Research and Development Technical Report
CECOM-TR-01-4

SYSTEM SAFETY LESSONS LEARNED HANDBOOK

Steven Chan
DIRECTORATE FOR SAFETY

JUNE 2001

CECOM
U.S. ARMY COMMUNICATIONS-ELECTRONICS COMMAND
DIRECTORATE FOR SAFETY ATTN: AMSEL-SF-SEP
FORT MONMOUTH, NEW JERSEY 07703-5024
email: amsel-sf@mail1.monmouth.army.mil

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position, unless so designated by other authorized documents.

The citation of trade names and names of manufacturers in this report is not to be construed as official Government endorsement or approval of commercial products or services referenced herein.

Destruction Notice

Destroy this report when it is no longer needed. For classified documents, follow the procedures in DoD 5200.22M, Industrial Security Manual, Section II-19, or DoD 5200.1-R, Information Security Program Regulation, Chapter IX. For unclassified documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 2001	Technical Report

4. TITLE AND SUBTITLE

SYSTEM SAFETY LESSONS LEARNED HANDBOOK

5. FUNDING NUMBERS

6. AUTHOR(S)

Steven Chan

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

US Army Communications-Electronics Command (CECOM)
Directorate for Safety
ATTN: AMSEL-SF-SEP
Fort Monmouth, NJ 07703-5024

8. PERFORMING ORGANIZATION REPORT NUMBER

CECOM-TR-01-4

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution authorized to U.S. Government Agencies and their contractors; Administrative or Operational Use; June 2001. Other requests for this document shall be referred to U.S. Army CECOM, Directorate for Safety, ATTN: AMSEL-SF-SEP, Fort Monmouth, NJ 07703-5024.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The purpose of this Handbook is to provide information in assisting Program Managers, Project Leaders and equipment designers in developing/providing safe equipment/systems to field users. The contents in the Handbook were collected from learned experiences by system safety engineers, reported equipment incidents, and current regulations/requirements. The major topics discussed in the Handbook are Shelterized Systems, Power Sources, Vehicular Trailer Applications, Antennas, Night Vision Devices and Software Safety. Safety issues and recommendations are discussed in each major topic. It is our hope that by learning the lessons in this Handbook, potential safety issues can be eliminated or minimized to an acceptable level prior to fielding equipment/systems to our soldiers.

14. SUBJECT TERMS

System safety; lessons learned; shelters; electric power; whip antennas; antenna masts; antennas; vehicles; night vision devices; software safety; software engineering

15. NUMBER OF PAGES

41

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18 298-102

USAPPC V1.00

TABLE OF CONTENTS

LIST OF FIGURES

APPENDIXES
(See FOREWORD, paragraph 6.)

APPENDIX A

SYSTEM SAFETY ENGINEERING TECHNICAL BULLETINS

Bulletin #1: Wiring for Proper Safety Grounding

Bulletin #3: Neutral Bus Isolation from Equipment Ground; ECU Grounding

Bulletin #4: Removal and Installation of Batteries

Bulletin #5: Leakage Current Testing

Bulletin #6: Critical Power Problems from Computer and Electronic Loads

Bulletin #7: Battery Compartment Design Guidelines for Equipment Using Lithium-Sulfur Dioxide Batteries, Rev. A

TECHNICAL REPORTS

CECOM-TR-93-1: Lightning Protection System Design, Applications for Tactical Communications Systems

CECOM-TR-94-10: Identification, Integration and Tracking of Software System Safety Requirements

CECOM-TR-95-3: Safety Guidelines for the Design, Operation, Test and Maintenance of Communications-Electronics Systems Operated On-The-Move

CECOM-TR-98-6: Earth Grounding and Bonding Pamphlet

CECOM-TR-00-1: A Guide to Pollution Prevention in the Acquisition of Commodities

Safety Guidelines for the Design of Vehicular Mounted Communications-Electronics Systems Using On-Board Power

APPENDIX B System Safety Design Verification Checklist

System Safety Design Verification Checklist Handbook

APPENDIX C System Safety Specification for Equipment Development

FOREWORD

1. The following six chapters contain system safety information that Program Managers, Project Leaders, and equipment designers should find helpful in providing safe equipment/systems to field users. The information includes general guidance from "LESSONS LEARNED" from safety issues that have surfaced over the years.

2. Detailed safety engineering information on specific topics (in the form of Technical Bulletins and Technical Reports) are included in Appendix A.

3. A Design Verification Checklist (SEL Form 1183), which covers generic safety concerns, is provided in Appendix B. The Checklist is a synopsis of the more important safety considerations that should be addressed during developmental stages, during Non-Developmental Item (NDI) procurement, and during hardware inspections.

4. Appendix C contains an unabridged System Safety Specification for a developmental materiel acquisition contract. This specification references the requirements for commercial electronic equipment to help assure that your equipment/system is safe to operate and maintain during its total life cycle. As a standard course of action, we have added requirements to this specification which reflect design needs established from "lessons learned" as a result of test incidents, hardware inspections, and field experiences. In this sense, what you are now reading is a "living document," which is tailored for each system being procured.

5. The readers/users of this handbook are reminded that an effective and well-managed System Safety Program (both contractor and government) will do much to assure your system design will provide our soldiers with safe equipment. It is our hope that this information will prove to be helpful to all involved in reducing safety risks. Further information may be obtained by contacting the CECOM Directorate for Safety DSN 992-0084, commercial (732)532-0084, or e-mail: amsel-sf@mail1.monmouth.army.mil.

6. Appendixes A, B, and C are not included in hardcopies of this handbook. They are provided in the CD format. Please contact the above for obtaining the appendixes.

CHAPTER 1

SHELTERIZED SYSTEMS

1-1. Physical Layout/General Design Considerations. The layout of equipment within the shelter needs to be carefully planned to allow for operational and maintenance efficiency while also providing for safety. Regardless of what is used as the basic enclosure, the following general safety considerations must be addressed:

a. Ingress/Egress - The entrance/exit door area needs to be clear of all impediments to allow for rapid and unobstructed movement of personnel. The incorporation of two exits should be considered in shelter design. All aisles must allow for reasonable mobility. For raised shelters, external platforms adjacent to entrance/exit doors should be of a non-skid design or have non-skid surfaces. This is especially true of truck tailgates, which may be lowered and utilized as part of the entrance/exit path. Boarding ladders, where used, are often at a steep angle and do not provide protection from falls. It is suggested that designers look at their particular system and determine if a ladder/handrail combination is needed. One such ladder is known to exist in the inventory under NSN 2540-00-854-4445. It is 72" X 20", has non-slip steps, and has one handrail. An alternative item having similar dimensions is NSN 2540-01-205-0071. If the shelter is installed on a different type of prime mover (e.g., a 5-ton truck instead of a 2½-ton truck), then a boarding ladder with sufficient height from the ground should be used to avoid accidents. Accidents have occurred in the past where personnel were injured by falling off boarding ladders that were too steep. In some instances, sandbags or other objects were used to make up the height. Please note that a ladder (NSN: 2540-01-432-9930) with adjustable legs has been designed for users switching from 2½-ton trucks to 5-ton trucks.

b. Center of Gravity/Lateral Stability - The equipment installed in the shelter must be properly located to evenly load all corners of the shelter. Problems have resulted in the past because of uneven weight distribution, excessive total weight, and a center of gravity that caused the system to be laterally unstable. Logically, the heavier components should be placed nearer to the floor. Equipment should be distributed throughout the shelter to equalize (to the extent possible) the overall load. In the past, overweight shelters have created roadability problems and can affect safety from the viewpoint that the structure/vehicle may be overstressed perhaps leading to structural fatigue/failure and possible accidents. Loading ancillary equipment (such as "camo" nets, crew bags, water, etc.) internally or externally onto shelter is a normal practice in the field. Said field loading could pose stability problems for the vehicle if the weight distribution is uneven or the gross vehicle weight is exceeded. Specific load plans should be developed for the shelter/vehicle and addressed in the TM. The center of gravity, lateral stability, and system weight must be addressed as part of the verification testing process.

c. Transportability/Roadability - As an adjunct to the previous topic, the shelter must be configured so that it can be loaded on transport vehicles, including aircraft where specified, without having to remove too many components to assure a fit or to eliminate

protrusion hazards extending into the path of transportation. Perhaps more importantly is the roadability of the vehicle and system. We have experienced problems in this area involving speed restrictions due to: insufficient maximum speed testing, non-existent roadability tests, improperly rated vehicle tires, poor system designs resulting in overweight conditions, weight imbalances, and centers of gravity that are too high. As with the previous topics, roadability needs to be addressed as early as possible and should be verified by actual testing. Making analogies to similar systems or making estimates are often insufficient due to differences between the actual system and the system used for comparison.

