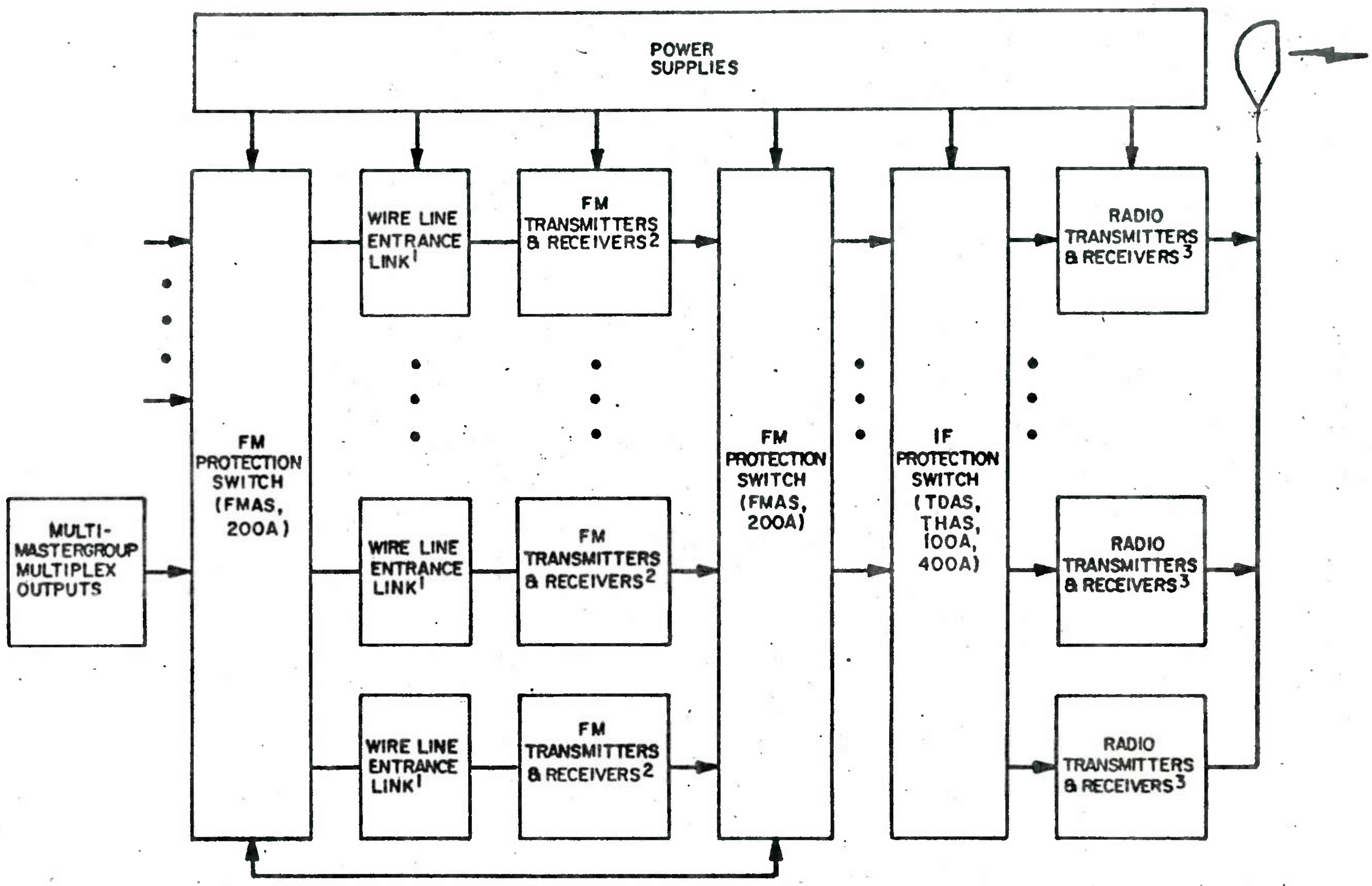
Channel Banks

The multiplex equipments combine 12 voice/data channels into a single group for input to the next multiplex stage which will accept 5 of the 12 channel groups. In very large manned stations as many as 300 of these equipments could be installed. Each equipment is connected to pairs of signal line cables that exit the facility with each pair usually protected by lightning arrestors.

Two versions were EMP tested, a vacuum tube type (A4) and a transisorized type (A5). The A4 unit was tested at low stress levels (5 Ap-p) and no vulnerabilities were uncovered. The A5 unit was tested at 80 Ap-p with the same result. This latter test current value is less than the required 130 Ap-p so conditionally it is probably immune to damage. However, by definition it will be damaged due to inadequate isolation from penetrators (damage rule 1).

Groups Multiplex Equipment

The LMX equipment combines ten groups of 60 voice/data channels each into a single group of 600 channels occupying a specified frequency bandwidth, i.e., 600 channels of 4 KHz separated from each other in frequency such that the total bandwidth is about 2400 KHz. In the largest stations, at least 6 of these equipments could be used. Damage to any given unit would lose from 60 to 600 voice/data circuits while upset causes only temporary interruptions that are self correcting.



