Bar Code →

PB97-207815

copy

DOT/FAA/CT-94/67

FAA Technical Center
Atlantic City International Airport,
N.J. 08405

FAA Technical Center Test Requirement Plan for the Enhanced Airport Security Test (EAST) Facility

Ray Schillinger
Walter Wall
Ron Cole

October 1994

Final Report

This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161.

Property of
Aviation Security Library

U.S. Department of Transportation
Federal Aviation Administration

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

Technical Report Documentation Page

1. Report No. DOT/FAA/CT-94/67	PB97-207815	3. Recipient's Catalog No.
4. Title and Subtitle A TECHNICAL CENTER TEST REQUIREMENT PLAN FOR THE ENHANCED AIRPORT SECURITY TEST (EAST) FACILITY		5. Report Date October 1994 6. Performing Organization Code ACA-400
7. Author(s) Ray M. Schillinger (ACA-600), Walter Wall (ACA-400), and Ron Cole (MSA)		8. Performing Organization Report No. A-2001001-94-U-10065
9. Performing Organization Name and Address U.S. Department of Transportation Federal Aviation Administration Technical Center Aviation Security Research and Development Service Atlantic City International Airport, NJ 08405		10. Work Unit No. 11. Contract or Grant No.
12. Sponsoring Agency Name and Address U.S. Department of Transportation Federal Aviation Administration Assistant Administrator for Civil Aviation Security, ACS-1 800 Independence Avenue, S.W. Washington D.C. 20591		13. Type of Report and Period Covered Final Report 14. Sponsoring Agency Code ACS-1

15. Supplementary Notes:

REPRODUCED BY: NTIS
U.S. Department of Commerce
National Technical Information Service
Springfield, Virginia 22161

Report Prepared by: DCS, Inc.
2511 Fire Road, Suite A-5
Absecon, NJ 08201

MSA, Inc.
4995 La Cross Road, Suite 2500
N. Charleston, SC 29418

16. Abstract

This report provides the technical rationale for, and a description of, a laboratory for the testing of security devices being considered for installation at airports and other facilities which are under the cognizance of the Federal Aviation Administration. The report is structured into three major divisions. The first is a description of the technologies and devices routinely employed in modern security systems. It provides the rationale for the second major portion, a description of the types of testing to be performed and the requisite equipment. The physical layout of the laboratory and test ranges, and approximate cost and schedule information comprise the third major section.

Cost information is included in this document, in terms of laboratory testing and support equipment, and general installation and construction costs. Cost information is presented as if the laboratory is to be implemented as a single effort (including both outdoor test ranges).

Property of
Aviation Security Library

17. Key Words Compatibility Testing, Prototype Testing, Electronic Security System, Camera Employment, Video Switching, Intrusion Detection Systems	18. Distribution Statement This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	68	

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

THIS PAGE INTENTIONALLY LEFT BLANK

Property of
Aviation Security Library

TABLE OF CONTENTS

1. INTRODUCTION 1

1.1 OBJECTIVES 1
1.2 ORGANIZATION 1
1.3 SCOPE 1

2. BACKGROUND 3

2.1 SECURITY SYSTEM TESTING 3

2.1.1 Types of Tests and Testing Objectives 3

2.1.1.1 Compatibility Testing 3
2.1.1.2 Prototype System Tests 4
2.1.1.3 Operational Testing 4

2.1.2 Test Categories 4

2.2 OVERVIEW 4

2.2.1 Security System Concepts 4

2.2.1.1 Surveillance Subsystem 8
2.2.1.2 Intrusion Detection Subsystem 8
2.2.1.3 Access Control Subsystem 9

2.2.2 System Coupling 9

3. SURVEILLANCE SYSTEMS 11

3.1 TECHNOLOGY AND DEVICES 11

3.1.1 Cameras 11
3.1.2 Camera Employment 11
3.1.3 Monitors 12
3.1.4 Video Switching 12
3.1.5 Video Motion Detection 12
3.1.6 Video Data Lines 13

TABLE OF CONTENTS (Continued)

3.2 TESTING REQUIREMENTS AND EQUIPMENT 13

3.2.1 Cameras 13
3.2.2 Camera Employment 13
3.2.3 Video Motion Detectors 14
3.2.4 Video Switchers 14
3.2.5 Monitors 14

4. INTRUSION DETECTION SYSTEMS 15

4.1 TECHNOLOGIES AND DEVICES 15
4.2 INTERIOR SENSORS 15

4.2.1 Door and Window Sensors 15
4.2.2 Glass Break Detectors 16
4.2.3 Passive Infrared (PIR) Detectors 16
4.2.4 Ultrasonic Sensors 16

4.3 FENCE SENSORS 16

4.3.1 Taut-Wire Types 17
4.3.2 Fence Movement Sensors 17
4.3.3 Electrical Field and Capacitance Fences 18

4.4 FREE-STANDING SENSORS 18

4.4.1 Buried Line Sensors 18
4.4.2 Bistatic Microwave 19
4.4.3 Monostatic Microwave 19
4.4.4 Fiber Optic Detectors 19
4.4.5 Other Devices/Sensors 20

5. ACCESS CONTROL SYSTEMS 21

5.1 PURPOSE 21
5.2 SYSTEM ARCHITECTURE 21
5.3 TECHNOLOGIES AND DEVICES 22

TABLE OF CONTENTS (Continued)

5.3.1 Magnetic Cards and Readers 22
5.3.2 Proximity Cards 23
5.3.3 Biometric Devices 23
5.3.4 Keypads 23
5.3.5 Cipher Locks 24

6. DATA AND COMMUNICATIONS 25

6.1 COMMUNICATION LINES 25
6.2 COMMUNICATIONS TESTING 26
6.3 TEST EQUIPMENT 26

7. EMI/RFI TESTING 27

7.1 INTERFERENCE 27
7.2 EMI/RFI GENERATION 27
7.3 EMI/RFI SUSCEPTIBILITY 28

8. TEST EQUIPMENT 30

8.1 SPECIFIC INSTRUMENTS 30
8.2 ELECTRONICS WORKBENCH EQUIPMENT 30

8.1.1 Electronics Workbench Support Equipment 34
8.1.2 Fiber Optics Workbench Test Equipment 36
8.1.3 Fiber Optics Support Equipment 36
8.1.4 Workbenches 37
8.1.5 Fabrication Workbench 37

9. LABORATORY AND TEST RANGES 38

9.1 PROPOSED FACILITIES AND LAYOUTS 38

9.1.1 Eastlab 38
9.1.2 Test Range 1 42
9.1.3 Test Range 2 42

10. CONCLUSIONS 46

11. RECOMMENDATIONS 47

TALBE OF CONTENTS (Continued)

APPENDICES

A - DEVICE TEST SHEET A-1

B - LESSONS LEARNED B-1

C - COST ESTIMATE - CONSTRUCTION C-1

LIST OF ILLUSTRATIONS

Figure 1. Electronic Security System Conceptual Diagram 7

Figure 2. FAA Eastlab Floor Plan (Conceptual) 39

Figure 3. Electronics Workbenches (Elevation A-A) 40

Figure 4. Test Systems Workspace (Elevation B-B) 41

Figure 5. FAA EASTLAB Test Range (Conceptual) 43

Figure 6. FAA Eastport Test Range (Atlantic City International Airport) 44

Figure 7. Electronic Security System Test Tower (Conceptual) 45

LIST OF TABLES

Table 1. General Purpose Equipment 33

Table 2. Specialized Equipment 33

Table 3. Support Equipment 35

1. INTRODUCTION.

1.1 OBJECTIVES. The requirements of the Aviation Security Act of 1990 have resulted in a series of actions to address civil aviation threats and issues. One facet of the actions under the cognizance of the Federal Aviation Administration is the establishment of research and development laboratories for the investigation of technologies and techniques for security enhancement at airports and related facilities.

The Enhanced Airport Security Test (EAST) Facility is the subject of this document, and is the proposed laboratory which is to investigate security systems, consisting of surveillance, intrusion detection, and access control equipments. As used in this document, the term "testing" means all types of measurements and investigations which may be found necessary to determine or certify the technical or operational performance of security systems and components. The purpose of this testing process is to develop a listing of known characteristics and subsystem compatibilities which can be used to guide the selection of security equipment for broad scale implementation. A secondary purpose is to provide for the evaluation of new technologies and/or enhancements of current devices. The EAST Facility will be capable of ascertaining the technical and operational performance of individual components (such as infrared motion detectors), of compatibility of alternative devices, and overall assessment of prototypes of complete systems. The types of tests will range from very specific measurements of technical parameters, to operational testing of overall system performance under heavy demand conditions.

1.2 ORGANIZATION. This document is structured into three major divisions. The first is a description of the technologies and devices which are routinely employed in modern security systems. It provides the rationale for the second major portion, a description of the types of testing to be performed and the requisite equipment. The physical layout of the laboratory and test ranges, and approximate cost and schedule information comprise the third major section. Two appendices provide "lessons learned" information from the operation of a Department of Defense agency's "Operational Test Facility" for security systems, and several sample formats for system or component testing.

1.3 SCOPE. This document provides the technical rationale for, and a description of, a laboratory for the testing of security devices being considered for installation at airports and other facilities which are under the cognizance of the Federal Aviation Administration. The totality of the "laboratory" includes an indoor laboratory with general-purpose and specialized equipment, an outdoor test range which may be operated under well-controlled conditions, and a second outdoor test area located in the vicinity of an actual commercial airport which provides an approximation of a realistic environment.

In so far as possible, all of these laboratory facilities are designed with maximum flexibility and adaptability, and to permit the testing of items from small individual components to emulations of complete systems and prototypes.

Cost information is also included in this document, in terms of laboratory testing and support equipment, and general installation and construction costs. Cost information is presented as if the laboratory is to be implemented as a single effort (including both outdoor test ranges); however, it would be reasonable to implement the laboratory in phases, including deferral of certain of the test equipments, to match a funding profile or a phased implementation of responsibilities.

Note that this document specifically excludes any discussion of the need for such a laboratory, and concentrates on what is required and how the capabilities can best be achieved. It further excludes any description of threats, except where necessary to describe security system testing requirements.