d. Personnel Environment - Heating, cooling, and ventilation may be provided by an Environmental Control Unit (ECU). The ECU needs to have an intake of fresh/clean air, or the shelter needs to have a separate fresh air intake. Contaminated air, such as from generators, prime movers, or other sources, must not be allowed to be drawn in by the ECU or fresh air intakes. This is an obvious, but often overlooked safety concern. For systems needing supplemental heating, electrical heaters (as opposed to the older multi-fuel heaters) are preferable from a safety viewpoint. Additionally, in accordance with DOD and DA policy, the use of Chlorofluorocarbon(CFC) refrigerants in ECUs is restricted.

e. Fire Suppression - Fire extinguishers should be mounted adjacent to the exit door(s) to allow for possible fire fighting without having to walk through the shelter itself. For high cost, mission critical equipment automatic fire suppression systems are highly recommended. Halon systems are now being replaced (along with CFCs) with non-ozone depleting substances. The available alternatives to Halon include carbon dioxide (CO_2) or dry chemical extinguishers. The health and safety effects on the operator when CO_2 fire extinguishers are used in shelters was tested by the US Army Aberdeen Test Center. Based upon the test and the risk assessments made by the US Army Center for Health Promotion and Preventive Medicine (USACHPPM), CO_2 fire extinguishers may be utilized for extinguishing fires in shelters. However, operators must be warned to exit the shelter and fight any fire from the outside. In addition, operators are to be instructed to ventilate the shelter after discharge of the CO_2 fire extinguishers and prior to operator re-entry into the shelter.

f. Noise – The total noise within the shelter must be addressed from both an operational impact and from a safety viewpoint. This should include all equipment under the most active operational scenario to include any reasonably expected externally generated noises (such as generators, etc.). We have seen systems requiring the addition of considerable noise reduction barriers/insulation to reduce the overall noise exposure to an acceptable level. Refer to MIL-STD-1474 for guidance.

g. Lighting - Most shelters have lights installed in the ceilings. These lights, unless they are somehow recessed, require “bump” guards to protect personnel from sharp edges, thermal hazards (bulbs get hot), and the possible breakage of the bulb itself.

Consideration should also be given to providing emergency lighting and/or exit signs in large shelters/vans/semi-trailers, etc., where exits may be farther away.

h. Mechanical Hazards - Sharp edges and corners are some of the most common mechanical hazards. Other mechanical hazards have also resulted in injuries. For example:

- The hinged power/signal entry panel covers on the outside of the shelter may become an eye level bump hazard.
- Wire may become pinched or damaged by improper placement.
- A catch/release mechanism mounted on top of a heavy full length console door can become a personnel entrapment hazard. The door, when opened into an aisle way and locked into position, could possibly trap an individual from reaching the exit, especially if the individual is alone and not tall enough to reach the catch mechanism.
- Other mechanical hazards noted in the past were:
  - drawers that did not have slide out stops and shelves or hardware that protruded too far into aisle ways;
  - large holes in tailgates have, in the past, allowed a human foot to pass through and could cause a severe injury; and
  - some equipment catch mechanisms were so poorly designed and difficult to operate that they created pinch/skinned knuckle injuries. (One must always be aware of potential "pinch" points, and moving parts/mechanisms that could be hazardous; these hazards should be designed out or suitable mechanical guards used.)

i. Shelter Roof Tops - In addition to the concern of bump hazards created by improperly extended signal entrance panel covers and other protruding items, systems requiring access to the shelter roof top will usually trigger concern due to requirements for adequate ladders for climbing to the roof. To enhance personnel safety, a non-skid surface should be applied to the roof and a railing or post and chain/rope mechanism should be employed to preclude operators from falling off the roof. Furthermore, if transmitting antennas are mounted on or near the roof, interlocks should be provided to override the controls inside the shelter. This will preclude unintentional transmission of hazardous RF energy while personnel are on or near the roof area of the shelter or vehicle. The interlocks should also prevent any antenna movement, which might hit an operator while on the roof.

j. Individual Equipment/Components - These units will require proper mounting devices. Where rack mounted with slide-out mechanisms they must have limit stops to preclude the accidental dropping of the item. Furthermore, where units are over the weight of the single person lift limit, adequate lifting provisions (handles, etc.) must be provided. Single person lift limits for equipment are as follows:

Handling Function	Weight(lbs)
Equipment lifted less than five feet above the floor.	37
Equipment lifted less than three feet above the floor	44
Equipment designed to be carried 33 feet or less.	42

Equipment exceeding single person lift limits shall be labeled with the total weight and with the required number of handlers. The values are doubled for two person lift limits (uniformly distributed equipment) with 75% added thereafter per person (see MIL-STD-1472).

Where more than a one-person lift is required, a sufficient number of handles must be provided to allow each lifter a proper handhold. Sometimes larger handles will have to be provided to accommodate a MOPP IV gear requirement. All too often we have seen very heavy equipment that has the required lift caution label prescribing a several person lift but has an inadequate number of handles or its handles in locations which result in awkward lift postures by personnel. Very heavy items (those requiring more than a two-person lift) might be better lifted by mechanical means, such as a davit or hoist. The heaviest items should be placed as low as possible in equipment racks to provide minimal lifting heights. Too often very heavy items are placed in hard to reach locations. Designers need to thoroughly consider these concerns and make adequate provisions for personnel safety during the removal and reinstallation of equipment/components.

1-2. Grounding of Shelters.

(NOTE: See Appendix A, CECOM TR-98-6, Earth Grounding and Bonding Pamphlet for instructions on earth grounding.)

a. A ground rod or equally effective earth grounding system is required for shelters. The system is connected via braided wire straps or another conductor to the ground stud located within or adjacent to the shelter power entry panel. We have had few problems with the grounding systems for shelters. One complaint that continually comes to us is that ground rods are difficult to drive into some soils - and even more difficult to remove. CECOM has developed a Surface Wire Ground System (SWGS) (see Figure 1) which minimizes this problem and provides an equal or better interface with the earth than does the conventional ground rod. The SWGS is an alternative grounding system, which has been designed primarily for use with systems requiring high mobility/quick installation and tear-down operational scenarios. It is more easily installed and removed and offers a reasonable option in situations where driving/retracting conventional ground rods would be difficult and/or too time consuming. It is not intended to replace the familiar ground rod or to be used as a permanent type facility grounding system. It should be considered as another option for use as situations/circumstances may warrant.

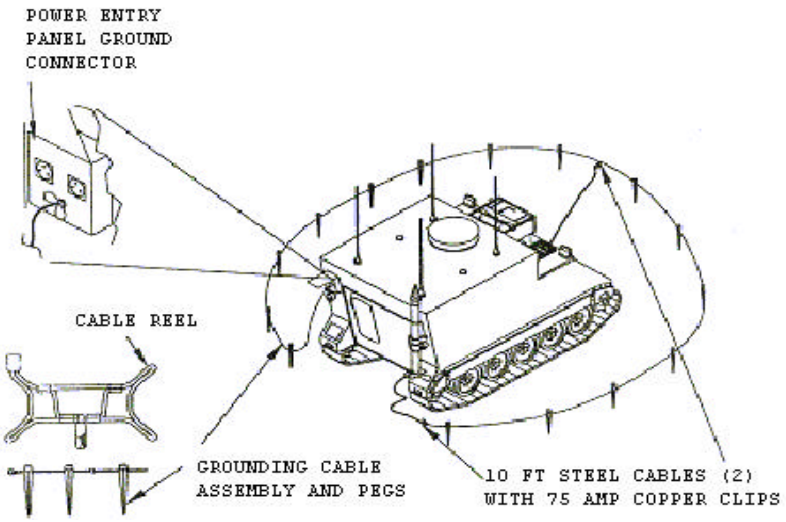

Figure 1. Surface Wire Ground System

As with any grounding system, the SWGS provides a preferred lightning discharge path, enhances safety, and controls noise in signal circuits. The total resistance of the SWGS to ground is equal to or less than that of a single ground rod. When properly installed, the SWGS may better survive a lightning strike than would the common ground rod configuration. Its ability to better survive a lightning strike is based, in part, on the multiple discharge paths created when the system is correctly installed; that is around the periphery of the object being protected and with the three required connections. Voltage step potentials created by any lightning strikes may, however, make the soil near the SWGS somewhat more hazardous than the soil surrounding a single ground rod since the SWGS does not penetrate as deeply into the earth. This phenomenon would be of very short duration, similar to the strike itself.

Regardless of which grounding system is used, the soil in the immediate vicinity of the SWGS or ground rod will be potentially dangerous during a lightning discharge. For this reason, personnel should make every effort to seek shelter within metal enclosures, vehicles, or other relatively safe locations when electrical storms are imminent. This same precaution applies even if a grounding system is not installed, since personnel may also become possible targets for a direct strike.

With all of the above in mind, the following precautions are essential to help assure safe use of the SWGS:

(1) Maintenance - The SWGS requires proper inspection before each installation (ensure no frayed cables, bent or damaged stakes, etc.) and should be periodically re-inspected to assure that proper connections and soil contact are maintained. Follow the

instructions provided with the SWGS, make sure the stakes/wires are firmly in contact with the soil and that all connections are tight. Minimize all vehicular and personnel traffic adjacent to the SWGS.