NOTES:

1. CAN BE A J68833 TUBE TYPE WLEL FOR SINGLE MASTERGROUP RADIO OR A 3A WLEL FOR MULTIMASTERGROUP RADIO (3B FOR TH-1).
2. CAN BE A J68336 FM TRANSMITTER (OR RECEIVER) FOR SINGLE MASTERGROUP RADIO, A 3A FMT (OR FMR) FOR TWO MASTERGROUPS, OR A 4A FMT (OR FMR) FOR THREE-MASTERGROUP SYSTEMS (3B FOR TH-1).
3. CAN BE TD-2, TD-3, TH-1, OR TH-3.

Figure 2.8. Long Haul Microwave Radio Systems

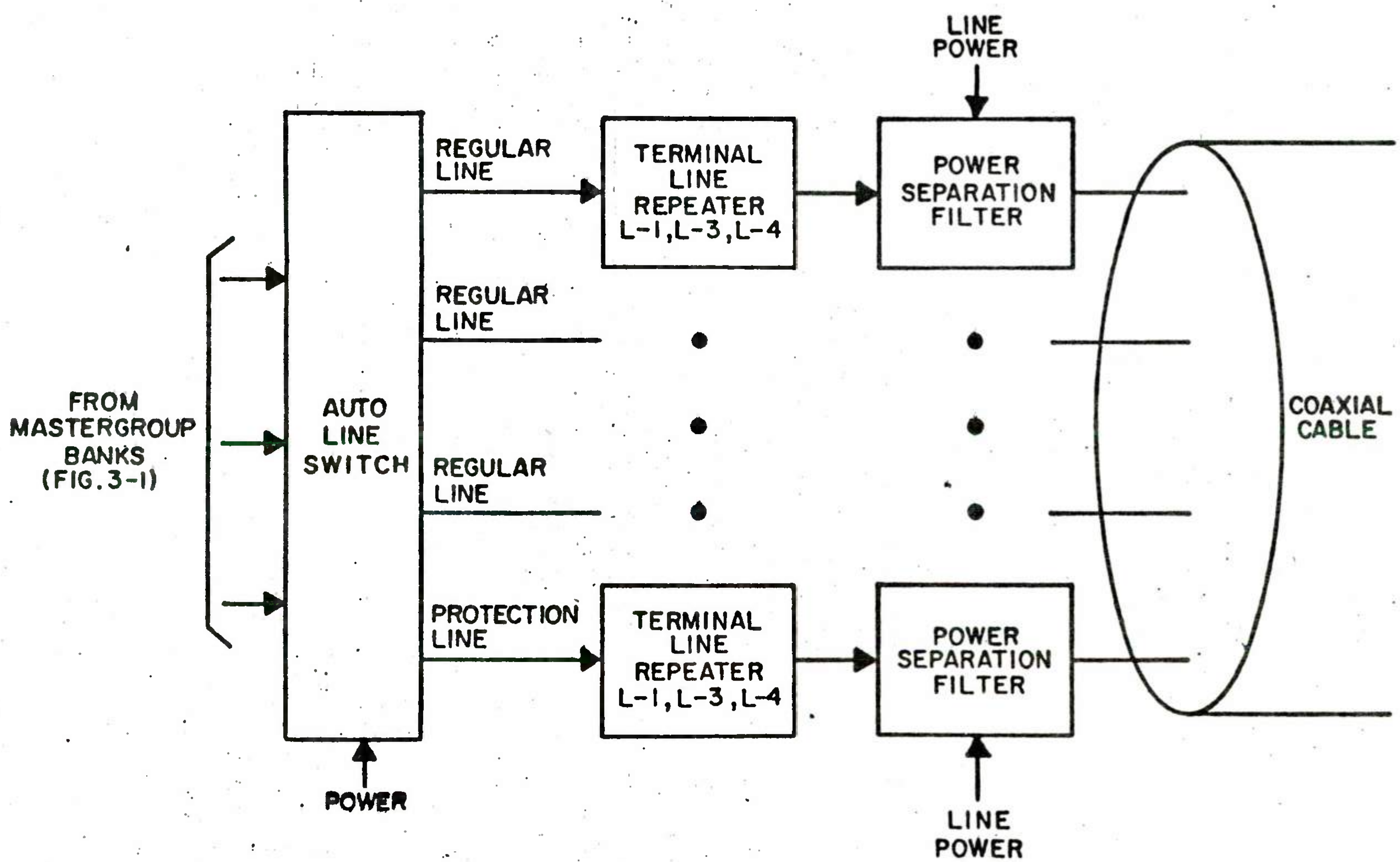


Figure 2.9. Coaxial Cable Systems (Transmitting Terminal)

Both vacuum tube (LMX-1), and transistor versions (LMX-2) were EMP tested. The LMX-1 was tested at 1 Ap-p, and the LMX-2 at 35 Ap-p, both without any indication of vulnerability. By definition, however, damage rule 1 applies as the units have inadequate isolation from penetrators.

Master and Multimaster Groups

This equipment performs the final combination of the channels into groups of 600 to 3600 for transmission over the cable or microwave radio systems.