2. BACKGROUND .

2.1 SECURITY SYSTEM TESTING. The overall purpose of the Laboratory is to conduct research and testing activities in support of initiatives to upgrade security systems for airports and related facilities. That general purpose requires that the Laboratory be capable of performing tests which have different overall objectives. Briefly, these different objectives may be summarized as follows:

2.1.1 Types of Tests and Testing Objectives. Tests to determine or measure specific technical parameters of devices. This category includes the measurement of technical parameters which are not published by the manufacturer, and tests to confirm published or advertised parameters. This type of testing is highly suited for the laboratory environment described in this document. It is noted, however, that in most cases, this type of testing requires that tests be made on statistically valid samples of the devices being investigated, potentially involving hundreds of repetitive tests, possibly over a protracted time period. The final product is a data base of known characteristics of available devices, which can be distributed or made available to design personnel. This data could also be used in the development of "standards" or "approved" device lists in the event that equipment requires certification prior to deployment.

- Types of Test and Test Objectives
- Compatibility Testing
- Prototype System Test
- Operational Testing

2.1.1.1 Compatibility Testing. This category includes tests to determine if devices or equipment from different manufacturers can be made to operate together, or if a new version of a manufacturer's device can be substituted directly for an older version. Most electronic security systems (including all three functions of surveillance, intrusion detection and access control) are, in fact, comprised of devices from many different manufacturers, and are integrated in ways not necessarily envisioned by the individual companies. Compatibility is also a significant issue in the upgrading of existing systems, by adding either new functions or "improved" versions of current functions. In theory, it should be possible to determine compatibility from review of published or measured device parameters, but there is no complete substitute for actual demonstration. The final product is a data base which will likely contain known incompatibilities as well as compatibilities. This category of testing is also well-suited to the proposed Laboratory, but it may require substantial investment in equipment and devices to be tested. (No provision has been made in the description of the Laboratory for storage of items no longer under active investigation or which are being retained for future potential tests. It is assumed that such equipment will be disposed of or stored in an appropriate facility external to the Laboratory).

2.1.1.2 Prototype System Tests. These tests would be performed to demonstrate or investigate technical aspects of proposed system designs (rather than of specific devices). They involve set-up of an entire system according to the proposed design, although in a "scaled-down" form. In most cases, this will make use of the indoor laboratory and one or both exterior test ranges, and using the communications links among those areas. The final product is validation or certification of a design at the system level. This category of testing is also within the capabilities of the proposed Laboratory, providing that scaled-down versions of the complete system can be adapted to the physical limits of the facilities.

2.1.1.3 Operational Testing. In this category, emphasis is placed on system performance, rather than purely technical aspects. It may also involve "human engineering" considerations. Some tests of this type are suitable for the proposed Laboratory, such as system response under peak loading conditions of multiple intrusion alarms, access requests per minute, etc. Tests of overall performance of full-scale systems are not within the proposed scope.

2.1.2 Test Categories. There is no absolute distinction between the categories of tests as described above. For example, "prototype testing" can be considered the ultimate form of "compatibility testing," and the measurement of device parameters is a major input to the process of determining compatibility. In fact, in terms of the laboratory test equipment requirements, it makes very little difference which types of tests are going to receive the greatest emphasis. All of the above types can be conducted, at least to some extent, with the test and support equipment identified in this document. The greatest constraint will be in the number of tests which can be performed concurrently, and mainly due to physical limitations of the facilities (indoors and outdoors). Although "operational testing" was discussed above as the category least suited to the proposed Laboratory, note that the equipment and expertise for such testing will be available in the proposed Laboratory, and a role may emerge for "deployable" support.

2.2 OVERVIEW.

2.2.1 Security System Concepts. The physical requirements for a testing laboratory, including test equipment and support equipment, and any associated test ranges, can best be defined by review of the characteristics and technologies of the various items which comprise a modern "electronic security system." The discussion which follows begins with an overview of such a system, primarily to describe relationships and interactions among major components. Following that overview, each of the major "sub-systems" (surveillance, intrusion detection, and access control) are dissected at a greater level of detail, and the pertinent features of each item are translated into laboratory or test range requirements.

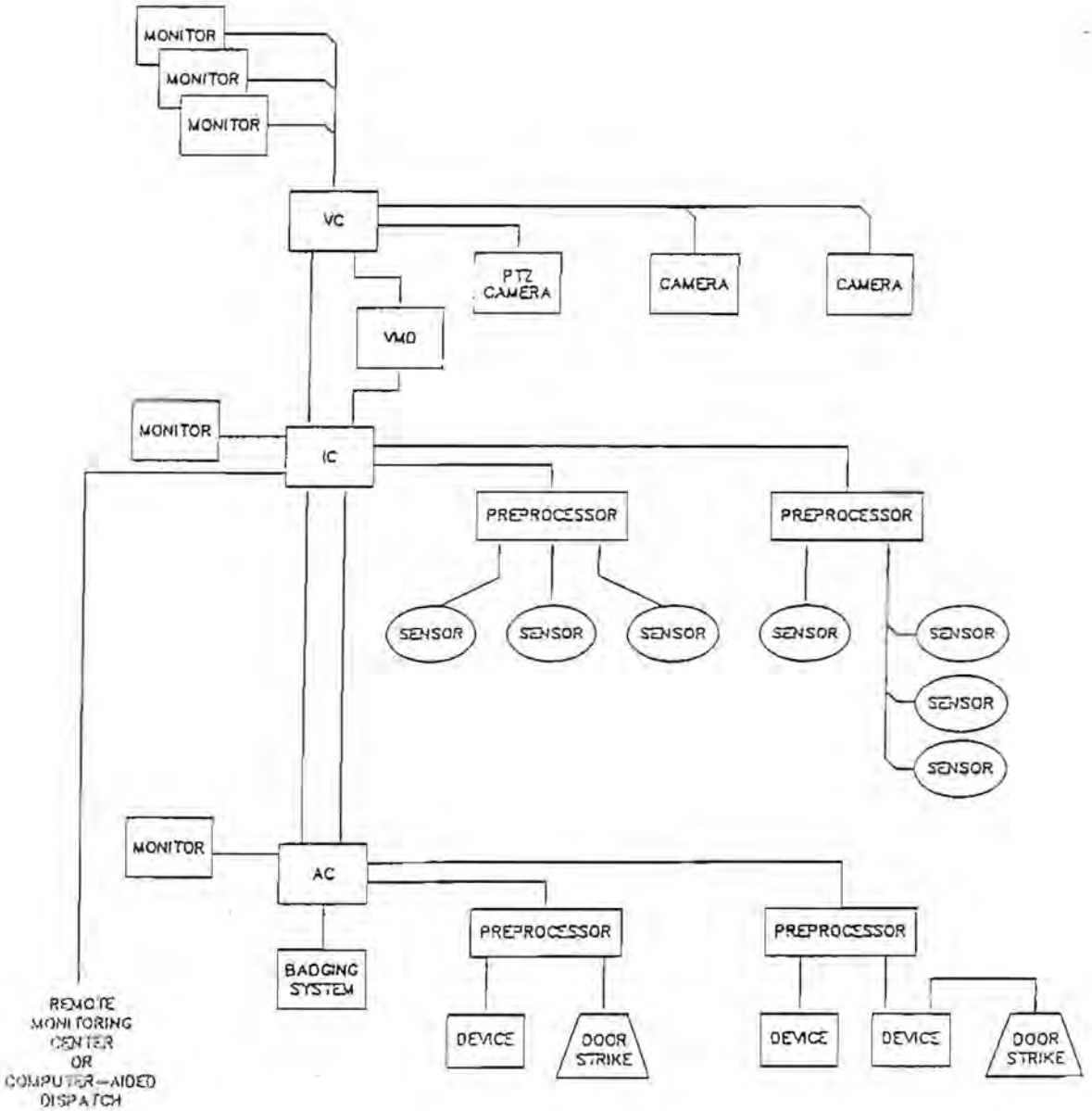
a. Figure 1 is a simplified block diagram of a modern security system, displayed according to the three major subsystems of surveillance, intrusion detection, and access control. Note that although all three subsystems are shown to support the related discussion, it is not necessary that all three subsystems actually be present in any specific real-world system. That is, any single "subsystem" could be independently employed, as could any combination of two "subsystems," depending on the anticipated threat, physical conditions, funding, and many other constraints. With advance planning, it is also reasonable to install a "complete" system in phases, so as to achieve the most urgent capabilities first (e.g., access control), then obtain the additional capabilities in a logical and responsible upgrade program. Regardless of how the final system is to be achieved, the desired objective is to have a fully integrated system which will provide the full spectrum of protection features while minimizing operational and maintenance costs. This requires that the subsystems be technically compatible, non-duplicative (unless planned redundancy is a requirement), and physically configured for efficient operations and maintenance.

b. As seen in Figure 1, each of the subsystems consist of a set of remote devices (sensors, cameras, card readers, etc.) at the locations to be monitored, data relay or concentration nodes, communications links, centralized processing and control equipment, and displays for presentation of events. The remote devices generally utilize specialized hardware unique to their function (infrared motion detectors, visible and/or infrared sensitive CCTV cameras, keypads, etc.). The respective data relay devices and communications linkages back to the central monitoring location generally also involve technologies and hardware unique to the respective subsystem. For example, the CCTV surveillance involves relatively wide bandwidth analog signaling, while an infrared motion detector may involve only a few bits of digital information to indicate a switch closure. Access control devices (such as card readers) tend to fall between those two extremes, with a requirement to exchange a moderate volume of data between the remote device and the central processing site. In most real-world systems, groups of similar devices will generally be connected to some form of intermediate "data concentrator" node which multiplexes or demultiplexes data, allowing for more economical use of fewer long data links back to the central monitoring site. In addition, the implementation of a large-area system (such as an airport) generally dictates that maximum use be made of physical paths and routes (cable trenches, etc.) so as to minimize the overall system installation costs.

c. A single physical path may contain fiber optic cables, coaxial cables, low- and high-speed digital data cables, twisted-pair copper (e.g., telephone lines), and various power cables (AC and/or DC), and interference among the various cables is always a concern. While fiber optic cables are relatively immune to most types of interference, they cannot be used to transmit power, and their total cost (including coupling and multiplexing devices) is currently higher than "copper" cabling.