(2) Operations - Assure that personnel find appropriate shelter during electrical storms. If personnel must be outside (i.e., during a real combat scenario) they will reduce their risk if they stay away (at least 6 feet) from any part of the SWGS. However, the danger of their being struck directly would still exist.

b. To help assure that shelterized systems are safe from a grounding standpoint, the following design requirements must be followed to ensure personnel protection from "fault currents" as well as high voltages/currents created by EMP and/or indirect/direct lightning strikes:

(1) An Equipment Grounding Conductor (EGC), which is a green wire, must be included in all AC circuits. The EGC must be connected to the wire terminations (plugs, etc.) in such a manner as to assure that it ultimately connects to the shelter ground (the wing nut where the ground rod attaches) and that it provides a low impedance path for all fault currents that may reasonably occur. This will provide for personnel protection and will cause the controlling unit breaker to trip under fault conditions. See Appendix A, Technical Bulletin #1, for instructions regarding safe methods of connecting and grounding the EGC in equipment shelters.

(2) All outer metallic equipment covers must be bonded to each other as well as to the shelter ground via the EGCs, bonding straps, other mechanical means, etc., to assure that all external surfaces are at the same (ground) potential.

(3) Neutral and Ground must not be connected together within the shelter. They must be isolated from each other (and within the power panel). The only place they will be tied together will be at the generator or at the transformer secondary (if commercial power is being utilized). This provides for the single-point grounding required for safety as well as EMI/TEMPEST, etc. See Appendix A, Technical Bulletins #1 and #3; and NEC, Article 250 for further details.

(4) For systems using on-board power, the neutral and EGC should be tied together with a jumper as close as possible to the generating source. For systems using multiple power sources (e.g., on-board generator and external commercial power, etc.), the system design must isolate different power source ground-neutral bonding points to avoid potential problems. Refer to Appendix A, "Safety Guidelines for the Design of Vehicular Mounted Communications-Electronics Systems Using On-Board Power" for additional information.

(5) Lightning Protection - Ground rods provide a preferred lightning discharge path. It should prove to be adequate to conduct excessive currents, which might travel over long "land lines" connected to your system. These are protected by surge arrestor

devices in your power and signal entrance panels. You are cautioned, however, to be aware that a direct lightning strike may cause unpredictable consequences. The optimum lightning protection system for direct hits involves an array of air terminals overhead to provide a cone of protection for your shelter. However, if personnel stay inside the shelter that is properly connected by a ground rod driven fully into the ground, personnel should be safe (although probably very scared and temporarily deafened if a direct or nearby strike occurs). Personnel must also stay clear of ground rods in such instances since step potentials created near them can be fatal.

(6) Bonding co-located shelters/generators - Shelters co-located within 8 feet of each other must be bonded together using a ground strap to ensure both shelters are at the same electrical potential in the event of a fault in one of the shelters. This will prevent personnel who may be in contact with both shelters at the time of the fault from receiving an electrical shock. The shelters must also be earth-grounded. There are numerous ways in which two or more co-located shelters can be earth-grounded. The most convenient method, as shown in Figure 2, is to install the SWGS around one of the shelters and then install a bonding strap (6 AWG braided ground strap) between the ground points of each co-located shelter at the power entry panel. Two or more shelters can also be grounded with a common ground rod, similar to the generators shown in Figure 3.

(7) Generator Grounding – A ground rod is usually provided with each generator and must be used for earth- grounding the generator separately from earth-grounding the shelter (see Figures 2 and 3). Generators co-located within 8 feet apart must be bonded together and earth-grounded. The bond can be made by utilizing a ground strap between both generators grounding points or by connecting both generators to a single, common ground rod, as shown in Figure 3.

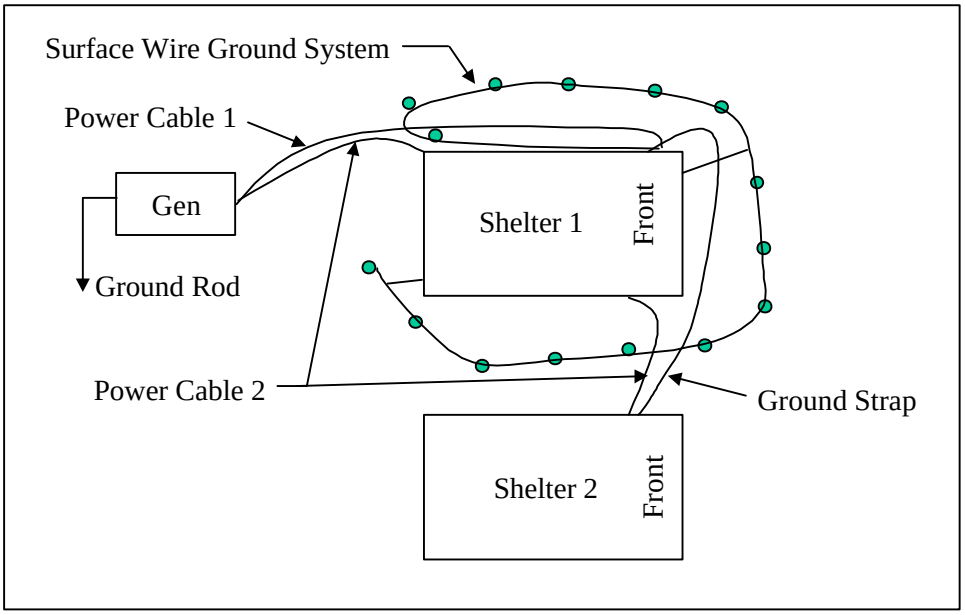

Figure 2. Grounding Co-located Shelters

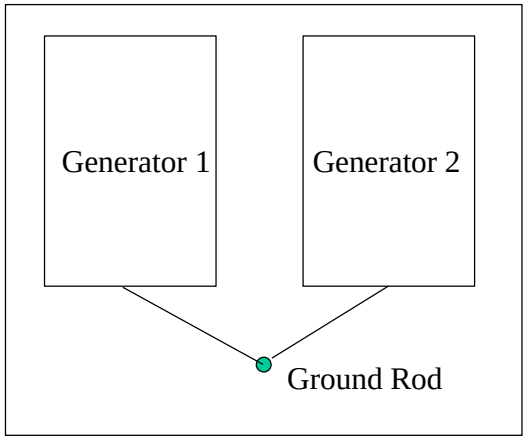

Figure 3. Grounding Co-located Generators

1-3. Electrical Design.

(NOTE: Shelter wiring and power distribution must be in compliance with applicable NEC requirements.)

a. Alternating Current (AC) Power

(1) Shelters usually have their AC power entry panels adjacent to the entrance doors. Immediately behind these panels and inside the shelter are EMI/RFI filters, and perhaps surge arrestors, followed by a power distribution panel or cabinet. The location of the power control panel immediately inside the shelter is not only economically desirable but also provides for safety since the main on-off switch can be more easily reached to shut off power during an emergency. This is especially true if a person farther into the shelter is in trouble. Although not often seen, an emergency switch, or "dead-fall" button, at the other end of the shelter would further enhance safety if power had to be turned off quickly. If an Uninterrupted Power Supply (UPS) is used, it does not have to be turned off by the main power breaker. However, the equipment that remains energized should be limited (segregate the power lines as much as possible, etc.). Additionally, power-down instructions and warnings must address this situation.

(2) Power panels, and especially power cabinets, need to be accessed from time to time and, where voltage barriers are impractical, it is suggested that interlocks be installed as an alternative to help protect the maintainer from accidental contact with high voltage.

(3) Branch circuits need to be protected by individual circuit breakers and the wiring must have mechanical protection via conduit and/or wire-mold type metal channels. Again, ground wires in the form of Equipment Grounding Conductors (EGC) – "green

wires" are required in every circuit and shall be terminated in the same manner as other conductors. Good workmanship and neat, proper dressing of wiring will go far in eliminating hazards and will facilitate maintenance. Proper color coding practices must be followed. AC supply conductors shall be color-coded black and white for line and neutral conductors, respectively. Black, red, and blue shall be used to identify three phase line conductors. The color coding reduces the probability that wire connections will be improperly made (possibly resulting in energized enclosures).

(4) Convenience outlets need to be chosen to preclude applying improper power to given equipment. Furthermore, plugs attached to equipment power cables must be matched to mate only with the appropriate voltage outlet configuration. External convenience outlets mounted on the outside of shelters must incorporate Ground Fault Circuit Interrupters (GFCI) to reduce hazards associated with powering externally used portable/remote tools, equipment, etc. For those instances, if equipment having excessive leakage currents (as described in section 1-3c(4) of this chapter) must be powered, dedicated outlets with special connectors should be utilized.

(5) Overvoltage Protection - Provisions should be made to incorporate overvoltage protection, and protection from improper application of power (applying incorrect voltages) to a system should also be provided. Equipment damages and fires have resulted in the field by improper application of power or improper wiring to the power source.

b. Direct Current (DC) Power - Sources of DC power, often 28 VDC, can be obtained from a prime mover or by housing batteries within the shelter itself. Our experience has shown that the following design provisions are essential in providing safe battery operation where DC battery power is obtained within a shelter (typically from lead-acid battery sources):

(1) Batteries need to be approved for each particular application IAW AMCR 700-83 by AMC Battery Management Office, ATTN: AMSEL-LC-P, Fort Monmouth, NJ, 07703. This requirement applies to all types of batteries/battery chemistries.