Two types were tested, a vacuum tube version (MMX-1) and a transistor version (MMX-2). The MMX-1 was tested at 2 Ap-p and the MMX-2 at 50 Ap-p with no indication of vulnerability. Therefore damage rule 1 applies.

2.1.1.2 Transmitting/Receiving Equipment

Figure 2.8 illustrates a typical microwave transmitting/receiving station, and the functional interconnections among its various equipment elements. Table 2.1 is a list of the equipment, and a tabulation of the reasons for vulnerability. These equipment types and their industrial counterparts are the work horses of the terrestrial communication network.

Microwave Transmitters and Receivers

The five types of RF transmitters/receivers tested were the TD2B, TD3, TH3, TM-1 and TL-2. The TD2B, TD3 and TH3 were tested at 30 Ap-p, 50 Ap-p and 60 Ap-p respectively without any indication of vulnerability. Damage rule 1 therefore applies, and inadequate isolation from penetrations is expected.

The TM-1 was tested at 25 Ap-p and the TL-2 at 4 Ap-p. The former equipment experienced a failure at this test level, which indicates inadequate isolation from the penetrators (damage rule 1). The experimenters attributed failure to penetrator coupling. This lends credibility to the damage categories that have been adopted.

It should be noted that these equipments are installed in small shelters, and thus are more apt to experience the maximum likelihood currents.

FM Transmitters/Receivers

These equipments convert the output signal of the wire line entrance links to an FM intermediate signal (IF) for processing by the microwave transmitters and receivers (see Figure 2.8).

Three types were tested, the J68336 (Vacuum Tube), the 3A, and 4A (Transistorized/Solid State). The J68336 was tested at 3.0 Ap-p while the 3A and 4A were tested at 35 Ap-p. The 4A unit experienced arc-over from a metal cased component to ground during one test series at currents of 20 Ap-p or about 2000 volts. This is consistent since arc-over usually can occur with physical spacing of about .100 inch. This data also validates the vulnerability categorization being used for this report, and indicates that the isolation of penetrations is essential to prevent arc-over and possible burn thru of wire insulation, blowing of fuses (arc-over from fuse to fuse holder cases), and connector pin to pin insulation destruction (carbon traces).

These three units therefore fall into damage category area 1, and do not have adequate isolation from penetrators.

Wire Line Entrance Links (WLEL)

These equipments provide an interface between the multiplex equipment and the radio equipment that compensates for transmission losses on long interconnecting cables.

Two units were tested, the J68833 (Vacuum Tube) and the 3A (Solid State) at 1.0 Ap-p and 35 Ap-p respectively with no damage vulnerability indicated. Damage rule 1 applies and inadequate penetration isolation exists.

FM and IF Protection Switches

The FM protection switch protects the WLEL and FM transmitters/receivers by switching in spare channels when failures occur. The IF switches protect the RF transmission channels by switching in spares when failures or excessive path fading occurs.

Two FM switches were tested, the FMAS and the 200A, at 5 Ap-p and 35 Ap-p respectively, without indications of vulnerability. Damage category rule 1 applies, and these switches require penetration isolation.

Two IF switches were tested, the TDAS (Vacuum Tube) and the 100A (Transistorized/Solid State) at 5 Ap-p and 100 Ap-p respectively. The TDAS, like all vacuum tube units in this report fall into damage category 1. Damage rule 2 has not been applied since experience indicates that vacuum tube designs are normally immune to EMP currents below 20 Ap-p.

The 100A switch falls into damage category 1, inadequate isolation from penetrations. Additionally, this unit was upset at test levels of 1.0 Ap-p causing the switch to falsely connect an unused channel. Upset category 3 applies and indicates an inadequate circuit design upset failure threshold. Additionally, it is reasonable that upset would occur for power line transients. The experimenters added capacitors to remove this vulnerability up to 100 Ap-p. It is suspected that damage would have occurred at less than 20 Ap-p test currents using the upset-damage relationship described earlier. (It is not known if a damage test without capacitors was performed.)

Recent test data on a new version of a similar switch shows no vulnerability at test currents greater than 20 Ap-p. Damage rule 1, inadequate penetration isolation applies.

FDM/Analog Channels for Coaxial Cable

The four long haul cable systems, L1, L3, L4, L5 are widely used within the United States. Figure 2.9 shows the typical main station equipment, their functional relationship and connection to the multiplex equipment. Table 2.1 lists the vulnerability reasons.

Only the L4 equipment was tested. Test currents of 110 Ap-p showed no damage vulnerability for the equalizer repeater, protection switches, or repeater power source. Coaxial cable test currents were 1500 Ap-p. The repeater upset threshold occurred at 8 Ap-p. This equipment is considered immune from EMP based on the combination of cable drive test currents of 1500 Ap-p and 110 Ap-p test currents for the equipment. Additionally, the equipment and repeaters are installed below ground level, which reduces the maximum likely current to less than 130 Ap-p.

The repeater upset requires upset rule 2 to be applied and indicates that the equipment has poor cable routing within its container or improper shield terminations. One would expect that lightning transients might also cause this upset problem.

Digital Channels, Time Division Multiplexing (TDM)

Digital communication links are being widely used for short haul cable systems. The most common is the T-1 carrier and its associated multiplexers. Later generations of this basic combination are now available.