At the central monitoring site, the various data and signals are "processed" in some manner, and routed to a display device or presented in some other fashion for operator action. Specifically, sub-system processing would include:

- Surveillance Subsystem
- Intrusion Detection Subsystem
- Access Control Subsystem



LEGEND:

VC = VIDEO SURVEILLANCE CONTROLLER

IC = INTRUSION DETECTION CONTROLLER

AC = ACCESS CONTROL CONTROLLER

Figure 1. Electronic Security System Conceptual Diagram

2.2.1.1 Surveillance Subsystem. In the case of CCTV surveillance, the "processing" phase may consist of nothing more than a video switcher, pre-programmed to connect each camera to a monitor in a fixed sequence. Conversely, the CCTV concept may involve switching of cameras/monitors in response to alarm events from the intrusion detection system, or in response to certain access control events from that system, and can become relatively complex. In its most sophisticated applications, a CCTV system may even involve the use of "pan-tilt-zoom" cameras controlled from the monitoring site, or the use of "video motion detectors" which sense changes in a fixed image, and automatically generate alarms in a manner exactly analogous to an intrusion detection device. In any event, there is likely to be an interaction between the "processing" device for the surveillance sub-system and the "processing" devices for the other sub-systems.

2.2.1.2 Intrusion Detection Subsystem. The "processing" device for the intrusion detection sub-system performs the overall function of monitoring the activity of the various remote sensors (including the connectivity and health status), and converting selected events into alarms. Generally, this requires a computer of the 80/386/486 class with a few specialized interfacing boards, one or more CRT monitors, a printer, and removable (floppy) and hard disks. The monitors may display either graphical depictions of the intrusion area, alpha-numeric messages, or both, depending on the manufacturer and software options. The printer and removable media provide long-term records of alarm and other activity. In addition to the primary function of generating intrusion alarms, the processor must also switch the various alarm "zones" or areas into "access" or "secure" modes, to permit authorized accesses without alarm conditions, and must regularly "poll" the sensors to be sure that they are in communications, and have not been subverted or failed. In all modern intrusion detection systems, the exchanges between the central computer and the remote devices and sensors is via digital data streams, consisting of device "addresses" and data bits for the various data items to be communicated. Modems are frequently required for communications over the typical lengths of lines required to cover a large area (e.g., an airport). The final major function of the processor (in some systems) is to transmit alerts or other messages to remote locations, such as guard posts. In the most sophisticated applications, this may even involve "computer-aided dispatching" (CAD), which is very selective in generating specific kinds of alerting messages in response to specified alarm events (including fire and medical alerts as appropriate). Intrusion detection systems frequently have an associated security communications system (i.e., a dedicated telephone system) which allows communications among authorized personnel and the central monitoring personnel, to activate/ deactivate alarm zones and coordinate emergency activities. In effect, these dedicated communications provide a very simple version of the third major type of sub-system, access control.

2.2.1.3 Access Control Subsystem. In its broadest sense, the access control sub-system not only provides a means of granting access to protected areas for authorized personnel, it may also provide an "audit trail" of ingress and egress activity which may be important in post facto investigation of the events surrounding a security breach or similar action. The primary purpose of the "processing" portion of the access control subsystem is to respond to access requests by granting or denying access, and keeping a record of such actions (who, when, ingress, egress, etc.). Certain kinds of activity may also be processed into an intrusion alarm, such as multiple denials of access within a short time period, attempts to use a stolen access card, etc. A computer (again of the 80x86 family or similar power) is required to process incoming requests from the remote devices (card readers, etc.), check the access requests against a stored data base, and respond accordingly (grant/deny/alarm). The computer generally must also monitor the communications and status of the remote devices to detect failure or subversion. In many access control systems, a portion of the data base may also be downloaded to an intermediate processor which services a subset of the access control devices, allowing for faster response to requests, and a moderate backup in case of failure of the communications back to the central processor. Although not a part of the "active" portion of the access control sub-system, Figure 1 also shows the existence of a "badging" workstation for the creation of access cards/badges, including pictures produced from video imaging or from photographs. The encoding of the badges, and the assignment of personal identification numbers ("PIN" numbers) are simultaneously entered into the access control processor data base when they are issued.

2.2.2 System Coupling. It should be clear from the foregoing discussions and from Figure 1 that there is considerable potential for interaction, at least at the "processing" level. In fact, it is entirely practical to combine some of the processing functions into a single computer, especially in the case of the intrusion detection and access control sub-systems. Sharing of the computer resources is generally more economical and operator-friendly, although at some cost in software complexity and processing speed. Other system resources are amenable to some degree of hardware sharing, such as printers, monitors and controls. Probably the most common instance is the use of a single computer to operate both the access control and the intrusion detection portions of the system, with CCTV video switching provided as an option, cued from the same computer.

Regardless of the specific system and the physical location, at the macro level, a modern security system consists of some mixture of "sensory" devices which react to physical events, a communications network which connects the "sensors" to a central control/processing location, and display/storage devices for interaction with the system operators.

Technological advances and competition within the industry will result in continual evolution in the makeup and performance of the specific hardware and software items, but this overall architecture is not likely to change significantly. For example, the availability of a new biometric technique for personnel recognition could result in changes in the specific hardware of the "sensors" in an access control system, but they would still be sensors communicating with a central processor via data links.

In terms of the implications for laboratory test equipment, there are actually very few concepts or technologies which are truly unique to security systems, at least at the theoretical level as presented in this section. The general requirements are for equipment capable of testing video equipment, microcomputers, and data networks, and a relatively small number of special-purpose electronic devices. In most cases, vendors of security systems adhere to applicable ANSI or other accepted standards.

Equipping of a laboratory becomes a matter of selecting appropriate "off-the-shelf" items based on the specific components known or expected to be tested. Specific devices and technologies employed in modern security systems are discussed in greater detail in the following sections, and specific test and support equipment is identified as appropriate for each type (surveillance, access control, intrusion detection). In addition, the concepts and equipments for data communications and RFI/EMI testing are addressed in the context of electronic security systems.

3. SURVEILLANCE SYSTEMS.

3.1 TECHNOLOGY AND DEVICES. In today's security systems, "surveillance" is virtually synonymous with "closed circuit television" (CCTV), so that the devices to be investigated in a laboratory are simply the available variants of CCTV technology.

3.1.1 Cameras. Although vidicon and similar camera tube technology is still available, newer systems employ solid state "charge-coupled device" (CCD) technology for greater resolution and reliability, and lower power requirements. CCD cameras are currently available with both coaxial cable and fiber optic video outputs. Exterior cameras are virtually always housed in weatherproof (and possibly heated) enclosures. Color cameras are substantially more expensive than monochrome, but provide higher operational performance when personal recognition is a requirement. CCD cameras are available with adequate response down into the infrared portion of the spectrum, and can be used with or without auxiliary infrared lighting. However, color fidelity of these cameras is greatly reduced when used with infrared, and with certain types of visible lighting (e.g., low-pressure sodium vapor lights).

3.1.2 Camera Employment. In many cases, surveillance needs can be met by a set of fixed-mount cameras, aimed and focussed on a specific area of interest, and no technology is involved. The same is true for cameras which repetitively sweep through a surveillance arc via some fixed motorized arrangement. The third employment method, however, is significantly more complex. This involves the use of remotely controlled "pan-tilt-zoom" (PTZ) cameras to enable the best possible scrutiny of an event within a relatively large surveillance area. In addition to the video signal and power wiring required with all cameras, PTZ cameras require a set of control lines, including position feedback signals. PTZ cameras may be "manually" controlled by means of a joystick, trackball, or similar device, operating through a translation device to convert hand movements into PTZ commands, and interpreting the position feedback information. The most sophisticated employment of PTZ cameras involves cuing the camera from an intrusion alarm. This requires that the intrusion detection software recognize which camera to activate, then direct it (in the PTZ sense) onto the specific alarm point within the given field of view. Finally, the software must insure that the video from the selected camera is routed to a monitor screen. Additional software functions may include activating more than one PTZ camera if the alarm point is visible to a second camera, activating a video tape recorder, and releasing the PTZ control to the operator for tracking/searching around the initial alarm point. Software of this nature obviously must be highly customized to the installation site.

3.1.3 Monitors. Standard CCTV monitors are used almost exclusively. Variants merely consist of monochrome/color, size of screen, and numbers of monitors versus number of cameras (see video switching paragraph below). Recently, however, at least one security system has been introduced which, in response to an intrusion alarm, and inserts a small video image onto the same screen which is used for intrusion detection functions. The live video can be monitored as desired, or a "frame grabbing" operation can be performed to retain the video image indefinitely. While this recent development is not likely to obviate the traditional bank of CCTV monitors, it is likely to be adopted by other vendors and come into more widespread use.

3.1.4 Video Switching. Except in those cases where every surveillance camera is permanently connected to its own monitor, some form of video switching is required. This may be nothing more than a time-based sequence which simply switches a single monitor from camera to camera, or may be a relatively complex operation involving many cameras and monitors, with manual control or cuing from intrusion detectors or access control devices. A frequent requirement is also for activation of a video cassette recorder (VCR) either in response to a programmed event, manual control, or at designated time intervals. Video switching technology generally involves solid-state switches, and careful designs to prevent feedthrough of stray signals. The higher quality video switchers also provide for switching in synchronism with the video frames, greatly reducing the tendency for a "vertical roll" after switching. Because of the normal interaction of the operators and/or other processors, video switchers are most commonly collocated with the associated monitors. This requires relatively large numbers of video signal lines to be homed to that location as well.

It is possible, however, to remote at least some of the switching equipment (i.e., for a "cluster" of cameras) and run a much smaller number of video lines back to the control and monitoring site. The trade-off is the requirement to run switcher control lines out to the switcher location(s).

3.1.5 Video Motion Detection. With the introduction of VMD technology, the traditional CCTV "surveillance" systems begin to evolve into automated "intrusion detection" systems. VMD devices operate by digitizing a frame of CCTV video and storing it in the digital memory of a microprocessor. At a later time (which may be only a few milliseconds) another video frame is digitized and compared on a bit-by-bit basis with the previous frame(s) in memory. The differences (if any) are processed through fairly sophisticated software algorithms, and result in alarms if programmed criteria are met. The algorithms must take into account the minor differences resulting from the digitizing process, as well as "allowable" differences such as the movement of objects due to wind/rain, etc. Increasingly complex algorithms look for certain object sizes, patterns of movement, speed, etc., in attempting to produce highly reliable detection with few false alarms. The employment of VMD systems is most useful in areas in which very little motion is expected (such as an

unoccupied indoor area). VMD technology is relatively new and still immature in the sense that the processors tend to be very expensive vis-a-vis their restricted utility, and the algorithms require expert "tuning" to the physical conditions of the installation site. However, VMD does offer a potential for augmenting and enhancing an existing CCTV surveillance system at very low cost compared to installation of a complete parallel intrusion detection system. Technological advances are likely to increase the use of VMD devices.