(2) The battery compartment should be made of a non-conductive materiel or utilize insulation, particularly for the top of the compartment.

(3) Forced positive ventilation to the outside of the shelter (and away from sources of ignition) is essential. Sensors and/or alarm systems are required to assure that the ventilation fan is working and that the vent door is open. An interlock might be used to shut off the charging circuit as an additional precaution and a more positive means of safe operation when ventilation is not present due to fan failure and/or vent door closing. An incident occurred due to loss of ventilation for the two vented lead acid batteries in an MSE shelter. In that case personnel inadvertently left the shelter battery vent hose disconnected after performing maintenance. The hydrogen produced during charging of

the batteries accumulated in the shelter and exploded by a spark from an electric heater. The accident could not have occurred if an alarm system had been provided.

(4) Where batteries will be recharged by a battery charging system built into the shelter, overcharging protection is required. If there is an option to use external power, provisions are required to prevent overcharging of the prime power batteries.

(5) Power disconnect in the form of a DC on/off switch and overcurrent protection in case of short circuits are required.

(6) DC supply conductors shall be color coded red and black for plus and minus polarity, respectively.

(7) See Appendix A, Technical Bulletin #4, for instructions regarding the safe removal and installation of batteries.

c. Electrical Hazards

(1) Operators/maintainers must be protected from electrical hazards IAW industry best practices as detailed in the NEC, 29 CFR 1910, and UL standards. Operators/maintainers need to be protected from voltages greater than 30V. Generally speaking, transparent dielectric protective covers must be placed over the hazardous electrical terminals and caution labels are also necessary to prevent unintentional contact. Holes drilled into the protective barriers that are just large enough to allow test probes to pass through will facilitate testing without necessitating the removal of the barriers, which often are not replaced. For voltages over 600V, separate enclosures with non-bypassable interlocks are required.

(2) High voltage circuits and capacitors within equipment may retain electrical charges after power is removed and can result in shock hazards. Automatic discharge devices and/or bleeder resistors are required to assure that all high voltage circuits drop to less than 30 volts and 20 joules of energy within two seconds after power is removed.

(3) Test points on high voltage equipment/circuits must never require measuring more than 300 volts AC or DC. Potential (voltage) dividers may be utilized in the circuitry to step down higher voltages and allow this limitation to be observed. (Thus, a 250 volt reading might correspond to the presence of 750 volts.) In one reported incident, an individual was electrocuted during the testing of a high voltage circuit. Although proper procedures were not being followed in this instance, if the test points had been voltage-limited, perhaps the consequences might have been less severe.

(4) EMI/RFI Filters - These devices are usually located just behind the point of power entry to a piece of equipment and/or a shelter. They are used to assure that undesirable frequencies are allowed to neither enter nor exit equipment. By design, and by operational mode, the undesirable frequencies are passed by the filters to the Equipment

Grounding Conductor (EGC) circuitry. This can result in excessive leakage currents being imposed on the EGC. Excessive currents are currents greater than five milliamperes, which are generally considered to be the maximum electrical current to which a person can be safely exposed (at a higher frequency, leakage current is measured in Measurement Indication Unit (MIU), and five MIUs are the limit). A two-fold safety problem exists where excessive filter leakage currents are present: (1) Ground Fault Circuit Interrupters (GFCI) (if used) will continually trip rendering the equipment inoperative, and (2) an open circuit condition in the ground circuit can produce a shock hazard by causing the outer metallic enclosure of the equipment to become energized. If low leakage current filters cannot be utilized, then redundant ground circuits can reduce the risk to an acceptable level. GFCIs can also be replaced with outlets having special connectors dedicated to powering only those pieces of equipment having excessive leakage current. Leakage current measurements IAW ANSI C101.1-1992 must be made to determine if excessive leakage current exists and if fixes are required. A qualitative test for the existence of leakage current is to plug the equipment into a GFCI equipped outlet. If the GFCI doesn't trip, then an unsafe leakage current level is not present. (See Appendix A, Technical Bulletin #5, for further information on testing Army C-E systems.)

Since filters may retain electrical charge, discharging devices may also be required.

CHAPTER 2

POWER

2-1. Power Sources. In this chapter the three principal power sources will be discussed; that is, mobile AC generators, commercially generated AC, and battery sources. These sources are the most commonly accessed and provide electrical energy to operate equipment/systems. Equipment designers can do much to reduce the inherent safety hazards associated with electrical power, regardless of where it is applied, by considering the following when developing equipment/system architectures:

a. Voltage Levels - Although some circuitry requires high voltage levels, where possible, low voltage levels should be utilized since, among other attributes, it reduces safety risks substantially. Use of modern day electronic components and Large Scale Integrated (LSI) circuits have helped to reduce size, weight, heat generation, and power requirements/levels. Safety has been enhanced as a result.

b. Power Supplies - These sources may be contained within individual equipment and get their primary input power using a 120 VAC power cord. These supplies may be designed in such a manner as to be modular and easily removed for troubleshooting, servicing, etc. Where feasible, the design should allow for Built In Test (BIT) and/or require only simple continuity measurements for maintenance and troubleshooting.

2-2. Mobile Electric Power (MEP).

a. The Army inventory includes several engine-generator sets and Tactical Quiet Generator (TQG) systems which provide for various types of alternating current (single phase, multi-phase) and power (kW) capabilities. To provide for the safety requirements of single-point grounding (tying of neutral and ground at only one location) for land-based equipment/systems, the neutral terminal of the generator must be connected to the generator frame with a jumper wire of at least a #6 AWG copper wire. On some of the more modern generators, an internal connection may already exist to provide this single tie point. This connection should only be eliminated if a floating (ungrounded) system is required and approved by the servicing safety organization. See Appendix A, Technical Bulletin #1, on wiring for safe grounding and Technical Report TR-98-6 for instructions on earth grounding.

b. The most frequent safety problems reported to us regarding the use of MEP are use of improper power to energize equipment/systems and/or improper connection of the power stub pigtails to the generator lugs. To help reduce these problems, designers, technical manual writers, and user trainers should be aware of the contents of Technical Bulletin 43-0125 "Installation of Communication-Electronics Equipment: Hookup of Electrical Cables to Mobile Generator Sets on Fielded Equipment To Meet Electrical Safety Standards." That manual contains detailed instructions on proper wire hook-up,

cable wire color coding, various generator models and system applications, etc. See Appendix A, Technical Bulletin #1, for more information.

c. Where more than one generator is utilized, a power distribution box having controls to allow for proper electrical application (phase and voltage level) is essential. Obviously, visual and preferably automatic means must be provided to reduce power interruptions and applications of incorrectly phased electricity, etc. Furthermore, power distribution boxes can be designed to allow for inputs from two or more generators as well as from commercially provided sources. Whatever the source of input to the distribution box, it must be remembered that all unused output connection ports may be energized and will require separate shut-offs and covers to preclude accidental contact with energized contacts. A sample power distribution box showing one possible way of allowing for generator or commercial hook-up is shown in Figure 3 of Technical Bulletin #1, Appendix A. Section 2-3 in this chapter provides further information on this type of hook-up.

d. A noise level study should be conducted to determine the noise level produced from generator sets. Usually, hearing protection is required when working near the generator set while it is running. (Hearing protection is required if the noise level exceeds 85 dBA.)

e. Refueling of generator sets while they are running should be avoided to prevent personnel from touching the hot engine surfaces and possibly starting generator fires. The generator exhaust must be pointed away from personnel and shelters. Obstructive objects must be kept away from air intakes and exhausts of generator sets. When personnel are working near air intake, and any rotating parts of generator sets, caution must be exercised and should be addressed in TMs to prevent potential injury. B/C type fire extinguishers should be mounted nearby generator sets to allow the suppression of possible generator fires.

f. When working near the generator set battery, the negative battery cable must be disconnected prior to servicing. In one instance, a fire was inadvertently started when an operator, working near the battery, accidentally shorted the positive terminal of battery to ground (negative vehicle ground) with a wrench.

2-3. **Commercial AC Power** - Commercial power for mobile land-based systems may be provided via a "pole drop" connected to residential electrical lines. The three most important safety considerations for utilizing such power sources are:

a. When hooking up to a pole drop, make sure source power is off (preferably have power company or skilled linemen do the initial connections).

b. Make sure power (phases, voltages, current availability, etc.) is compatible with your equipment/system requirements and that wiring is properly connected.

c. The single ground tie point in commercial pole drop situations will require tying the neutral to the ground at the pole drop (similar to that performed at a construction site where there is a temporary meter and circuit breaker box mounted on an 8-10 foot pole), or it may be tied through connections made at a power distribution box. Again, Figure 3 of Technical Bulletin #1 in Appendix A shows one way of accomplishing this connection. Note, however, that a breaker which disconnects or opens both hot and neutral of the incoming commercial power would be required if the power distribution box is used as the tie point. This feature is necessary since we must keep the motor generator wiring neutral separated from the ground within the power distribution box since it is already tied together at the generator. Additionally, make sure the circuit breakers chosen are adequate to protect the system being connected.