Only limited test data is available. The tests currents were not listed, but the usual currents for the test apparatus employed are about 15 to 20 Ap-p or more. Two damage failures were recorded for semiconductors. Engineering judgment dictates that the equipment requires improved isolation from design. Damage categories 1 and 2 apply.

2.1.2 Unmanned Station Equipment Vulnerabilities

Unmanned leased stations are usually small in size, and of varying construction techniques. In this report an unmanned station has been loosely defined as one that serves a repeater or gain equalizer function. Typical repeaters include voice amplication units, cable repeaters for gain regulation and equalizing, line or wire pair loading coils and microwave transmitting/receiving radio repeaters. Figure 2.2 lists these kinds and types of equipment. Table 2.2 also lists the vulnerability reasons associated with Figure 2.2. All equipment listed in Table 2.2 have been discussed previously (see Table 2.1) except for the loading coils and build out capacitors. Unmanned stations do not have a special vulnerability category of reasons except that their small size makes it mandatory to have adequate isolation between penetrations and equipment. Practical considerations therefore tend to indicate that these buildings or containers be shielded to simplify the diversion of EMP penetration currents.

2.1.2.1 Transmitting/Receiving Radio Repeaters

See Table 2.2 and the discussion in section 2.1.1.2.

2.1.2.2 Cable Repeaters.

See Table 2.2 and the discussion in section 2.1.1.2.

2.1.2.3 Signal Conditioning Equipment

This category includes loading coils and build out capacitors that are used to frequency compensate cable wire pairs. Their vulnerabilities are entirely dependent on EMP penetration currents and the voltage produced by these currents. EMP data is not available but since the components are passive, i.e., inductors and capacitors, the probability of EMP damage exists for component terminals due to arc-over and possible burn through of insulation. These are the same effects that would be caused by lightning strokes which normally have far more energy that EMP. Engineering judgment indicates that these components are immune to EMP currents unless they are near the end of their useful life or have been hit by a large number of previous lightning strokes.

Loading Coils and Build-Out Capacitors

HEMP immunity for these components is expected and is given additional credence due to the requirements for these components to pass specifications, like the Rural Electrification Administration, (RE-30) for capacitors and RE-26 for loading coils.

For example, each capacitor must be capable of withstanding surges of two and one-half times the rated voltage with a rise time of the surge to half crest voltage of 4 us and a decay time to half creast of 100 us. Additionally, they must be capable of withstanding a potential of 20,000 Vdc for not less than 3.0 seconds. Loading coils must be capable of withstanding a dielectric strength test of 8kVdc minimum for not less that 0.5 seconds between it windings and dielectric strength test of 20 kVdc for not less than 0.5 seconds plus a minimum of 10 kVdc dielectric strength between its winding. An EMP test, however, would require a rise time, energy, and source impedance specification to assure immunity.

2.1.3 Unmanned User Termination Equipment Vulnerabilities

This category has a few special equipment items not normally needed for unmanned repeater stations, such as telephones, data sets and private branch exchanges (PBXs), both automatic and manually switched to subscribers within a particular complex. This category has an additional uniqueness since the cabling between equipments, shielding for penetration cables and buildings/ rooms are not constructed or designed for protection against transients or interference from radio, radar, power and lightning. (For example, California sites may not have lightning arrestors.) This fact is not unusual or unexpected since voice equipment and power equipment are low cost items and expendable. Installation in many cases is in buildings that have little penetration isolation or shielding simply due to cost considerations.

HEMP transients affect wide geographical areas, however, and the high volume of telephones, say 100 million in use might be affected as a total group. Repairs of 10 or 20 million telephones, or 500,000 data sets at user locations could be crippling to important government services and create an untenable position. This group category was singled out for this important reason.

Little HEMP data is available for the known equipment at user sites. Sample survey's have verified that the penetrators in most buildings are installed without isolation. Therefore, all user locations must be considered as having vulnerability for that cause. See Figure 2.3 and Table 2.3 for equipment types (generic only), and a listing of suspected vulnerability reasons.

2.1.3.1 Signal/Supervisory Processing Equipment

Telephones - Touch Tone/Dial. HEMP data is available for a touch tone telephone and shows that a solid state component failure occurs at the test levels expected from EMP penetration currents above 20 Ap-p. This failure did not affect telephone operation due to the nature of the failure. Category 1 damage rule applies.

Dial Telephones. No data.

Data Sets. Available data indicates upset thresholds are below 2.0 Ap-p. Damage rule 1 and upset rule 3 therefore apply. Also, the upset threshold circuit design capability is inadequate.

2.1.3.2 Subscriber Switching Equipment

This group includes PBX, PABX, and special call processing equipment for holding, transferring calls, and ringing third parties, etc. No HEMP or equipment data is available. The range of vulnerability reasons is not expected to be different from those tabulated in Figure 2.1 and Table 2.1.

Table 2.3 and Figure 2.3 list these probable equipments and vulnerability reasons for completeness. If additional data becomes available, it will be added.

2.1.3.3 Transmitting/Receiving Equipment

This category might include subscriber microwave or cable systems purchased from industrial sources. At the present time, no data is available.