3.1.6 Video Data Lines. Both coaxial cables and fiber optic cables are routinely used for transmitting the camera video to the monitor location. Many vendors offer cameras with both types of outputs, and video switchers are available for both types. Matching of the fibers to the terminating equipment is somewhat more critical than with coaxial cables, and specifications at both ends need to be observed. While fiber optic systems offer the advantage of compact size and immunity to electromagnetic interference, they are currently more costly than copper cables, and copper cables can sometimes be used to also send operating power to a remote device (viz., a camera).

3.2 TESTING REQUIREMENTS AND EQUIPMENT

3.2.1 Cameras. Testing could reasonably include camera operational performance under various lighting levels (and spectral contents if artificial illumination is to be used), to include performance in the infrared region if required by the intended employment. There are no known objective tests or equipment, however; "testing" of this nature would be primarily subjective viewing on a monitor. Another important test would be of environmental housings for exterior surveillance systems, to determine limits of operation under extremes of temperature and humidity. The environmental chambers required for such testing are considered beyond the intended scope of the proposed laboratory, however, and are not included in the equipment or support facility listings. If such tests are to be performed, the cost-effective alternative is to rent the use of environmental chamber(s) as required. Camera resolution may also be a subject of interest, for example when positive personnel recognition is required.

3.2.2 Camera Employment. PTZ cameras can be tested in both a technical and an operational sense. The electromechanical aspects of the system can be tested for accuracy, speed, and precision of control, repeatability, and other such technical characteristics. These tests require a suitable camera mount (i.e., at a typical elevated position at least 20 feet high), and "targets" placed at various angles and distances from the camera mount. Testing would then involve use of the manual and/or computer controlled PTZ operations, and observation of results on a monitor. In the case of computer-controlled positioning, the computer software is also involved in any such tests, and it may be important to analyze the actual command data leaving the computer, and the feedback data returning from the camera, to determine where and problems are originating. This will require a data analyzer with the proper adapters (RS-232, RS-485, etc) for the data protocols of the equipment under test.

3.2.3 Video Motion Detectors. Given the relative immaturity of VMD technology, testing of these devices is likely to be of very high interest if they are being considered for general usage. However, no special test equipment is involved, other than perhaps an oscilloscope to determine the quality of input video and a noise source to determine the effects of poor quality signals. Testing would be of an operational nature, such as minimum size and speed of detected objects, ability to adapt to various weather conditions, etc., and these tests are tests of the processing algorithms, rather than of hardware. Although some user adjustments and functional programming are necessary, it is highly unlikely that the VMD manufacturer will release any of the processing software for investigation, and may request to be present for any significant testing periods.

3.2.4 Video Switchers. Other than correct switching operations, the major tests would be of "crosstalk" between outputs. This can be measured using a video signal generator (or other video source including a live camera) and an oscilloscope. Synchronized switching can be tested by observing the absence/presence of vertical roll on the monitor when switching between video sources.

3.2.5 Monitors. Very little useful testing can be performed. One item of interest would be the time required for the display to stabilize after a switching operation (also a function of the video switcher technology). No equipment is required; direct observation will suffice. A second item would be EMI/RFI generation, and investigation of the Extremely Low Frequency (ELF) radiation which is postulated to have long-term health implications for the operators. These phenomenon can be measured with a spectrum analyzer and an ELF sensor, respectively.

4. INTRUSION DETECTION SYSTEMS.

4.1 TECHNOLOGIES AND DEVICES. Intrusion Detection Systems (IDS) depend on a physical phenomenon, detected by one or more "sensors," with the outputs of the sensors transmitted to a centralized processing and display location. The technology involved in these "sensors" ranges from physical movements or stresses of objects, to sonic, ultrasonic, radio-frequency, microwave, and infrared spectra. Regardless of the phenomenon, however, most intrusion detection sensors eventually act very much like a switch closure. That is, after some specialized amplification, filtering, or other processing of a transducer signal, the final "output" of the sensor device is an "off-on" transition, indicating an intrusion. In most applications, the sensor devices contain "tamper" detectors (such as switches inside the device covers) which also report as switch closures when any attempt is made to subvert them. Since most IDS systems have many sensor devices communicating via a data bus architecture, each device must also be identified to the central processor with an unique "address" word along with the alarm signal. The central processor also routinely "polls" the sensors, to determine if they are still in communications and are functioning.

Intermediate processors are used in most systems to service a number of collocated sensors, allowing them to share the long-haul communications path back to the central monitoring site. These intermediate processors usually also provide a limited range of functions (such as absolute device "address" decoding), to offload a portion of the processing workload from the central processor. Various communications media can be used for the communications links, including twisted pair, coaxial, and fiber optic cables, and radio/microwave links. At the central monitoring location, one or more computers process the sensor data into information to be displayed, most commonly on a computer monitor screen, using alpha-numeric and/or graphical displays. The computer also controls the operating modes of the IDS, such as putting selected zones into an "access" condition to allow greater access during normal working hours. As discussed in the section on surveillance systems, the IDS computer may also control some portions of a CCTV system, giving the operators an immediate view of any alarm point. The IDS computer may also interact (or be physically integrated with) the central computer of an access control system. As far as laboratory testing is concerned, the greatest interest is in the "sensor" portion of the IDS, and the bulk of this section discusses those requirements. Only the test equipment or support items unique to the particular sensor type are identified in the respective sections; other equipment requirements are those shown in the "general-purpose" section.

4.2 INTERIOR SENSORS.

4.2.1 Door and Window Sensors. These devices detect the opening of a door or window. They most commonly consist of magnetically-operated switches, with the magnet on the moving item, and the switch on the frame. Tests of these devices involve measurement of alignment accuracies which may be required, and amount of movement required to set off the alarm condition. **Unique equipment: none.**

4.2.2 Glass Break Detectors. These consist of a microphone, amplifier, and audio filter circuitry which can be tuned for the characteristic sounds of breaking windows. **Unique equipment: a special noisemaker** is available from the manufacturers of these devices, to be used to test or adjust the sensitivity.

4.2.3 Passive Infrared (PIR) Detectors. These devices all operate on the principle of detecting the changes in infrared radiations emitted by all warm objects, the human body in particular, and responding to changes in the received radiations. They are, of course, most useful in environments which do not involve moving machinery or other heat-generating objects. They are available in a large variety of patterns of sensitivity, including omni-directional, fan, conical and multiple beams, etc. The sensitivity patterns are generally produced by lenses inserted into the device cover, with the device then being mounted at heights and angles appropriate for the area to be covered. Effective range depends on the sensitivity patterns to some extent, as well as on any "background" radiations, and can range up to about 100 feet. The sophistication of these devices has progressed from very simple detection of infrared intensity, to multiple beam processing, whereby two or more adjacent beams must each report radiation within a programmed time frame before an alarm is generated. Even so, and especially in a "warm" environment, false alarms and sensor sensitivity will be items of interest and worthy of investigation. In this case, the only known useful "target" to be used is a human, since there are no test devices which simulate the characteristic IR emissions of people. Since they are generally intended for indoor use, PIR sensors can easily be tested in a laboratory environment. They are mounted on a wall or from an overhead fixture as appropriate for their sensitivity pattern, while a "target" person moves about the room. **Unique equipment: none.**

4.2.4 Ultrasonic Sensors. These devices are, in effect, "radar" systems which operate in the ultrasonic spectrum, generally around 40 Khz. A transmitter "illuminates" the area to be covered, and reflected waves are received and processed. Either changes in the intensity of the reflected waves, or frequency changes (due to doppler effects) are processed into alarms. These systems are useful only in relatively small areas (i.e., rooms) which will be unoccupied and have absolutely no moving items when secured. **Unique equipment: none.**

4.3 FENCE SENSORS. This category of intrusion detectors consists of devices which are used in conjunction with, or are an integral part of, perimeter protection systems for relatively large outdoor areas (e.g., an entire airport.) In most cases, they provide both a physical deterrent and an alarm system which indicates the general or specific location of an intrusion attempt.

4.3.1 Taut-Wire Types. Used as a free-standing system, or in conjunction with an existing fence, taut-wire systems combine a physical barrier (barbed wire) with an intrusion detection system by means of tension or movement sensors mounted on the fence posts and attached to the fence wires. Any significant change in the wire tension (due to cutting, climbing, separating, etc.) results in an alarm. The "sensor" itself generally consists of a flexible resistance element physically coupled to the wire(s) and to an amplifier-processor circuit to convert resistance changes into typical "switch closure" information for the central processor. Along the fence runs, the sensor posts detect both "left" and "right" tension changes; in normal operation, two adjacent sensor posts will detect the intrusion, one reporting "left" and the other reporting "right." The two detections together serve to localize the intrusion to the fence segment between the two reporting posts, so that each fence segment is treated as an independent alarm "zone." The exact nature of the sensor element, its method of coupling to the fence wires, and the electronics of the post processor, are proprietary to the manufacturers. The processors (a circuit card containing integrated and discrete electronic circuits) generally has adjustments for sensitivity. They may also contain circuitry for compensating for changes in wire tension due to ambient temperature changes. The individual fence wires also require careful and relatively precise tension settings at the actual installation location. The user of the fence may specify several fence parameters, such as wire deflection (e.g., inches) which will create an alarm, force required to deflect a wire by a given amount, spacing of sensor posts, etc. The rigidity of the sensor posts, intermediate posts, and ending or anchor posts is a major factor in long-term stability in fence performance. **The large number of variable factors results in a significant requirement for testing and experimentation for such fences.** The major areas of investigation include the interaction between wire tension and tension changes (deflections) which result in alarms, correct "left/right" reporting, correct adjacent post reporting, and the effects of ambient temperature changes. **Unique equipment: torque wrenches, strain gauges, spring scales, thermometers. An outdoor test range will also be required, suitable for construction of test fences, to include corners and end posts.**

4.3.2 Fence Movement Sensors. Several types of sensors may be added to conventional fences (i.e., chain link fences) to detect movement due to cutting, climbing, jacking, etc. These sensors generally depend on either an "acoustic" effect involving audio-frequency vibrations, inertial masses which translate fence motion into switch closures, or distributed strain sensors which sense strain changes in an cable attached to the fencing. Each of these sensor types involves proprietary or unique methods of physical attachment of the sensors to the fence fabric, and specialized signal processors to translate the detected phenomenon into the typical "switch closures" indicating an alarm. Adjustments of both the mechanical and electronic elements are required, although the mechanical aspects are much less critical than in the case of the taut-wire fencing discussed previously. Another factor of importance, however, is the effects of wind and other weather variables, particularly since the chain-link fences have a much greater "sail area" than do taut-wire fences, and tend to move more. Fence fabric tension is a major factor for the same reason. At least one major manufacturer of these sensors has an on-going research program for computer algorithms to increase the

processing of the sensor outputs, so as to recognize the patterns associated with wind, rain, and other effects, and reduce the false alarm rates. For the "acoustic" type of sensors, ambient noises typical of airports/runways may be an important factor requiring investigation in depth and on site. **Unique equipment requirements: none. An outdoor range is required, possibly making use of an existing "conventional" fence.**

Testing in a runway environment is almost mandatory for the acoustic-effect sensors; a spectrum analyzer is required, suitable for use in the sonic-ultrasonic range.