2-4. Battery Power.

a. Battery power is often preferable, or may be the only practical means, for providing electrical energy to portable equipment. Batteries may also be utilized as backup power sources. Whatever battery configuration or type is being considered as part of the design process, AMC Regulation 700-83 requires that battery assignment approval be obtained from the AMC Battery Management Office, ATTN: AMSEL-LC-P, Fort Monmouth, NJ, 07703. This approval process is intended to minimize the proliferation of battery types and also assures that the battery power and current producing requirements are well within the capability of the battery selected. The latter will, of course, enhance safety.

b. Normally, a battery is contained in a box or enclosure. This battery compartment must be designed to provide any required ventilation and preclude major system damage or serious personnel injury in the event of violent gas venting or rupture of battery cells. Furthermore, the design of battery compartments which house lithium-sulfur dioxide batteries will need to be verified by actual rapid-rise pressure testing IAW Appendix A, Technical Bulletin #7, Battery Compartment Design Guidelines for Equipment Using Lithium-Sulfur Dioxide Batteries. This TB also contains equipment and battery compartment design recommendations to minimize failure and injury. Where equipment will be exposed to weather, a watertight battery compartment may also be required to preclude corrosion and possible shorting out of the battery terminals.

c. An airtight plate or panel may be provided to separate wiring connections between batteries in a separate compartment and the power input to an equipment. This is to preclude any explosive gases from the battery from entering the electronics and being ignited. The resultant explosions caused by leaking connectors have surprised more than one soldier carrying an AN/PRC-77 manpack radio when hydrogen gas leaked into the radio compartment. Fortunately, no real serious injuries have occurred, but the potential for serious injuries has required a redesign of the connector to be airtight.

d. Ventilation - As previously mentioned in Chapter 1, adequate ventilation may be required depending on battery type to prevent the build-up of explosive and/or toxic

gas/fume mixtures. Obviously, all sources of ignition near the battery/box vent must be relocated or guarded (such as airtight enclosure or panel) to prevent fire/explosion.

e. Terminals of some batteries may need to be guarded since they are often a source of high currents. Shorting across an automotive type 12-volt battery with a tool or personal jewelry has frequently caused severe skin burns (as well as other injuries due to reflex actions or explosions of the battery). Where batteries must be installed into compartments that are not easily accessible or where nearby metallic objects may be accidentally contacted, applicable personal protective equipment should be worn. For battery removal and installation procedures refer to Technical Bulletin #4, Appendix A.

f. Charging - Since more rechargeable batteries are being used to meet the requirement of reducing the Army battery procurements by 50 percent, recharging of batteries will be more frequently done in the field. The following safety precautions should be included in the technical manuals:

(1) Batteries should be recharged with only the authorized charger.

(2) Batteries may overheat if overcharged or if not recharged in accordance with the manufacturer's requirements.

(3) If multiple batteries are being charged in a single location, adequate ventilation must be provided to exhaust possible hydrogen gas release during charging.

(4) All equipment must use only the authorized rechargeable batteries.

(5) Placing different types of rechargeable batteries together could result in explosive consequences.

(6) The batteries may overheat and leak if the terminals are short-circuited.

(7) Primary (non-rechargeable) batteries must never be installed onto chargers.

g. Lithium batteries have come a long way in their design and are relatively safe. Design features reduce the risk of internal and external shorts, thermal runaway, and charging of the battery, etc. Nevertheless, there are safety precautions that the equipment designer should take into consideration:

(1) Metallic lithium batteries are not to be charged, or shorted.

(2) If equipment uses two batteries, replace them in matched sets (same State Of Charge (SOC), manufacturer, date codes, etc).

(3) Remove batteries from equipment if they are not going to be used for extended periods of time (more than 30 days).

(4) Proper battery storage and disposal procedures must be followed. The activation of Complete Discharge Device (CDD) of the battery should be performed only by designated personnel.

(5) Void volume in the battery compartment is preferable from an unexpected venting standpoint. It facilitates removal and installation of the batteries by not requiring excessive force or distortion of the batteries themselves. See Appendix A, Technical Bulletin #7, for other design requirements for battery compartments.

CHAPTER 3

SAFETY CONCERNS FOR VEHICULAR/TRAILER APPLICATIONS

Vehicular mounted C-E equipment, including shelters mounted semi-permanently to trucks and systems installed on/within trailers, semi-trailers, vans, etc, need to be designed with the applicable guidance provided in Chapter 1. Also, some of the following guidance, which has resulted from lessons learned, will apply to non-vehicular mounted systems. That is, land-based systems that are moved or transported periodically from location to location, as opposed to systems that are highly mobile and/or operating "on-the-move." Major safety concerns which involve vehicular/trailer mounted systems include the following:

3-1. Exhaust/Emissions - Vehicle exhaust and/or vehicle/trailer mounted generators (co-located with shelters, etc.) may create Carbon Monoxide (CO) or other health hazards from the diesel fuel. Operating scenarios may require vehicle engines to be running to provide both power to equipment and mobility. If speeds are slow and/or generators are mounted on the same vehicle, health hazards from the exhaust may occasionally occur unless extreme care is taken to route exhausts away from occupied enclosures, air intakes, etc. Testing needs to be performed to assure that potential hazards do not exist. CO monitors mounted inside shelters have been found to be unreliable in detecting unsafe CO levels. This is because they cannot withstand transport vibration, do not work through the entire operational temperature range, and often require recalibration.

3-2. System Noise - Overall system noise may well be greater in a mobile configuration due to the proximity of vehicle and generator. Communication quality may be affected by excessive noise level. Operator fatigue could also result from excessive noise and vehicle vibration. Design to minimize noise must be emphasized.

3-3. Weight/Load Distribution - As previously mentioned in Chapter 1, this is of even greater concern for highly mobile vehicular/trailer mounted systems since overall weight and weight distribution will greatly impact the roadability of the overall configuration. Testing of the full system in its mobile configuration must be performed to determine maximum safe speeds over various terrain and road types. Again, an overweight system will most likely create additional operational restrictions and possible safety concerns (e.g., vehicle structural failure, etc).

3-4. On-the-Move Configurations - Where operating procedures will require personnel to be located inside the equipment enclosure while a vehicle is moving, approved seating and seat belts must be installed. Equipment and hardware mounting locations may create potential head bumping and tripping hazards. An intercom system between the vehicle driver and shelter occupants must be provided for constant communications and for emergency situations. Adequate ventilation is required in shelters to provide good air quality. Sometimes, vehicular mounted whip antennas must be extended for transmit/receive modes, and therefore antenna tiedowns may not be in place

to minimize hazards of striking tree limbs, overhead power lines, etc. Designers need to consider different antenna design to minimize hazards. If new design cannot be made, well-enforced driver precautions/operating procedures may be the only way to minimize these risks. Further design information regarding “On-the-Move Configurations” is provided in Appendix A, CECOM-TR-95-3.

3-5. Ingress/Egress - Vehicular mounted systems normally require boarding ladders, and the same safety design considerations as described in paragraph 1-1a of Chapter 1 apply.

3-6. Trailers - We have learned of some rather unique safety related problems involving a trailer mounted antenna system. The problems involved the trailer tow-bar area, which contains structural metal members connecting the trailer to a ring called a "lunette." The lunette, in turn, is connected to a prime mover via a towing pintle, which is a “C” shaped hinged device, allowing its upper half to be moved upwards to permit the lunette to be placed over the lower portion of the pintle. After this is accomplished the upper hinged portion of the pintle is pulled downward to its closed and locked position. Two specific problems have been reported:

a. The tow bars were too short, and as a result the trailer structure would hit the prime mover during the execution of sharp slow speed turns causing structural damage.

b. Both pintle and lunette were capable of rotating 360°. An engineering analysis revealed that under some conditions these rotations may result in the pintle becoming positioned upside down with the lunette resting (and applying considerable downward pressure) on the moveable/hinged portion, which is not designed to sustain that stress or to function in that manner. The lunette should rest mainly on the stronger, lower portion of the “C” shaped pintle.

The lessons learned here are to assure that the design of the trailer (tow bars, in this case) does not create the hazard of damaged equipment and that lunettes should be fixed (non-rotating), assuming the prime mover pintle allows for rotation.

3-7. Grounding - If operational scenarios allow, the vehicular mounted system that uses external power, should be provided with an earth ground similar to that of shelters. This is especially true if the system will have land-lines connected to it or if antennas are mounted on the system. Highly mobile systems, especially those that are "on-the-move” most of the time, may not allow enough time to install and remove a conventional ground rod system. In those situations, the physical configuration needs to be analyzed to assess the risk of not utilizing an earthen ground. Normally earthen grounds will not be required if the system is totally contained on the vehicle, has no external cables connected to it, and no high antennas which obviously might attract lightning.