2.2 Government Owned Communication Systems

These systems have been categorized into the same groupings as the common carrier leased systems described in section 2.1. Figures 2.4, 2.5, 2.6 list the data while Tables 2.4, 2.5, and 2.6 list the vulnerability reasons in the same format as before.

HEMP or equipment data is not available as can be seen from the tables and figures for either type of unmanned station. It appears rational to assume that the vulnerabilities are not different from the leased categories. Very little data is available on manned stations, but several unique systems have been carefully studied. These include a Message Switched System, several Satellite Earth Terminals, and a digital microwave radio system.

2.2.1 Manned Station Equipment Vulnerabilities

2.2.1.1 Switching System Equipment. Switching systems fall into two classes, circuit switches and message/record switches. The former class is represented by types, AECo and 4W5 which connect specific users to each other using separate and exclusive wire pairs/radio channels. The latter class represented by AUTODIN has users that receive a message/record in digital form, store it, extract its messages, and forwards the remaining or same message to the next user terminal.

Message Switching System. Several types of switches and switch equipment elements have been EMP tested, and represent three generations of equipment evolution. An early generation equipment test indicated that EMP upsets were produced at levels corresponding to 2.0 to 20 Ap-p with random semiconductor damage occurring at higher levels that correspond to penetration current values. These failures were attributed to long unshielded cable lengths attached to the damaged components. These test results indicate that damage rules 1, 2, and upset rule 2 apply.

A second generation equipment test indicated only upset at levels that correspond to current levels above 20 Ap-p. No damage was reported but test currents were below the most likely maximums and damage rule 1 applies.

A third generation equipment has been tested, but final data is not available. Preliminary indicators are that damage rule 1 applies.

2.2.1.2 Transmitting/Receiving Equipment. Only two systems of transmitting and receiving equipment have been studied for EMP effects. Satellite terminals of three types were studied, and two types were tested. The second system studied was the digital microwave transmitter/receiver/multiplexer system.

Satellite Terminals. The satellite terminal data indicated that unshielded and poorly terminated shields on cables leading from antenna drive motor electronics were the primary reasons for vulnerability. Other causes were inadequate damage threshold circuit designs for components connected to signal lines and power lines. HEMP failure levels were not recorded in sufficient detail to assign specific categories, but the reasons provided justify assigning damage categories 1 and 2 plus upset category 2.

Digital Microwave Equipment. HEMP surveys and reviews were performed on this type of equipment but no tests were performed. The analysis of this equipment and its facilities indicate adequate damage thresholds up to 20 Ap-p due to extensive inter-rack shielding but inadequate penetration isolation is indicated based on the technique used for grounding and shielding of the penetrators. Damage rule 1 applies to this equipment for this reason.

2.2.1.3. Multiplex Equipment. No data available.

2.2.1.4 Signal/Supervisory Processing Equipment. No data is available but the information and equipment types of section 2.1.1 are expected to apply. The reader should refer to Table 2.1 and Figure 2.1.

2.2.1.5 Technical Control Equipment. Some survey data on equipment location, cable arrangements and configurations is available. This data indicates potential vulnerability above 20 Ap-p caused by inadequate penetration isolation (damage rule 1). In general, technical control equipment consists of patch bays, jacks, meters, and a few pieces of special test equipment. Damage is only likely for the special test equipment or in some cases system status alarms. In some cases damage rule 2 may apply also.

2.2.2 Unmanned Station Equipment Vulnerabilities. No data is available. See section 2.1.2, Table 2.2 and Figure 2.2 since this sections' vulnerability reasons, are expected to apply to this category.

2.2.3 Unmanned User Termination Equipment Vulnerabilities. No available data, see section 2.1.3, Table 2.3 and Figure 2.3 since this section's vulnerability reasons are expected to apply to this category.

3.0 Power Equipment Vulnerability

Power equipment may be divided into the three categories DC power, AC power, and Power-Conversion. The first category includes batteries, DC - DC converters, and regulators. The second, AC - AC converters/transformers, generators and regulators. The last category includes AC/DC or DC/AC converters and battery chargers.

In communication facilities much of the equipment is powered from batteries continually charged by battery chargers operating from the commercial AC power. Usually a standby generator is available to ensure service during periods of commercial power loss. The DC Power is then converted/regulated/filtered as required for equipment operation.

The vulnerability rationale is that DC power and AC standby power will experience the EMP currents and energies directly coupled to the AC power lines and cables. These currents are very large, 20K Ap-p and produce voltages that exceed a megavolt.

DC power equipment HEMP vulnerability data is available for a wide range of equipment. See Table 3.1.

AC/DC Conversion. A rectifier operating above 100 volts DC failed at 60 Ap-p which is below the maximum likely EMP current of 130 Ap-p. A circuit design change to add a terminal protection device protected the circuit to over 200 Ap-p. A second rectifier operating at 24vdc failed at 40 Ap-p. After repair it survived to 300 Ap-p. The conclusion is that these fixes adequately isolated the rectifiers from penetrator effects. Damage rule 1 applies.