4.3.3 Electrical Field and Capacitance Fences. These fences involve the use of a set of insulated wires run along the desired fence line. With no disturbances, the electric fields emitted from these wires is sensed by other parallel wires, or in reference to a ground screen. An intruder causes a field disturbance which is sensed as either a field strength or a capacitive reactance change, and processed into an alarm condition. These fences are not "electric fences" in the sense of producing painful or lethal electrical shocks; the voltage levels are much too low, and are not intended as deterrents. When a physical barrier is desired, these fences must be used in conjunction with other fences (chain link, etc.). Variables and subjects for testing include the adjustments of sensitivity for intruder size (including small animals, etc.), proximity of intruder to fence, weather effects (especially snow and rain), and sensor/ground screen wire number and spacing. EMI/RFI generation and susceptibility should also be tested, especially for an airport environment. **Unique equipment: none.**

4.4 FREE-STANDING SENSORS. Unlike the "fence" sensor systems previously described, this category of perimeter protection systems provides for intrusion detection only, without physical deterrence. These systems employ physical devices which may result in "psychological" deterrence, while others are completely concealed, and provide covert detections of intrusion across a perimeter. (The concealed types can be used in conjunction with a fence so as to provide overt physical protection and covert intrusion detection.)

4.4.1 Buried Line Sensors. This covert system uses two buried, specially-constructed, coaxial cables, in parallel along a perimeter. One cable, referred to as the "transmit" cable, emits a weak radio-frequency signal which is received by the parallel "receive" cable a few feet away. After installation, the system is adjusted for a specific received signal level. Any object which crosses the strip between the two cables will then cause a change in the received signal level which can be processed into an alarm. The cable pairs function as individual segments of the perimeter, with intrusions localized only to a specific segment. The manufacturers provide information on recommended depth and separation of cables, minimum and maximum lengths for individual cable runs, and system adjustments. Testing requirements involve verification of object detection for a given physical arrangement (ideally conducted with the same soil types for the intended installation site), the effects of rain/snow

and soil dampness, and long-term stability of adjustments. These are only reasonably tested in an outdoor environment, and over a protracted period. Since these devices involve the emission and reception of radio-frequency energy, EMI/RFI generation and susceptibility are also of concern, and may be problems in an airport environment, due to radars and communications equipment. **Unique equipment: Ground resistance and/or soil moisture content meters.**

4.4.2 Bistatic Microwave. Infrared and Laser Systems: These types of intrusion detectors use highly directive beams of energy from a transmitting device, along the protected perimeter, to a receiving device. Disruption of the beam indicates an intrusion. The transmitting and receiving devices (and the beams in the case of lasers) are visible to any potential intruder. The infrared and laser systems make use of relatively small beamwidths, and may be used in multiple-beam arrays, similar to the parallel wires of a taut-wire fence. Microwave system beamwidths tend to be in the range of a few degrees, and employed as a single (or perhaps dual) beam system. In all cases, the received energy is amplified and processed, and changes in amplitude above an adjustable threshold are interpreted as alarms, typically as "switch closures." Factors for investigation include beam alignment accuracy, beamwidth for detections, maximum/minimum ranges, and susceptibility to precipitation. EMI/RFI generation and susceptibility is an obvious additional concern for microwave systems. **Unique equipment: none.**

4.4.3 Monostatic Microwave. These systems are based on the use of collocated transmitting and receiving antennas, with the energy reflected from an object giving rise to the alarm. These systems tend to be "volumetric" sensors rather than "linear" or perimeter sensors. That is, they can be employed for detections in a relatively small 3-dimensional space, such as the approach to a parked aircraft, a gate or other access point, etc., and may also be used indoors. Portable systems of this technology are particularly suitable for temporary use or enhancement of existing systems. In some instances, the equipment must be "tuned" to the specific reflection conditions of the employment location (walls, gates, fences, etc.), and sensitivity adjustments made on site. Areas of possible investigation include system performance in confined areas or areas of high reflectivity, versus totally open areas, and effects of precipitation if outdoor use is planned. RFI and EMI are concerns as with most other radio-frequency devices. **Unique equipment: none.**

4.4.4 Fiber Optic Detectors. A relatively new technology involves the use of long loops of fiber optic cables, driven by a laser source, and using optical interferometry techniques to detect changes in the phase and amplitude of the light as propagated through the loop. Even minute changes in the fiber optic path, due to pressure or other stresses, will result in a change in the returning light wave which can be processed into an alarm. Only a single manufacturer is known for this patented technology, originally developed at the Sandia National Laboratory. That manufacturer claims to obtain excellent detection performance

over fiber runs as great as 30 kilometers, and an enhanced processing technique which can locate the source of the intrusion down to a few meters. Although the prime application would appear to be in the protection of long outdoor perimeters, the technology is also applicable to indoor uses. In either case, the manufacturer claims sensitivity adequate to even detect voices (at maximum gain), induced through the acoustic waves striking an exposed fiber cable. Testing of this new technology would involve range of sensitivity adjustments, ability to discriminate among various types of intrusion sources (vehicles, footfalls, etc.), maximum/minimum loop lengths, effects of precipitation, and depth of burial in various soils. Accuracy of intrusion location should also be verified, for both the standard and enhanced versions. RFI and EMI are probably not important factors. **Unique equipment: none known.**

4.4.5 Other Devices/Sensors. There are a number of devices which involve the breaking of fiber optic or the breaking or stressing of electrical cables imbedded in a protected structure such as a screen across a culvert. Although these systems generally contain some form of specialized "processing" circuitry which depends on the phenomenon involved, virtually all such systems ultimately produce a "switch closure" output which indicates the alarm condition. There are no known unique requirements for test equipment.

5. ACCESS CONTROL SYSTEMS.

5.1 PURPOSE. The primary purpose of an access control system is to allow authorized personnel to gain access to selected areas while rejecting unauthorized personnel. The types of devices (such as card readers), and the processing equipment which grants/denies access, can also be used for related purposes such as "audit trails" of persons who have accessed an area, real-time displays of numbers or identities of persons currently in an area, and alarms if entry attempts are made by unauthorized personnel. In most modern access control systems, the persons requesting access must interact with a device (keypad, card reader, etc.) in a way which is recognized by a system computer; the computer processes the access request by checking the entered information against a data base, and grants or denies access. Thus, a necessary adjunct to the access control system is a means of "registering" authorized personnel, frequently including the physical assembly of access cards and badges. Access control systems are frequently integrated with intrusion detection systems, allowing the central processor to perform both functions. Even if installed as separate systems, there is usually an interaction between the central processors, at least to the extent that improper access attempts are reported as alarms.

5.2 SYSTEM ARCHITECTURE. The system architecture of access control systems is similar to that of intrusion detection systems, and not highly dependent on the nature of the access control devices themselves. The nature of this system architecture is sets of access control devices (e.g., card readers) connected to nearby "intermediate processors," with several of those intermediate processors connected, in turn, to a central processor. The numbers and mixes of devices, and the amount and exact nature of the intermediate processing, is dependent on the manufacturer and, the geometry of the installation site itself. All access control systems depend on matching input data from the entry device against a data base of authorized personnel. In modern systems, the data base is distributed to some extent among the central processor, one or more intermediate processors, and the entry devices themselves. That is, a single card reader may contain enough stored data to grant access to those personnel who normally use that access point without reference to a data base at the next level in the hierarchy (i.e., an intermediate processor). Most types of access control devices contain at least a microcontroller and RAM/ROM circuits, in addition to the signal processors which are required for the detection of the access request (reading a magnetic strip on a card, etc). Card reader devices are currently available which are capable of storing authorization data for 8000 personnel, and approach the computational power of an 8086 microcomputer. Similarly, at the intermediate processor level, 80286 processor power is available, and data storage for hundreds of thousands of users. This system architecture and distribution of processing power is employed for the sake of speed of access, minimizing the data transfer requirements among the various components, and allowing at least a limited continuation of the access control function if communications are lost with the central computer. The decision power inherent in each component becomes significant, also, in systems which are subjected to very high peak demand during "shift changes," when hundreds of access requests may occur in a few minutes. Furthermore, when the access

control system is integrated with an intrusion detection system, it is important that intrusion events not be delayed while the central computer is processing routine access requests. The processing and memory distribution is a highly competitive area of development, and can be expected to continue to evolve along with computer technology.

Depending on the operational requirements, access control devices may also be required to exit an area. This occurs most commonly when a continuous audit trail is required so that persons present in an area at a certain time can be retrieved in reconstruction of some event. Exactly the same types of control devices can be used for exit control.

Every access control operation normally terminates with the activation of some mechanism which releases the door or gate at the entry point. This may be accomplished by the access device itself (i.e., card reader), or by the intermediate processor. One of the most common mechanisms is a "door strike," affixed to the door frame. A signal from the controller closes a switch, activating a solenoid, and releasing the lock mechanism.

The overall performance of an access control system is highly dependent on the adequacy of the data networks which interconnect the system components.