Mobile configurations may be mounted on tracked vehicles. The treads of such vehicles do not provide an adequate ground connection to earth. Therefore, a tracked vehicle should be treated the same as a wheeled vehicle with respect to earth grounding.

Normal electrical bonding, and inclusion of Equipment Grounding Conductors (EGC - green wire) on the vehicular or trailer mounted system, will provide for personnel safety. In mobile configurations, the principal purpose of an earth ground system is to provide a preferred lightning discharge path for those system configurations having a likelihood of being struck by lightning.

It is suggested that, where possible, ground rods be employed. Where impractical, an analysis by a qualified safety engineer needs to be performed to determine the level of risk involved and recommendations regarding the acceptance of the safety risk involved. A possible alternative ground (earth) connection for highly mobile systems is the Surface Wire Grounding System (SWGS) mentioned previously in paragraph 1-2a of Chapter 1.

CHAPTER 4

ANTENNAS

The safety problems that we have experienced with antennas, for the most part, have been accidents involving antenna contact with overhead power lines and puncture wounds caused by relatively sharp antenna elements. Unfortunately, several severe injuries and fatalities have resulted from accidents involving B16 managed antennas. Safety engineering design guidance to reduce these problems is provided below for two general families of antennas (whip antennas and antenna/mast systems).

4-1. Whip Antennas - These items may be attached to mobile or fixed systems. The following design recommendations will help preclude or greatly reduce the number of accidents most frequently experienced with whip antennas:

a. Incorporate permanently affixed tip caps or blunt design on upper section to reduce/eliminate puncture wounds. Where possible, size of cap should be large enough to preclude penetration of the human eye socket, which has been the entry point of several accidents involving antenna elements.

b. Antenna tie-downs - Whether a whip antenna is mounted on a HMMWV, tank, mobile shelter, or on a system infrequently moved; the need to tie down the antenna will most likely occur. Since transmitting/receiving is required during mobile operations, the antenna should be designed so that it does not protrude outside of the "safe envelope" (that is: no possibility of striking overhead power and obstructions, etc.). Impaling of soldiers and contact with overhead power lines (especially overhead railroad power lines at rail crossings) have necessitated the following:

(1) Tie-downs shall be such as to minimize side-to-side movement. A two-point tie-down assembly may be required. Excessive lateral sway with a single rope tie-down point resulted in an antenna being impaled into a soldier's eye as he was walking along the side of the road that the vehicle was traveling. In situations like that, even tip caps or blunt ends do not totally prevent serious injuries.

(2) Tie-down clamps are desirable for those systems which require frequent antenna tie down and release. A tie-down clamp permanently attached to a tie-down assembly must be designed to only permit the antenna to be placed under the clamp, preventing unintentional dislodging due to vibration or striking objects (e.g., overpasses or tree limbs, etc). The main thing to remember is that the tie-down needs to be easy to use. It must tie the antenna in position so that it will clear all overhead objects and power lines, will not allow excessive swaying, and will only allow intentional release. This guidance cannot be overemphasized, much equipment and soldier's lives have been adversely impacted by the lack of or improper tie-down of whip antennas.

c. Antenna restraint boots - Some whip antennas, especially those that are relatively short, may require a restraining device (boot) for crew members' protection to limit forward rebound of the antenna after it has struck an overhead obstacle. Tests are usually required to see if such a device will be required for each antenna geometry. The AS-2731 is an example of an antenna requiring this device.

d. High Voltage (H.V.) Protection - Where design constraints permit, dielectric coating should be considered to reduce the safety risk if accidental contact with power lines occurs. High voltage protection may also be enhanced by utilizing H.V. protection devices (antenna sections incorporating capacitive networks). One such device has been developed for use with CECOM's AS-1729/VRC Whip Antenna. While these measures certainly will enhance safety and reduce the probability of serious injuries, a false sense of total safety must not be allowed. Good common sense in using antennas, staying away from overhead power lines when possible, and enforcement of use of proper tie-down procedures, etc., must still prevail.

4-2. **Antenna Mast Systems** - Included in this group will be field type masts, towers, and metal poles, etc. used to support antenna elements/dishes, wires, and so forth. For these items/systems, implementation of the design criteria noted below will help to enhance their safety and will again greatly reduce the occurrence of the two most prevalent antenna related accidents (eye injury and contacting power lines).

a. Since masts, towers, and antennas must be installed as far away from power lines as possible, permanent-type labels affixed to a lower mast section will help the user to remember the rule of keeping the mast/tower a distance of at least twice its height away from power lines. A similar warning should also be printed on the antenna bag and a warning note should be incorporated into the TM.

b. Antenna elements must not have sharp or small cross-sectional areas at their ends. We have learned of several fatalities, and one permanent paralysis caused by antenna element ends entering victims' eyes and penetrating into their brains. Accidents occurred when soldiers walked/ran into lowered elements and, in one case, a soldier was injured due to mast failure and the falling of the antenna cone assembly. Permanently affixed tip caps or bluntly designed ends (bigger than 1.75 inches in diameter) are essential to avoid any further deaths or serious injuries.

c. Antenna masts need to be rugged enough to withstand considerable use (and abuse) in the field. If operational scenarios require rapid deployment and relocation of a mast system, a flexing design may not be desirable to the user. Case in point: The OE-254 Antenna mast has often been referred to as "old spaghetti" because of its excessive bending, which necessitates skilled and careful erecting procedures. It cannot always be rapidly erected and can be a problem where site availability necessitates installation amongst trees and other nearby overhead objects. Field users of this particular antenna mast have used unauthorized camouflaged poles (used for installing camouflage netting) since they are somewhat interchangeable and provide a much more rigid mast which is

more easily/quickly raised and lowered without being concerned with "reverse bends," etc. The lesson learned here is to make sure the mast design fully meets the user's needs so as not to cause him to "jury rig" the system and possibly create additional hazards. In this example, the additional hazard was created by additional stress on the OE-254 mast sections by the less than optimal fit between the authorized and unauthorized sections (resulting in mast section cracking and failure).

d. High Voltage Protection - Dielectric mast sections may be incorporated to reduce the risk if power lines are accidentally contacted. However, it must be remembered that electricity may still flow down the antenna lead-in wire, and if the user was near that wire, he/she would still probably be at great risk. As with the whip antennas, a false sense of security should not dictate abandonment of common sense to stay clear of power lines.

e. Antenna mast systems need to incorporate ground rod connection stubs at their base. A threaded bolt or stud with wing nut can be welded to the lowest mast section and will facilitate placing an earthen ground near the base of the assemblage. Antenna discharge devices, used for lightning protection, should be incorporated where possible to allow the dumping of high voltage/high current surges, EMP, etc., to earth via the mast ground. If antenna mast sections do not provide a reliable low impedance path at their mating joints or are not conductive, a separate dedicated down conductor would be required. A separate air terminal should be incorporated at the highest mast point, or the antenna itself may be utilized for that purpose. In that instance, the antenna lightning protection discharge device would be essential. See Appendix A, CECOM-TR-93-1, for further information.

f. Guy wire assemblies must be engineered to provide for safe erection procedures without overtaxing the prescribed number of installers. Furthermore, guy wire anchors must allow for various soil applications (firm, loose, etc.) and be tested to assure that maximum designed wind velocities and icing can be safely survived.

g. Hydraulically Actuated Masts - We see more of these systems which are frequently mounted on trailers or mounted on shelters or vehicular systems. Hydraulic or other assisted erecting mechanisms need to be fail-safe, that is, not allow the mast to fall or unintentionally retract if hydraulic, electrical, or other failures should occur. Antenna masts that can be raised from inside of shelters/vehicles, pose a problem in that they can be raised into overhead lines. An accident was reported that a soldier received a severe shock and was hospitalized when an antenna mast, which was set-up from inside the shelter, was too close to power lines, and it fell. Therefore, precautionary procedures must be provided and exercised during this kind of antenna set-up.

h. Stability – Most antenna mast systems that are erected on the ground obtain their stability via properly placed guy wires and anchors. Vehicular or trailer mounted systems may do the same, or rely totally on vehicle/trailer stability, or incorporate a combination of both. Stability may be verified as part of the maximum wind velocity test.

Installation of heavy antenna dishes, antenna rotators, etc., high up on the mast can create stability problems and needs to be covered in designing the system. Do not forget, vehicular mounted shelters or any antenna system, which is vehicular or trailer mounted, must be tested for roadability.

i. Equipment mounted on masts - We have experienced problems with improperly welded components mounted high up on masts. Obviously any structural or workmanship deficiency may well create a potential safety hazard due to possible falling of heavy objects from above.

j. Personal Protective Equipment (PPE) - The antenna-related accidents involving penetration of antenna elements into victims' eyes may have been significantly less serious had the users been wearing PPE. Helmets or hard hats, ANSI approved eye protection (goggles), and gloves must be worn at all times during antenna erecting/lowering procedures, etc. Management must assure that individuals are properly trained, that PPE is available and use is strictly enforced.

k. Installation and tear-down procedures - Incidents on the MSE 30-meter mast were attributed to incorrect training and published instructions. The TM and training courses called for a larger installation team than the Operational Requirements Document (ORD) and specification required. Subsequently, installation and tear-down procedures were changed to safely accommodate a smaller team. Lessons learned are as follows:

(1) Procedures for installing and tearing down antenna masts should be verified through testing before they are published in the technical manuals and before the operator training course is approved. These procedures should cover normal and adverse conditions, especially wind loading.