DC/DC Conversion. A DC-DC converter EMP failure at 10 Ap-p was fixed to a level of over 600 Ap-p using special filter capacitors. This units failure requires a damage rule 1 and 2 categorization.

Battery Chargers. EMP data indicates rectifier diode failures above 130 Ap-p. Direct isolation from penetrators is required. Damage rule 1 applies.

VULNERABILITIES OF POWER EQUIPMENT

FUNCTION	EQUIPMENT TYPE	VULNERABILITY REASONS
Rectifiers & Converters	24 Volts 130 Volts 250 Volts	Inadequate circuit design damage thresholds & inadequate isolation from penetrators
Battery Chargers	Various	
Fuse	-	Inadequate isolation from penetrators causing arc-overs & subsequent fuse failure
Standby Equipment	-	Inadequate isolation from penetrators
Power Controls	-	Inadequate isolation from penetrators and inadequate circuit design upset thresholds for EMP Lightning and power transients.

Table 3.1

Transformers, Circuit Breakers. No failure data. Most units are theoretically immune.

Fuses. A limited amount of data is available. This data suggests that some fuse holders are susceptible to arc-over at currents less that 130 Ap-p. This arc-over can cause the fuse to blow and remove equipment from service. This suggests that damage rule 1 applies.

4.0 Vulnerability Commonality and Differences

The vulnerability causes cited in this report were (1) inadequate isolation from penetrations, (2) inadequate circuit design thresholds, and (3) improper shielding of cables, ineffective cable shield terminations, improper routing or inadequate separation of cables from each other. Table 5.1 summarizes the causes of telecommunication vulnerabilities and their frequency of occurance in past experiments and studies.

These vulnerability groupings appear to be independent of whether the stations are manned or unmanned, leased or government owned. Essentially the differences are too small to permit a clear distinction between groupings. The differences appear to depend only on the design attention given to preventing the causes listed above.

5.0 Conclusions/Recommendations

Three primary causes of vulnerability were distinguished in this study. Each cause is related to design attributes that are easily controlled in the engineering sense. Standards and specifications to control these attributes should be developed. The available vulnerability data however, is deficient in several important respects. The two most critical are the failure to test equipment at the maximum most likely EMP currents coupled by facility building penetrators. The second is the absence of a correlation between EMP currents and the energy failure threshold of components that includes source impedances and rise time effects.

The initial effort in a standards program, therefore must include this correlation and define the degree of protection required and obtainable in a practical way for the vulnerability causes cited. This improved correlation and specification has been performed on an analytical basis and is included below in Tables 5.1 through 5.5 for each category. These tables include the missing parameters from available EMP data and are a reasonable engineering starting point for a standard program. The categories listed in these tables are recommended for this initial effort. The major elements of the categories are illustrated in Figure 5.1.

VULNERABILITY REASON/CAUSE	FREQUENCY OF OCCURRENCE
Inadequate Isolation from Penetrators	29
Inadequate Shielding, Wire Routing	4
Inadequate Circuit Design Thresholds	7
Immune	3