5.3 TECHNOLOGIES AND DEVICES.

5.3.1 Magnetic Cards and Readers. Whether supplied as "wallet-type" cards, or as badges to be worn on site, magnetic-strip cards and their associated readers are possibly the most common form of automated access control. With the current state of the art, approximately 50 bits of information can be encoded in the magnetic strip, enough to identify the registered owner and site-unique information on access levels. In most systems, the card reader performs the functions of reading the strip, comparing the information with some amount of internally-stored data, and either requesting further information from a higher-level data base or triggering a release mechanism for the access point (door, gate, etc.). In most systems, even if local data storage is adequate to permit the access decisions, access events (personnel identities) may still be recorded and relayed to the central processor for a permanent record of who gained or attempted access and at what times. In terms of technical testing, there are **no unique equipment** requirements for card readers themselves. For overall evaluation of a particular manufacturer's equipment, however, it may be very useful to conduct response time tests and other load-related tests of a prototype system. In most cases, this will require computer simulation of hundreds or thousands of access events, with the results accumulated by a computer and tabulated for human review. Such tests can be conducted by the access control computer itself, with vendor-supplied programs, or software written by the laboratory staff.

5.3.2 Proximity Cards. Unlike the magnetic-strip cards which must be physically "swiped" through a reader to pick off the coded information, proximity cards need only be brought "near" the "reader." These type cards contain microelectronic circuits which emit a response when illuminated by a matching radio frequency transmission. The "reader" for these cards consists of a low-powered RF transmitter of the appropriate frequency and a receiver to pick up the card emissions. The effective range is dependent on the exact technology used by the manufacturer, but is especially dependent on the size and power of the transmitter portion of the "reader." common ranges are from a few inches to several feet. In the latter case, it is not even necessary to visually expose the card--it may be concealed in a pocket or even inside a wallet--and the user need only approach the access point and be granted access with no overt action whatsoever. As in the case of magnetic strip cards, there are several possible architectures for supporting the reader functions of data base look-up, door strike control, communications with an intermediate or central processor, etc., and the discussion in that section pertains. However, in terms of testing, proximity card readers are dependent on the emission and reception of radio-frequency energy, and **EMI/RFI testing is appropriate.**

5.3.3 Biometric Devices. A variety of devices have been invented which make use of some unique biological feature of individuals to grant/deny access. These techniques include eye retina pattern recognition, fingerprints, hand geometry (ratio of finger lengths, etc.) and voice recognition. The obvious advantage of biometric systems is the elimination of cards or other devices which can be lost, stolen, or simply forgotten; the authorized person simply presents him/her self at the access point. To date, however, these systems have not been shown to have extreme reliability, or are relatively slow or awkward to use. It is likely that such systems will be improved in those regards, and be adopted for more widespread use. Again, the preceding discussion of data storage, intermediate and central processors, etc., pertains; the exact nature of the user-recognition operation does not alter the basic architectural concepts. Other than functional testing through repeated access requests, there are no known testing requirements and **no special equipment is required.**

5.3.4 Keypads. Similar in concept and appearance to a "touch-tone" telephone or a calculator, keypads may be used for access control, either alone, or with a device such as a card reader. The person requesting access "keys in" an unique set of numbers or letters; the entries are compared with a data base and access granted or denied. Each authorized person is normally assigned an unique "personal identification number" (PIN). The combination of keypads and card readers provides a high degree of protection against the misuse of lost or stolen cards. Since keypads immediately produce a digital data stream, no special sensors (such as magnetic read heads) are involved, and keypads are relatively simple to integrate into an access control system. **No unique test equipment is required,** other than the ability to analyze the data stream back to a processing device.

5.3.5 Cipher Locks. These are the electrical equivalent of mechanical combination locks. The user simply presses a number of key switches in the correct sequence, and access is granted. Cipher locks are considered very low security devices, and are not integrated into modern access control systems. They do have a limited application in preventing casual and unrestricted access to selected areas. **No unique equipment is required.**

6. DATA AND COMMUNICATIONS.

6.1 COMMUNICATION LINES. Electronic security systems (surveillance, intrusion detection, and access control) have a common general architecture of centralized processing equipment, and components which are distributed over a relatively large geographic area. Thus, the requirement for communications circuits is inherent and critical to all systems. Communications media can be any of the appropriate technologies, including single wire, twisted-pair, coaxial cables, fiber optic cables, and radio/microwave.

Actual telephone lines are frequently used, as are "dry lines" which are provided by a telephone company but which do not have the dial/ring functions. In-line repeaters and buffers may be required in long runs, and multiplexers/demultiplexers may be used to make more efficient use of available bandwidths.

The surveillance systems, normally employing CCTV cameras, require relatively wideband analog video circuits, and are unidirectional (i.e., from the cameras to the monitors) unless camera positioning controls are involved. Fiber optic cables and coaxial cables are the only physical media which provide the requisite bandwidths for runs of more than a few feet. Microwave systems are also suitable where cabling is not practical or is too expensive. (Frequency allocation constraints and bandwidth requirements virtually preclude the use of VHF or UHF radio.) On the other hand, intrusion detection and access control systems have requirements for digital, medium-speed, bi-directional data links. The bi-directional requirement arises from the need for polling of sensors, setting of "secure" and "access" modes, verification of functional conditions, downloading of access authorization data, and similar operations which originate in the central computer. Between the central computer and the usual intermediate processors, data exchanges are of a computer-to-computer nature, most commonly in 8-bit bytes. Proprietary bit, character, and frame definitions are the rule rather than the exception, although ASCII and other standardized formats are used by some manufacturers. RS-232 and RS-485 are the dominant signalling levels, probably because of the wide availability of ancillary equipment such as modems which adhere to those standards. In access control systems, there may also be a significant "computer-to-computer" data exchange as, for example, when access data base information is further downloaded to a card reader. In intrusion detection systems, the data exchanges between a sensor and an intermediate processor is most commonly in the form of simple binary off-on ("switch closure") information, with a correspondingly very low effective data rate. Many different physical media and radio/microwave systems can be used for the various data requirements. Modems are almost always required between intermediate processors and the central computers, and may be required between access control devices and their intermediate processors, depending on site geometry. Modems are virtually never required between intrusion detection sensors and intermediate processors since the data rate is so low.

6.2 COMMUNICATIONS TESTING. Although some of the equipment requirements turn out to be the same, it is important to distinguish between technical tests of laboratory hardware, and tests of a full-scale, real, system. This is because in communications testing, the actual path length and media will determine propagation times, signal attenuation and distortion, noise susceptibility and similar factors which determine the ultimate quality of the circuit. Some types of tests will then require representative path and media to be used, such as testing via thousands of feet of cable. In a laboratory, this can be simulated with good accuracy by using cables on reel, with both cable ends brought out. For tests which involve radio media, however, laboratory tests (using greatly reduced power, etc.) are a poor substitute for free space testing. Likewise, equipment which is used for testing fiber optic splices is almost essential to test the splices which will be found necessary in the course of using fiber optic cables, but the testing of a specific splice on a specific jumper used in the laboratory will reveal nothing about how well another specific splice will perform when installed in an operating system. Attenuation or insulation resistance tests on copper cables suffer from the same general problem; such tests need to be performed on cable to be used in the laboratory, but those tests say almost nothing about the very next reel of the same type of cable from the same manufacturer. On the other hand, some types of communications tests are highly suitable for laboratory testing, and the results can be generalized in terms of "real" system performances. Examples would be the testing of handshaking and data rate compatibility between a processor and modem(s) proposed for a particular application, or analyzing the data words exchanged between a card reader and an intermediate processor during various functions.

6.3 TEST EQUIPMENT. Communications equipment and devices testing requires the following:

a. OTDR;
b. Data Analyzer;
c. Bit Pattern Generator (if not in data analyzer);
d. Portable video monitor; and
e. Spectrum analyzer.

It will be found necessary to assemble a wide variety of cables and connectors, both metallic and fiber optic. Tools and materials include:

a. splice kits;
b. BNC and type "N" connectors; and
c. fiber optic splicing tools (Camsplice, etc....).

7. EMI/RFI TESTING.

7.1 INTERFERENCE. The continuous growth in the use of electronic and electrical equipment has resulted in a continuous growth in problems which are generally categorized under the headings of "electromagnetic interference" (EMI) or "radio frequency interference" (RFI). Although "RFI" can properly be considered a category of "EMI," in common usage, RFI is used when discussing problems arising from devices which intentionally emit radio-frequency signals, while EMI is most often used in the case of unintentional radiations, especially radiations below the ordinary radio-frequency range beginning around 300 khz. This document will follow that common usage. This document also briefly covers a very closely-related topic of growing concern, that of power line anomalies (surges, spikes, brownouts, etc.) which can be especially harmful to equipment which uses microprocessors and other integrated circuits. There is an enormous body of literature on these topics, as well as a multitude of regulations and standards which apply under varied conditions. Even a brief summary would be beyond the scope of this document. The emphasis here is on the testing appropriate to the "bottom line" of EMI and RFI efforts: to insure that new equipment introduced does not introduce interference to existing equipment, and that existing equipment will not interfere with the new. Respectively, these two objectives require testing for EMI/RFI generation and susceptibility. (The section on susceptibility also treats the power-line anomaly topic.)

7.2 EMI/RFI GENERATION. Airports make extensive use of radio and electronic equipment, from radios used by security, flightline, taxi, and airline employees, to aircraft and control tower radios, to radars and ranging equipment. They are also frequently located in urban areas which also make extensive use of all available spectrum space. Any electronic security system which intentionally or unintentionally emits signals has a potential for generating EMI and RFI to the existing systems. It is fortunate in that sense that electronic security systems employ relatively few intentional emitters, and unintentional emissions (from properly adjusted equipment) are not usually a source of problems.

The possible intentional emitters include RF and microwave data links, microwave intrusion detection sensors, buried line intrusion detection systems, and proximity card readers. The primary area of investigation of these systems involves the determination that they are actually emitting within their intended frequency range and power. If so, then RFI considerations devolve into the issue of "electromagnetic compatibility" (EMC), or the compatibility of those types of emissions with the existing environment, and generally is a part of the frequency allocation process for obtaining permission to use the systems.

The unintentional emitters potentially involve virtually every active electronic device in the security system. These range from extremely low frequency (ELF) radiations from computer and CCTV monitors, to broadband noise generated by digital integrated circuit components, to electromagnetic pulses from the solenoids which operate door strikes. Spurious radiations are also possible from malfunction or misadjustment of intentional emitters such as radio data

links. Note that ELF radiations, from computer monitors in particular, has become a controversial subject in terms of possible health effects on the operators, and could become the subject of new OSHA (etc.) standards.