(2) The maximum safe wind loading for erection, operation, and survivability of the mast should be determined through the test program. The Directorate for Safety and the Research, Development and Engineering Center (RDEC) should be involved in planning and witnessing these tests.

CHAPTER 5

NIGHT VISION DEVICES

Night Vision Devices (NVDs) make it possible for users to perform a wide variety of tasks during periods of darkness. However, there are limitations to this technology, it does not turn night into day. In the past we have encountered problems due to inherent design limitations of the equipment, quality control, and integration concerns. Lessons learned from these concerns apply in a generic sense to the design of all military systems. Here's what we found:

5-1. Design Limitations. Inherent design limitations (such as limited field-of-view, blooming, and reduced depth perception) can be minimized, but not eliminated. These limitations must be identified and evaluated through analyses, and actions must be taken to minimize their effects. For example, one limitation of a night vision goggle is a reduced field of view (40^{o} for the Aviator's Night-Vision Imaging System (ANVIS)). The system design attempts to maximize the field of view. However, scanning techniques must also be developed and implemented by users to overcome this limitation. If the inherent design limitation is serious enough, a System Safety Risk Assessment will have to be performed to determine if the user is willing to accept the risk(s) associated with these limitations.

5-2. Specifications and Quality Control. Specifications must be carefully written, and quality control inspections must be performed to ensure that changes have not occurred which will degrade the performance of the system. One example demonstrates the importance of both of these points. Investigation revealed that a distortion problem with the ANVIS and AN/PVS-5 was related to several Class C aircraft accidents. The source of this distortion was traced to a fiber optic inverter used in the image intensifier tubes. The equipment specification called out a maximum allowable distortion level, and investigation revealed that many of the tubes in the field exceeded this maximum level. This indicates that the contractor was performing inadequate quality control. However, an additional study determined that the distortion level listed to begin with in the equipment specification was considered unsafe by pilots. Although the contractor was at fault for producing “out-of-spec” systems, the government was also responsible for a number of systems, which were within the limits of the original specification but still considered unsafe by users. This problem resulted in the temporary deadlining of many night vision systems, a lengthy inspection process, and ultimately the loss of approximately 10-15% of fielded image intensifier tubes (with the cost shared by the government and the contractor). Conclusions: (1) the values that are set for safety-critical parameters must be proven (preferably by test) before they are accepted and (2) the quality control measures for these parameters must be rigorously enforced.

5-3. System Integration. The design of a piece of equipment must consider the environment in which the equipment will be used. When the ANVIS was developed it was realized that the aircraft cockpit lighting would interfere with the performance of the night vision goggles and could cause them to shut down. To counter these effects, two measures were instituted:

a. A filter was designed into the ANVIS, which prevents blue-green light from being intensified.

b. A new specification was published to require all equipment installed in aircraft cockpits to be compatible with the ANVIS. All equipment intended for use in Army aircraft must comply with MIL-L-85762A, "Lighting, Aircraft, Interior, ANVIS Compatible."

Additional information regarding night vision lessons learned can be found on the Army Safety Center's Risk Management Information System (RMIS) website, at http://rmis.army.mil. Current aviation NVD safety messages can be located at: www.rucker.army.mil/atb/nvd/nvdb.htm.

CHAPTER 6

SOFTWARE SAFETY

In the past, industry in general considered increased productivity as the most important aspect of Software Engineering. Very little was mentioned about the reliability of the software product and nothing was mentioned about the safety of the software.

In recent years a primary role of software and hardware has become the command and control of complex and costly systems upon which human lives may depend. This role has compelled the Department of Army as well as Industry to establish goals of highly reliable and productive, safe software in which hazard-causing faults or errors are unacceptable. These new goals require the support of professionals who have attained some level of expertise in the various aspects of software and firmware. System Safety Engineers are no exception. The Safety Engineer should be able to apply system safety methods and techniques to the analysis of software systems with a reasonably high level of confidence in order to certify the safety of the system that software controls.

Recent cases of software whose use was unsafe are strongly suggestive of the risks involved. We believe that System Safety Engineers should recognize that software is just another system component, and that this component can contain errors or defects which can cause undesired events in the hardware system it is controlling. System Safety Engineers should work with Software Engineers to identify those errors which can cause hazards or produce undesired events.

6-1. Therac Radiation Therapy Machine Fatalities.

a. Summary

Eleven Therac-25 therapy machines were installed, 5 in the US and 6 in Canada. They were manufactured by the Canadian Crown (government owned) company AECL. The Therac-25 model was an advanced model over earlier models (-6 and -20 models, corresponding to energy delivery capacity) with more energy and automation features. Although all models had some software control, the -25 model had many new features and had replaced most of the hardware interlocks with software versions. There was no record of any malfunctions resulting in patient injury from any of the earlier model Theracs (earlier than the -25). The software control was implemented in a DEC model PDP 11 processor using a custom executive and assembly language. A single programmer implemented virtually all of the software. He had an uncertain level of formal education and produced very little, if any, documentation on the software.

Between 6/85 and 1/87 there were six known accidents involving massive radiation overdoses by the Therac-25. Three of the six resulted in fatalities. The company did not respond effectively to early reports citing the belief that the software could not be

a source of failure. Records show that software was deliberately left out of an otherwise thorough safety analysis performed in 1983 which used fault-tree methods. Software was excluded because "software errors" have been eliminated because of extensive simulation and field testing. Also, software does not degrade due to wear, fatigue or reproduction process. Other types of software failures were assigned very low failure rates with no apparent justification. After a large number of lawsuits and extensive negative publicity, the company decided to withdraw from the medical instrument business and concentrate on its main business of nuclear reactor control systems.

The accidents were due to many design deficiencies involving a combination of software design defects and system operational interaction errors. There were no apparent review mechanisms for software design or quality control. The continuing recurrence of the accidents before effective corrective action resulted was a result of management's view. This view had faith in the correctness of the software without any apparent evidence to support it. The errors were not discovered because the policy was to fix the symptoms without investigating the underlying causes (of which there were many).

b. Key Facts

- The software was assumed to be fail-safe and was excluded from normal safety analysis review.

- The software design and implementation had no effective review or quality control practices.

- The software testing at all levels was obviously insufficient, given the results.

- Hardware interlocks were replaced by software without supporting safety analysis.

- There was no effective reporting mechanism for field problems involving software.

- Software design practices (contributing to the accidents) did not include basic, shared-data and contention management mechanisms normal in multi-tasking software. The necessary conclusion is that the programmer was not fully qualified for the task.

- The design was unnecessarily complex for the problem. For instance, there were more parallel tasks than necessary. This was a direct cause of some of the accidents.

c. Lessons Learned

(1) Changeover from hardware to software implementation must include a review of assumptions, physics and rules.

(2) Testing should include possible abuse or bypassing of expected procedures.

(3) Design and implementation of software must be subject to the same safety analysis, review and quality control as other parts of the system.

(4) Hardware interlocks should not be completely eliminated when incorporating software interlocks.

(5) Programmer qualifications are as important as qualifications for any other member of the engineering team.

6-2. Missile Launch Timing Causes Hangfire.

a. Summary

An aircraft was modified from a hardware controlled missile launcher to a software-controlled launcher. The aircraft was properly modified according to standards and the software was fully tested at all levels before delivery to operational test. The normal weapons rack interface and safety overrides were fully tested and documented. The aircraft was loaded with a live missile (with an inert warhead) and sent out onto the range for a test firing. The aircraft was commanded to fire the weapon, whereupon it did as designed. Unfortunately, the design did not specify the amount of time to unlock the holdback and was coded to the assumption of the programmer. In this case, the assumed time for unlock was insufficient and the holdback locked before the weapon left the rack. As the weapon was powered, the engine drove the weapon while it was attached to the aircraft. This resulted in a loss of altitude and a wild ride - but the aircraft landed safely with a burned out weapon.

b. Key Facts

- Proper procedures were followed as far as specified.

- The product specification was reused without considering differences in the software implementation, such as the timing issues. Hence, the initiating event was a specification error.

- While the acquirer and user had experience in the weapons system, neither had experience in software. Also, the programmer did not have experience in the details of the weapons system. The result was that the interaction between the two parts of the system was not understood by any of the parties.

c. Lessons Learned

(1) Because the software-controlled implementation was not fully understood, the result was flawed specifications and incomplete tests. Therefore, even though the software and subsystem were thoroughly tested against the specifications, the system design was in error, and a mishap occurred.

(2) Changeover from hardware to software requires review of design assumptions by all relevant specialists acting jointly. This joint review must include all product specifications, interface documentation, and testing.