VULNERABILITY CAUSE FREQUENCY OF OCCURRANCE
Table 4.1

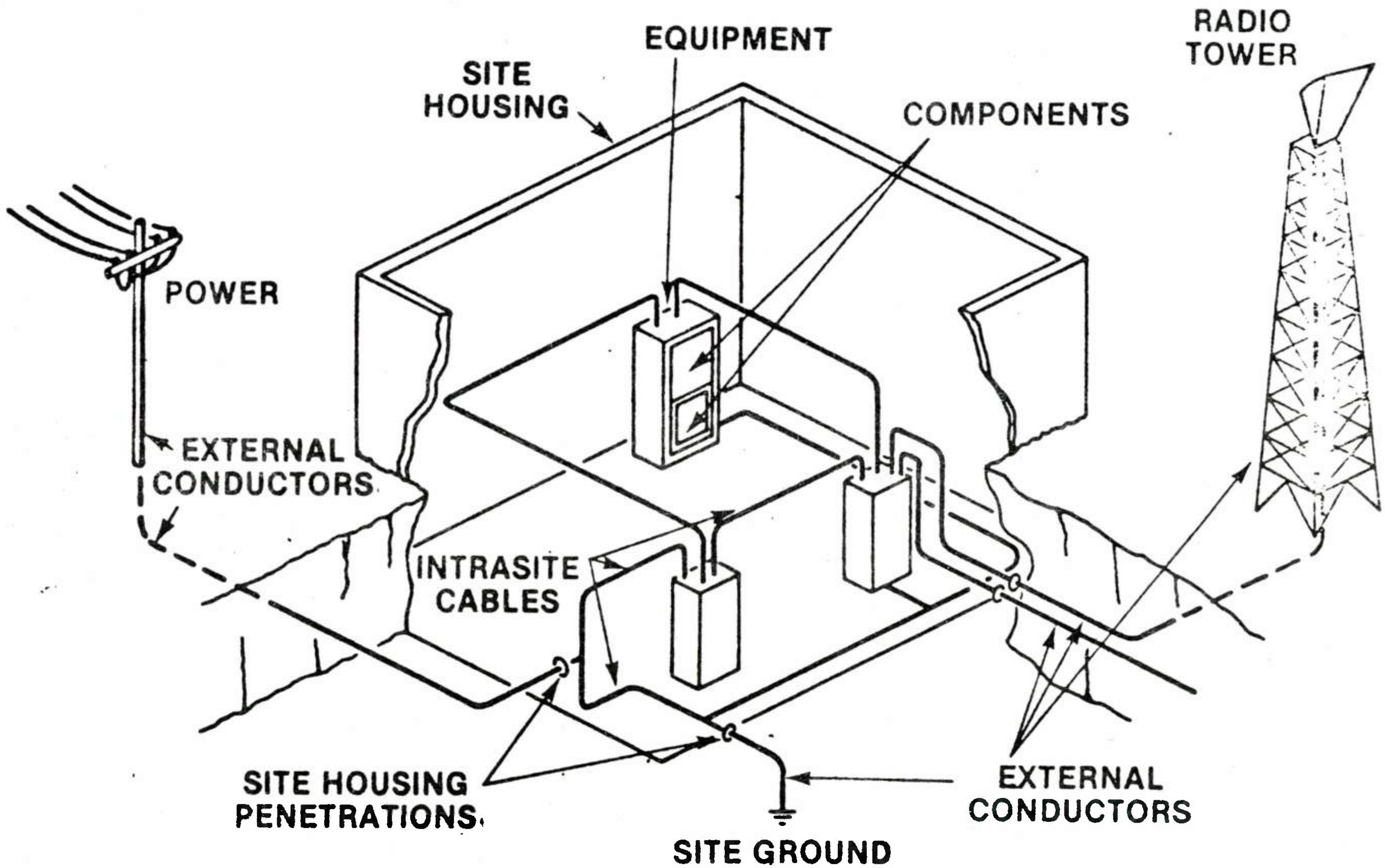


Figure 5-1. Typical Telecommunications Facility

TABLE 5-1. SPECIFICATIONS FOR COMPONENTS

PIE	AMPLITUDE	IMPEDANCE (OHMS)	RATE OF RISE	BANDWIDTH (MHZ)	WAVE-SHAPE	COMMENTS
AC POWER	1 KV	100	10 V/NS	1--15	MDS	FO = 1, 2.5, 5, 10, 15 MHZ; $1/\alpha$ = 6 μS (AC power through control cables)
DC POWER	1 KV	100	10 V/NS	1--15	MDS	
SIGNAL CABLES	1 KV	100	10 V/NS	1--15	MDS	
CONTROL CABLES	1 KV	100	10 V/NS	1--15	MDS	
ANTENNA	1 KV	100	100 V/NS	.01--100	XX	
GROUNDING	400 V	20	5 V/NS	.1--10	XX	
STRUC DFFUSD FLD	1.6 KV/M	100	160V/M/NS	1--10	MDS	FO = 1 MHZ, 10 MHZ; $\alpha = 10^6$ (struc diffusd fld and apertures)
APERTURES	1.6 KV/M	100	160V/M/NS	1--10	MDS	

XX = DOUBLE EXPONENTIAL
DS = DAMPED SINUSOID
MDS = MULTIPLE DAMPED SINUSOID

TABLE 5-2. SPECIFICATIONS FOR EQUIPMENT

POE	AMPLITUDE	IMPEDANCE (OHMS)	RATE OF RISE	BANDWIDTH (MHZ)	WAVE-SHAPE	COMMENTS
AC POWER	10 KV	100	100 V/NS	1--15	MDS	
DC POWER	10 KV	100	100 V/NS	1--15	MDS	F0 = 1, 2.5, 5, 10, 15 MHZ
SIGNAL CABLES	10 KV	100	100 V/NS	1--15	MDS	$1/\alpha = 6\ \mu S$
CONTROL CABLES	10 KV	100	100 V/NS	1--15	MDS	
ANTENNA	100 KV	300	20 KV/NS	.01--100	XX	
GROUNDING	2 KV	20	20 V/NS	.1--10	XX	
STRUC DFFUSD FLD	50 KV/M	377	10 KV/M/NS	.1--100	MDS	F0 = 1 MHZ, 10 MHZ
APERTURES	50 KV/M	377	10 KV/M/NS	.1--100	MDS	$\alpha = 10^6$

XX = DOUBLE EXPONENTIAL
DS = DAMPED SINUSOID
MDS = MULTIPLE DAMPED SINUSOID

TABLE 5-3. SPECIFICATIONS FOR INTRASITE (IN-PLANT)