Test Equipment for EMI/RFI generation: A spectrum analyzer is indispensable, equipped with appropriate antennas and probes. Signal generators will be required, covering the various frequency ranges and power levels. Specialized devices to measure ELF radiations have recently appeared, and are identified in the equipment lists.

7.3 EMI/RFI SUSCEPTIBILITY. Since any new electronic security system will be "inserted" into an environment which is rich in emissions, and the susceptibility of the new equipment can be an important factor in its operational performance. Since the environment of any specific airport cannot be predicted well in advance, and could only be accurately determined by an instrumented EMI/RFI survey, the role of the laboratory becomes that of testing representative devices to document their susceptibility to interference. This information can then be used to predict potential problems when those devices are candidates for real-world installations. As in the case of the investigation of EMI/RFI generation, some distinction is necessary between tests of devices which are intended to receive electromagnetic signals and those which are not.

All of the devices which depend on the reception of signals for their operation (radio data links, microwave detection systems, etc.) will have some form of antenna and radio receiver front end. In terms of EMI/RFI, these are the most vulnerable portions of the system, and the focus of testing. The major items are antenna beamwidth and bandwidth, and receiver bandwidth and intermodulation characteristics. While an anechoic chamber or a shielded room would be necessary for extremely pure testing, much practical testing can be conducted in the proposed laboratory facility and/or the proposed test ranges described elsewhere in this document. (On those occasions when more exacting test conditions might be considered necessary, rental of the use of an anechoic chamber would be the cost-effective alternative.) In the laboratory, a spectrum analyzer may be used to determine if the device under test is being subjected to significant signals other than those intended by the testing process. The testing requires the set-up of the devices in a geometry appropriate for the device (either in the laboratory or on a range), and illuminating them with appropriate frequencies and power levels while observing the results.

Most of the active devices in a security system will also have some degree of susceptibility to EMI/RFI, particularly if connected to any wiring which can act as an antenna and couple signals into electronic circuits. The most common of these "inadvertent antennas" are communications lines and power lines. The pertinent technologies of shielding, grounding, bonding, and filtering provide the solutions to most such problems. The devices themselves (card readers, etc.) can be susceptible to direct interference, particularly if used near a high-powered emitter such as a radar or radio transmitter site. Practical tests for many such susceptibilities may be conducted in a laboratory or test range. The procedures are virtually

identical to those outlined for "intentional" devices, in terms of geometry and illumination with appropriate signals. It may be necessary to simulate high-power emitters by very close coupling to the device under test, removing any metallic case, etc.

Power line anomalies include "sags" (lowered line voltage lasting for up to a few seconds), "surges" (increased voltage lasting up to a few seconds), "spikes" (very high voltage transients lasting a few microseconds), "dropouts" (total or near-total loss of voltage), and "brownouts" (frequently caused by loss of one phase of a multi-phase line). The sources and causes of these anomalies can range from nearby electrical equipment (motor starting power demands, etc.) to totally unpredictable occurrences in the power grid hundreds of miles away. The effects on security systems can range from very temporary anomalies (such as false alarms) to destruction of computer circuitry or data bases, to total loss of a system which does not have battery or generator backup. The central computer and monitoring complex for a security system virtually demands the provision of an "uninterruptable power system" (UPS), which will at least maintain operations for a few minutes when power is lost. Battery back-up of the "remote" components of the system are also usually necessary, unless powered by lines originating from the UPS-protected central complex. Most UPS systems provide a reasonable amount of filtering protection against spikes and surges, as well as providing the power during total loss of the feeder lines. Stand-alone filters may also be used, with or without an UPS. Although this area is one of great concern for the real-world operation of security systems, there is relatively little practical laboratory testing opportunity. The most reasonable of those would be in observing the purity of output of candidate UPS and power line filters. **Test Equipment for susceptibility: Again, a spectrum analyzer is the major required instrument, with appropriate antennas and probes. A suitable power line analyzer is also identified in the equipment list.**

8. TEST EQUIPMENT.

8.1 SPECIFIC INSTRUMENTS. In order to be able to effectively evaluate and/or test potential airport security enhancements, a variety of test and support equipment may be necessary. The goal is to measure, view or count various phenomena or events in order to determine either compliance with specifications or test objectives. Depending on whether the items under test are related to access control, perimeter security or surveillance will determine the appropriate test and/or support equipment. The items to be evaluated, ranging from individual sensor components to fully integrated security systems, will also have a bearing on the type and amount of equipment required. Components can range from relatively simple mechanical devices to micro-processor based control systems. Three areas will be established to provide specific tools and equipment to perform specific tasks, they will include electronics testing, fiber optics work and fabrication.

8.2 ELECTRONICS WORKBENCH EQUIPMENT. This section provides an expanded description and identification of test equipment recommended for the EASTLAB and test ranges. The equipment listing is divided into general purpose, basic equipment which will be necessary for virtually any testing, and special-purpose equipment which is useful in certain kinds of tests. These two types of equipment are summarized in Table 1 and Table 2 respectively. Support equipment is identified in Table 3.

a. Oscilloscopes. The EAST Facility should have at its disposal at least two oscilloscopes for signal analysis and troubleshooting; (1) A bench type digital storage scope, 2 channel, 20 MHZ bandwidth and plotter output. The Tektronix model 2201 with plotter output option (approx. price $2,000) or the B&K Precision type 2522 (approx. price $1,100) offer the necessary capabilities; and (2) A portable type oscilloscope, 2 channel, 20MHZ bandwidth with external battery power pack. The Tektronix model 2205 (approx. price $2000) or the B&K Precision type 1422 (approx. price $1200) satisfy these requirements;

b. Function Generator. A function generator serves as a signal source in troubleshooting and testing of various components used in security systems. Typically a 0.2 Hz to 2.0 MHZ, 10V p-p into 50 ohm load with sine, square and ramp output will suffice. The B&K Precision Type 3011B (approx. price $260) or the Tektronix CFG250 (approx. price $365) will meet these specifications;

c. Multimeters (volt-ohm-milliammeter). A general purpose multimeter, either digital or analog, is necessary for measuring voltage, resistance, current and continuity. There are a number of models available that will do the job including the Simpson 260 (analog, approx. price $180) or Fluke 77 (digital, approx. price $165). Although equivalent performance is available at a lower cost, these models are known for their proven durability;

d. Megohmmeter. A Megohmmeter is for performing ground tests, and soil resistivity measurements, which are crucial to prevent physical and equipment damage resulting from over-voltages. Typical applications include measuring for 10 ohms or less on single and multiple ground electrodes used in security systems. The Biddle model 250300 (approx price $2,100 for megger and accessory kit) will perform ground resistance checks as well as soil resistivity checks;

e. Power Supplies. Both AC and DC power supplies are necessary for troubleshooting and testing various sensors and security equipments. The regulated DC supply should provide variable 0 through 30VDC, 0-6A output. The Topward Lab regulated DC power supply model 2306 (approx. price $450) offers a dual DC power supply that will meet these requirements. For AC, a power supply that provides continuously variable voltage for 0 through at least 120VAC is desired. The Vector-Viz model WP32 dual output, provides 0 through 150VAC @ 0-10 amps (approx. price $676);

f. Strip Chart Recorder. A means of recording events for later review or documentation should be available to the lab. The Vector-Viz model VR-202 is a two channel, with 15 pre-calibrated input ranges (1mv to 125 volts) and +/- .25% accuracy (approx price $2400) that should satisfy most requirements;

g. Data Communications Test Equipment. In order to analyze the communication networks between control computers and security system components, a protocol analyzer that is capable of interfacing the various data transmission methods is required. The Hewlett Packard 4957A (approx. price $6990) protocol analyzer will interface RS-232C/V.24, RS449/422/423, and V.35. Another device that is useful in monitoring the RS-232 data stream between devices is an RS-232 cable monitor such as the Black box Quick Test Model (QT-B) (approx. price $40). This gives a visual indication via LED's of the data;

h. Spectrum Analyzer. For work involving radio frequencies (RF), a spectrum analyzer will be required. Investigations of radio frequency interference (RFI) are a prime example of the testing that call for a spectrum analyzer. The IFR Systems A-7550 10 khz to 1 ghz spectrum analyzer (approx. price $8,200 w/options) is a reasonably priced unit to perform these operations;

i. Electrical/magnetic Field Meter. This device is designed for the measurement of electric and/or magnetic fields, and is useful for testing for potentially hazardous fields emitted from the cathode-ray tubes which are used in computer and CCTV monitors. The requirement is to be able to measure extremely low frequency fields (DC to 3 khz), with sensitivity down to approximately 1 milligauss (magnetic) and .5 volts/meter (electric). The "TriField" monitor manufactured by AlphaLab, 1272 alameda Dr., Salt Lake City, UT, 84102, cost $145.00, is one such device. (The possible health hazard of such fields is controversial at this time, apparently without any confirmatory medical evidence);

j. Computer. An IBM compatible personal computer (PC) should be available for use in test and evaluation. Current technology often uses a PC to handle the control function in larger security systems. The availability of a PC will enable the tests to include "stress" tests of the system by creating multiple alarms, determine ability to handle simultaneous alarms or unique requirements. A 386/486 PC with 4 megabytes of RAM, a 60 meg hard drive, a data acquisition/output board, an SVGA monitor and printer will provide the capability to test most devices (approximate cost $2,000); and

k. EPROM Programmer. An EPROM programmer (approximate cost $1,100-$1,500) is necessary when firmware needs to be changed to either to correct a deficiency or modified to suit a specific situation. An EPROM eraser (approximate cost $100-$150) is also necessary to erase existing firmware.