(3) The test, verification, and review processes must each include end-to-end event review and test.

6-3. Reused Software Causes Flight Controls to Shut Down.

a. Summary

A research vehicle was designed with fly-by-wire digital control and, for research and weight considerations, had no hardware backup systems installed. The normal safety and testing practices were minimized or eliminated by citing many arguments. These arguments cited use of experienced test pilots, limited flight and exposure times, minimum number of flights, controlled airspace, use of monitors and telemetry, etc. Also the argument justified the action as safer because the system reused software from similar vehicles currently operational.

The aircraft flight controls went through every level of test, including "iron bird" laboratory tests that allow direct measurement of the response of the flight components. The failure occurred on the flight line the day before actual flight was to begin after the system had successfully completed all testing. The flight computer was operating for the first time unrestricted by test routines and controls. A reused portion of the software was inhibited during earlier testing as it conflicted with certain computer functions. This was part of the reused software taken from a proven and safe platform because of its functional similarity. This portion was now enabled and running in the background.

Unfortunately, the reused software shared computer data locations with certain safety-critical functions and it was not partitioned nor checked for valid memory address ranges. The result was that as the flight computer functioned for the first time, it used data locations where this reused software had stored out-of-range data on top of safety-critical parameters. The flight computer then performed according to its design when detecting invalid data and reset itself. This happened sequentially in each of the available flight control channels until there were no functioning flight controls. Since the system

had no hardware backup system, the aircraft would have stopped flying if it were airborne. The software was quickly corrected and was fully operational in the following flights.

b. Key Facts

- Proper procedures were minimized for apparently valid reasons, i.e., the (offending) software was proven by its use in other similar systems.

- Reuse of the software components did not include review and testing of the integrated components in the new operating environment. In particular, memory addressing was not validated with the new programs that shared the computer resources.

c. Lessons-Learned

(1) Safety-critical, real-time flight controls must include full integration testing of end-to-end events. In this case, the reused software should have been functioning within the full software system.

(2) Arguments to bypass software safety, especially in software containing functions capable of a Kill/Catastrophic event, must be reviewed at each phase. Several of the arguments to minimize software safety provisions were compromised before the detection of the defect.

6-4. Flight Controls Fail at Supersonic Transition.

a. Summary

A front-line aircraft was rigorously developed, thoroughly tested by the manufacturer, and again exhaustively tested by the government and finally by the using service. Dozens of aircraft had been accepted and were operational worldwide when the service asked for an upgrade to the weapons systems. One particular weapon test required significant telemetry. The aircraft change was again developed and tested to the same high standards including nuclear weapons carriage clearance. This additional testing data uncovered a detail missed in all of the previous testing.

The telemetry showed that the aircraft computers all failed -- ceased to function and then restarted -- at a certain airspeed (Mach 1). The aircraft had sufficient momentum and mechanical control of other systems so that it effectively "coasted" through this anomaly and the pilot did not notice.

The cause of this failure originated in the complex equations from the aerodynamicist. His specialty assumes the knowledge that this particular equation will asymptotically approach infinity at Mach 1. The software engineer does not inherently understand the physical science involved in the transition to supersonic speed at Mach 1.

The system engineer who interfaced between these two engineering specialists was not aware of this assumption and, after receiving the aerodynamicist's equation for flight, forwarded the equation to software engineering for coding. The software engineer did not plot the equation and merely encoded it in the flight control program.

b. Key Facts

- Proper procedures were followed to the stated requirements.

- The software specification did not include the limitations of the equation describing a physical science event.

- The computer hardware accuracy was not considered in the limitations of the equation.

- The various levels of testing did not validate the computational results for the Mach 1 portion of the flight envelope.

c. Lessons Learned

(1) Specified equations describing physical world phenomenon must be thoroughly defined, with assumptions as to accuracy, ranges, use, environment, and limitations of the computation.

(2) When dealing with requirements that interface between disciplines, it must be assumed that each discipline knows little or nothing about the other and therefore must include basic assumptions.

(3) Boundary assumptions should be used to generate test cases as the more subtle failures caused by assumptions are not usually covered by ordinary test cases (division by zero, boundary crossing, singularities, etc.)

6-5. Incorrect Missile Firing From Invalid Setup Sequence.

a. Summary

A battle command center with a network controlling several missile batteries was operating in a field game exercise. As the game advanced, an order to reposition the battery was issued to an active missile battery. This missile battery disconnected from the network, broke down their equipment and repositioned to a new location in the grid.

The repositioned missile battery arrived at the new location and commenced setting-up. A final step was connecting the battery into the network. This was allowed in any order. The battery personnel were still occupying the erector/launcher when the connection that attached the battery into the network was made elsewhere on the site.

This cable connection immediately allowed communication between the battery and the battle command center.

The battle command center, meanwhile, had prosecuted an incoming "hostile" and designated the battery to "fire," but targeted to use the old location of the battery. As the battery was off-line, the message was buffered. Once the battery crew connected the cabling, the battle command center computer sent the last valid commands from the buffer and the command was immediately executed. Personnel on the erector/launcher were thrown clear as the erector/launcher activated on the old slew and acquire command. Personnel injury was slight as no one was pinned or impaled when the erector/launcher slew.

b. Key Facts

- Proper process and procedures were followed as specified.

- Subsystems were developed separately with interface control documents. Messages containing safety-critical commands were not "aged" and reassessed once buffered.

- Battery activation was not inhibited until personnel had completed the setup procedure.

c. Lessons Learned

(1) System engineering must define the sequencing of the various states (dismantling, reactivating, shutdown, etc.) of all subsystems with human confirmations and reinitialization of state variables (e.g., site location) at critical points.

(2) System integration testing should include buffering messages (particularly safety-critical) and demonstration of disconnect and restart of individual subsystems to verify that the system always transitions between states safely.

(3) Operating procedures must clearly describe (and require) a safe and comprehensive sequence in dismantling and reactivating the battery subsystems with particular attention to the interaction with the network.

6-6. Operator's Choice of Weapon Release Overridden by Software.

a. Summary

During field practice exercises, a missile weapon system was carrying both practice and live missiles to a remote site and was using the transit time for slewing practice. Practice and live missiles were located on opposite sides of the vehicle. The

acquisition and tracking radar was located between the two sides causing a known obstruction to the missile's field of view.

While correctly following command-approved procedures, the operator acquired the willing target, tracked it through various maneuvers, and pressed the weapons release button to simulate firing the practice missile. Without the knowledge of the operator, the software was programmed to override his missile selection in order to present the best target to the best weapon. The software noted that the current maneuver placed the radar obstruction in front of the practice missile seeker while the live missile had acquired a positive lock on the target and was unobstructed. The software therefore optimized the problem and deselected the practice missile and selected the live missile. When the release command was sent, it went to the live missile and "missile away" was observed from the active missile side of the vehicle when no launch was expected. The "friendly" target had been observing the maneuvers of the incident vehicle and noted the unexpected live launch. Fortunately, the target pilot was experienced and began evasive maneuvers but the missile tracked and still detonated in close proximity.

b. Key Facts

- Proper procedures were followed as specified and all operations were authorized.

- All operators were thoroughly trained in the latest versions of software.

- The software had been given authority to select "best" weapon but this characteristic was not communicated to the operator as part of the training.

- The indication that another weapon had been substituted (live vs. practice) by the software was displayed in a manner not easily noticed among other dynamic displays.

c. Lessons Learned

(1) The versatility (and resulting complexity) demanded by the requirement was provided exactly as specified. This complexity, combined with the possibility that the vehicle would employ a mix of practice and live missiles was not considered. This mix of missiles is a common practice and system testing must include known scenarios such as this example to find operationally based hazards.

(2) Training must describe the safety-related software functions such as the possibility of software overrides to operator commands. This must also be included in operating procedures available to all users of the system.

6-7. Case Sensitive Input Changes AFATDS Operator's Situational Awareness.

A residual safety hazard was found to exist within the Advanced Field Artillery Tactical Data System (AFATDS) software. When an AFATDS operator entered a coordinate location using lower case letters in the Military Grid Reference System (MGRS) grid zone designator (instead of upper case) for the alpha characters, the coordinate location was moved entirely off the portion of the AFATDS map where the operator was currently working. The operator's situational awareness was thus compromised. Inaccurate displays of coordinate locations can result in missions being fired into areas occupied by friendly troops. Fratricide can possibly result.

This safety hazard went undetected throughout the development and testing of the software and was only detected after the software was fielded. Common shortcuts to "key jamming" a location in MGRS (such as "drag and drop" and the use of other coordinate systems) allowed developers, testers, and even operators to enter location data without encountering this anomaly.

Case sensitivity in critical data must be considered for its impact on the operation of the software and to the safety of our troops. Enabling operators to use either upper case or lower case letters to enter MGRS grid locations subsequently eliminated the described AFATDS hazard. Remember: Software always works as designed, but not necessarily as intended.

As of August 94, additional guidance has been available via a CECOM Research and Development Technical Report (CECOM-TR-94-10) entitled "Identification, Integration and Tracking of Software System Safety Requirements."