POE	AMPLITUDE	IMPEDANCE (OHMS)	RATE OF RISE	BANDWIDTH (MHZ)	WAVE-SHAPE	COMMENTS
AC POWER	100 KV	100	1 KV/NS	.1--10	XX	
DC POWER	100 KV	100	1 KV/NS	.1--10	XX	
SIGNAL CABLES	50 KV	100	1 KV/NS	1--10	DS	F0 = 3 MHZ, $\alpha = 10^6$
CONTROL CABLES	50 KV	100	1 KV/NS	1--10	DS	F0 = 3 MHZ, $\alpha = 10^6$
WAVEGUIDE	20 KV	20	1 KV/NS	1--10	DS	F0 = 3 MHZ, $\alpha = 10^6$
ANTENNA	.7 MV	300	30 KV/NS	.01--100	XX	
WATER	1 KV	20	10 V/NS	.01--10	XX	
SEWAGE	1 KV	20	10 V/NS	.01--10	XX	
FUEL	1 KV	20	10 V/NS	.01--10	XX	
AIR CONDITIONING	1 KV	20	10 V/NS	.01--10	XX	
GROUNDING	20 KV	20	1 KV/NS	.01--10	XX	
STRUC DEFUSE FLD	50 KV/M	377	10 KV/M/NS	.1--100	XX	
STRUC CONDUCTED	1 KV	20	100 V/NS	1--10	DS	F0 = 3 MHZ, $\alpha = 10^6$
APERTURES	50 KV/M	377	10 KV/M/NS	.1--100	XX	

XX = DOUBLE EXPONENTIAL
DS = DAMPED SINUSOID
MDS = MULTIPLE DAMPED SINUSOID

TABLE 5-4. SPECIFICATIONS FOR SITE HOUSING

PIPE	AMPLITUDE	IMPEDANCE (OHMS)	RATE OF RISE	BANDWIDTH (MHZ)	WAVE-SHAPE	COMMENTS
AC POWER	100 KV	100	1 KV/NS	.1--10	XX	
DC POWER	100 KV	100	1 KV/NS	.1--10	XX	
SIGNAL CABLES	50 KV	100	1 KV/NS	1--10	DS	F0 = 3 MHZ, $\alpha = 10^6$
CONTROL CABLES	50 KV	100	1 KV/NS	1--10	DS	F0 = 3 MHZ, $\alpha = 10^6$
WAVEGUIDE	20 KV	20	1 KV/NS	1--10	DS	F0 = 3 MHZ, $\alpha = 10^6$
ANTENNA	.7 MV	300	30 KV/NS	.01--100	XX	
WATER	1 KV	20	10 V/NS	.01--10	XX	
SEWAGE	1 KV	20	10 V/NS	.01--10	XX	
FUEL	1 KV	20	10 V/NS	.01--10	XX	
AIR CONDITIONING	1 KV	20	10 V/NS	.01--10	XX	
GROUNDING	20 KV	20	1 KV/NS	.01--10	XX	
STRUC DIFFUSD FLD 0	50 KV/M	377	10KV/M/NS	.1--100	XX	
STRUC CONDUCTED	1 KV	20	100 V/NS	1--10	DS	F0 = 3 MHZ, $\alpha = 10^6$
APERTURES	50 KV/M	377	10KV/M/NS	.1--100	XX	

XX = DOUBLE EXPONENTIAL
DS = DAMPED SINUSOID
MDS = MULTIPLE DAMPED SINUSOID

TABLE 5-5. SPECIFICATIONS FOR PLANT EXTERIOR

POE	AMPLITUDE	IMPEDANCE (OHMS)	RATE OF RISE	BANDWIDTH (MHZ)	WAVE-SHAPE	COMMENTS
AC POWER	10 MV	500	.5 MV/NS	.01--50	XX	
DC POWER	2 MV	300	.1 MV/NS	.01--50	XX	
SIGNAL CABLES	.7 MV	300	30 KV/NS	.01--50	XX	
CONTROL CABLES	.7 MV	300	30 KV/NS	.01--50	XX	
WAVEGUIDE	.5 MV	100	20 KV/NS	.1--100	XX	
ANTENNA	.7 MV	300	30 KV/NS	.01--100	XX	
WATER	10 KV	20	.2 KV/NS	.01--10	XX	
SEWAGE	10 KV	20	.2 KV/NS	.01--10	XX	
FUEL	10 KV	20	.2 KV/NS	.01--10	XX	
AIR CONDITIONING	10 KV	20	.2 KV/NS	.01--10	XX	
GROUNDING	200 KV	20	20 KV/NS	.01--50	XX	
STRUC DFFUSD FLD	50 KV/M	377	10KV/M/NS	.1--100	XX	
STRUC CONDUCTED	10 KV	20	.2 KV/NS	.01--10	XX	
APERTURES	50 KV/M	377	10KV/M/NS	.1--100	XX	

XX = DOUBLE EXPONENTIAL
DS = DAMPED SINUSOID
MDS = MULTIPLE DAMPED SINUSOID

BIBLIOGRAPHY

1. Final Report, Effects of EMP on Bell System Long Haul Transmission Facilities, April 1974, Bell Laboratories, Contract DAHC60-70-C-0071 (Unclassified).

2. Final Report, Safeguard Communications Agency EMP Effects Analysis and Test Program (U), MITRE Corp., M74-220, August 1974 (Secret).

3. DCPA Report TR 61, "EMP Threat and Protective Measures", August 1970.

4. DCPA Report TR 61A, "EMP Protection for Emergency Operating Centers", July 1972.

5. DCPA Report TR 61B, "EMP Protective Systems", July 1976.

6. DCPA Report TR 61C, "EMP Protection for AM Radio Broadcast Stations", July 1976.

7. DCPA Report 61D, "EMP and Electric Power Systems", July 1973.