Table 1. General Purpose Equipment

QTY	NOMENCLATURE	APPROXIMATE PRICE
1	Oscilloscope, bench, storage	$ 2,000.00
1	Oscilloscope, portable, battery powered	2,000.00
1	Function Generator	365.00
1	Multimeter	180.00
1	Megohmeter	2,100.00
1	Power Line Analyzer	2,000.00
1	Power Supply, DC	450.00
1	Power Supply, AC	676.00
	SUBTOTAL:	$ 9,771.00

Table 2. Specialized Equipment

QTY	NOMENCLATURE	APPROXIMATE PRICE
1	Strip Chart Recorder	$ 2,400.00
1	Protocol Analyzer	6,990.00
1	Cable Data Monitor	40.00
1	Spectrum analyzer	8,200.00
1	Electromagnetic Field Meter	145.00
1	Computer	2,000.00
1	Eprom Programmer	1,500.00
1	Eprom Eraser	150.00
1	Optical Time Domain Reflectometer	12,000.00
1	Fiberscout	5,200.00
1	Optical Tester	930.00
	SUBTOTAL:	$39,555.00

8.1.1 Electronics Workbench Support Equipment.

a. Anti-Static Control Workstation. Although the Electronics bench is equipped with an electrostatic dissipative (ESD) surface, an anti-static workstation grounding kit should be utilized to avoid damaging ESD sensitive devices. The Newark series 8020 kit (approximate cost $260) contains a 2'x4' table mat, 4'x6' floor mat, 15' ground cord, wrist strap and grounding system and will provide the required protection;

b. Soldering Station. To effect repairs to printed circuit boards and the fabrication of some connectors a soldering/desoldering station is required. The station should offer variable soldering temperatures of 550-850 degrees fahrenheit and desoldering temperatures of 500-1000 degrees fahrenheit. The Ungar type 4624 or Weller DS100 soldering/desoldering station (approx. price $850) are suitable units to accomplish this requirement;

c. Benchtop Fume Absorber. During soldering/desoldering operations a fume absorber is necessary to trap airborne pollutants. The OK Industries Benchtop Fume Absorber model SA-9-E-115 (approx. price $170) will perform this function; and

d. Electronics Tool Kit. A selection of hand tools is necessary to carry out day to day maintenance, repair, and installation of the various sensors and security systems.

A technicians/field engineer tool kit would be the foundation, supplemented by special purpose tools to accomplish specific functions. The Specialized Products Co. model SPC-95 (approx. price $600) is typical of a number of tool kits available on the market. This kit provides a 10 piece spline key set, combination crimp tool, inspection mirror, two ball-end hex sets (metric and inch), two combination wrench sets (metric and inch), soft brush, two alignment tools, center punch, two pin punches, ball peen hammer, hand reamer, screw-starting screwdriver, two wire strippers (10-18 and 22-32 AWG), receptacle analyzer, combination spring hook tool, reversible retaining ring plier, contact burnisher, electricians scissor, hemostat, 4"and 8" adjustable wrench, chain nose plier, 4"and 5" diagonal cutting plier, utility plier, long nose plier with cutter, small vise grip plier, precision plier, regular blade handle, ratcheting blade handle, two sets nutdrivers (metric and inch) five slot blade screwdrivers, four phillips screwdrivers, six piece Torx driver set and tool box. The Xcelite model TC-100/ST tool kit (approx price $660) is another that includes; 53 individual nutdrivers, screwdrivers, pliers and wrenches, 31 Series 99 interchangeable screwdriver-nutdriver blades and handles, and two screwdriver-nutdriver sets. Additional items that are needed include crimping tools (approx price $200), tension gauges (approx. price $150), Integrated circuit insertion and removal tools (approx price $100), wire wrap tools (approx price $100), Punch down tool (approx price $70), heat gun (approx price $100), bench magnifier lamp (approx. price $100). Other miscellaneous items would include spring scales (to 150#), tape measure (100 ft.), flashlight, etc.

Table 3. Support Equipment

QTY	NOMENCLATRUE	APPROXIMATE PRICE
1	Workbench, ESD surface	$ 725.00
2	Workbench, laminated surface	660.00
1	Anti-static workstation	260.00
1	Soldering station	850.00
1	Benchtop fume absorber	170.00
1	Tool kit	1,700.00
1	Fiber optic splice tool kit	850.00
1	Fiber optic connector tool kit	900.00
1	Drill, electric, 3/8", vsr	60.00
1	Drill, electric, 1/2"	100.00
1	Drill press	500.00
1	Hydraulic knockout punch set	550.00
1	Welder AC/DC w/accessories	550.00
1	Bench vise, 5"	175.00
6	C-clamps, 4"	150.00
6	C-clamps, 6"	150.00
1	Bending brake, vise mount	140.00
1	Tristand	300.00
1	Pipe threader w/ dies	450.00
1	Rivet tool kit	40.00
	SUBTOTAL:	$9,280.00

8.1.2 Fiber Optics Workbench Test Equipment.

a. Optic Fault Finder. In order to determine the condition of fiber optic cable and connections a fiber optic fault finder is necessary. An optical time domain reflectometer (OTDR) is one device that can accomplish this but the performance and relative expense (approx. price $12,000) is not normally required to satisfactorily conduct the testing. A device that will handle most normal testing requirements is the Tektronix TFS 20/20 Fiberscout (approx. price $5200). The Fiberscout will identify and locate breaks or major loss problems in fiber optic cable systems, which are typical of the problems encountered; and

b. Optical Tester. The Siecor Optical Tester, model OT-100, (approx. price $930) with ST connectors, incorporates a power meter and a stabilized light source in a single unit. It is used for trouble-shooting, maintenance, continuity checks, and attenuation testing of optical fiber cables connections, and installed systems.

8.1.3 Fiber Optics Support Equipment.

a. Fiber Optic Splice Tool Kit. The fiber optic splice tool kit provides the tools necessary for tasks associated with the installation and maintenance of fiber optic cable. Tool kits are made to support specific manufacturer splices. The kit selected supports Siecor's Cam Splice. Based on experience this splice has proven to be reasonably easy to install and provide a connection that is sufficient to support most light budgets encountered in the test and evaluation of security system fiber optic links. The Siecor Cam Splice Tool kit, model TKT-100-02 (approx. price $850) can be used with Siecor Cam splices and contains the tools necessary for splicing fiber optic cables. The kit includes an assembly tool, buffer tube cutting tool, fiber coating stripping tool, fiber cleaver and carrying case. If another manufacturer's splice is required then a tool kit appropriate for that spice will be required; and

b. Fiber Optic Connector Tool Kit: As with the fiber optic splice tool kit the fiber optic connector tool kit is designed to support a specific manufacturer's connector. The Siecor Camlite ST-compatible multimode field installable connector, combines Siecor's high-precision ferrule with the Camsplice to provide a connector that requires no polishing, no fiber sizing, and no epoxy or curing. Siecor bonds a fiber "stub" into the connector ferrule and polishes it to a "physical contact" (PC) finish. The other end of the stub is precisely cleaved and placed into the alignment mechanism of the Camsplice. The assembly process requires only cleaving the fiber, inserting it into the splice section, actuating the splice and attaching the connector hardware and strain relief. The Siecor field termination kit, model TKT-020 (approx. price $900) for Siecor ST-compatible, Camlite connectors contains all tools necessary to terminate connectors.

8.1.4 Workbenches. The work benches should provide an area that can be used for testing and evaluation of the many different components that may be used in a security system. It should be sturdy and provide sufficient area that the item under test and the necessary test equipment can be set up without danger to the equipment or personnel conducting the tests. Sufficient power should be available so that the test setup does not place an undue load upon the electrical circuit. The bench top used for electronics should be electrostatic dissipative (ESD) and the one used for fabrication should be able to withstand the rigors of heavy work. Enclosed storage areas will provide secure storage for the tools and materials used in the test and fabrication. C&H Distributors model 53-139A for ESD top work bench (approx. price $725), and model 53-144A for laminated maple top (approx. price $660) have 72x30" work areas, built-in power strips, 18" high riser shelf, and cabinet and four drawer storage pedestals. One bench with the ESD surface and two with the laminated maple top are required.

8.1.5 Fabrication Workbench. The ability to fabricate a variety of items called for in testing and evaluating different devices and systems will require the availability of a number of tools. An industrial grade electric drill, 3/8" variable speed, reversible is adequate for most tasks although the availability of an 1/2" drill is also desirable. Either of these is available for between $50 and $100. A drill index equipped with bits up to 1/2" will suffice for the majority of jobs. A drill press, either bench top or floor model (preferred) is also useful when a greater degree of precision is required. One with a 14" capacity and multiple speeds with a 5HP motor are available for around $500.

In order to connect conduit to the different equipment enclosures, a hydraulic knockout punch driver kit is required to cut holes without distorting the enclosure. A Greenlee or Rigid hydraulic knockout punch set with 1/2", 3/4", 1", 1 1/4", 1 1/2", and 2" "Slug Buster" punches and dies run about $550. A small AC/DC welder is often necessary to fabricate mounting assemblies or other test apparatus. A Lincoln 225/125 AC/DC welder will handle most routine requirements and costs around $400. Necessary safety accessories, i.e. helmet, gloves, welding apron etc. will run an additional $100-$150. A five inch medium duty mechanics vise (approximate cost $175) should also be mounted to the bench for holding items being worked on. Additional 4" (six each) and 6" (six each) medium to heavy duty "c"-clamps (approximate cost $25 each) should also be available to facilitate fabrication. A small, vise mount, hand bending brake (approximate cost $140) is also useful in performing a wide variety of bending jobs. To work with rigid conduit, a tristand pipe vise (approximate cost $300) and ratchet pipe threader (approximate cost $450), to handle pipe up to two inches in diameter is required. A rivet tool kit (approximate cost $45) is often useful in the fabrication process in making enclosures, brackets etc. Other small hand tools such as ball peen hammers, hacksaws, wrenches, vise grips etc. will be required to accomplish the various fabrication tasks.

9. LABORATORY AND TEST RANGES.

9.1 PROPOSED FACILITIES AND LAYOUTS.

9.1.1 Eastlab. The primary indoor facility, EASTLAB, will consist of a single room approximately 30 ft by 35 ft, in the Laboratory Building. The basic configuration is as displayed in Figure 2, consisting of two Offices, three workbenches (electronics, fiber optics, fabrication), and a test system workspace (table and equipment racks). The remainder of the room is left available for other devices or equipment. Overhead cable trays are provided, for connecting devices and components in the test racks to the test equipment on the workbenches. Elevation views of the benches are shown in Figure 3 and 4, respectively. Since the overall scope includes two outdoor test ranges which must often be connected to the indoor Laboratory, two "cable head" junction boxes are also required, shown as mounted on the exterior wall near the rollup door. A ground bus is required; it is shown as traversing the room, and exiting through one of the exterior cable runs to a ground rod. (The exterior rod and cable may be deleted if an existing earth ground is located in the room.) The recommended workbenches are pre-wired with power outlets; a dedicated power line may be desired for these benches, in lieu of using the existing wall sockets. The total power requirement for the workbenches is approximately three kva. A separate power cable should be run to the test system workspace, able to supply approximately 2 kva, and terminating with at least ten outlets.

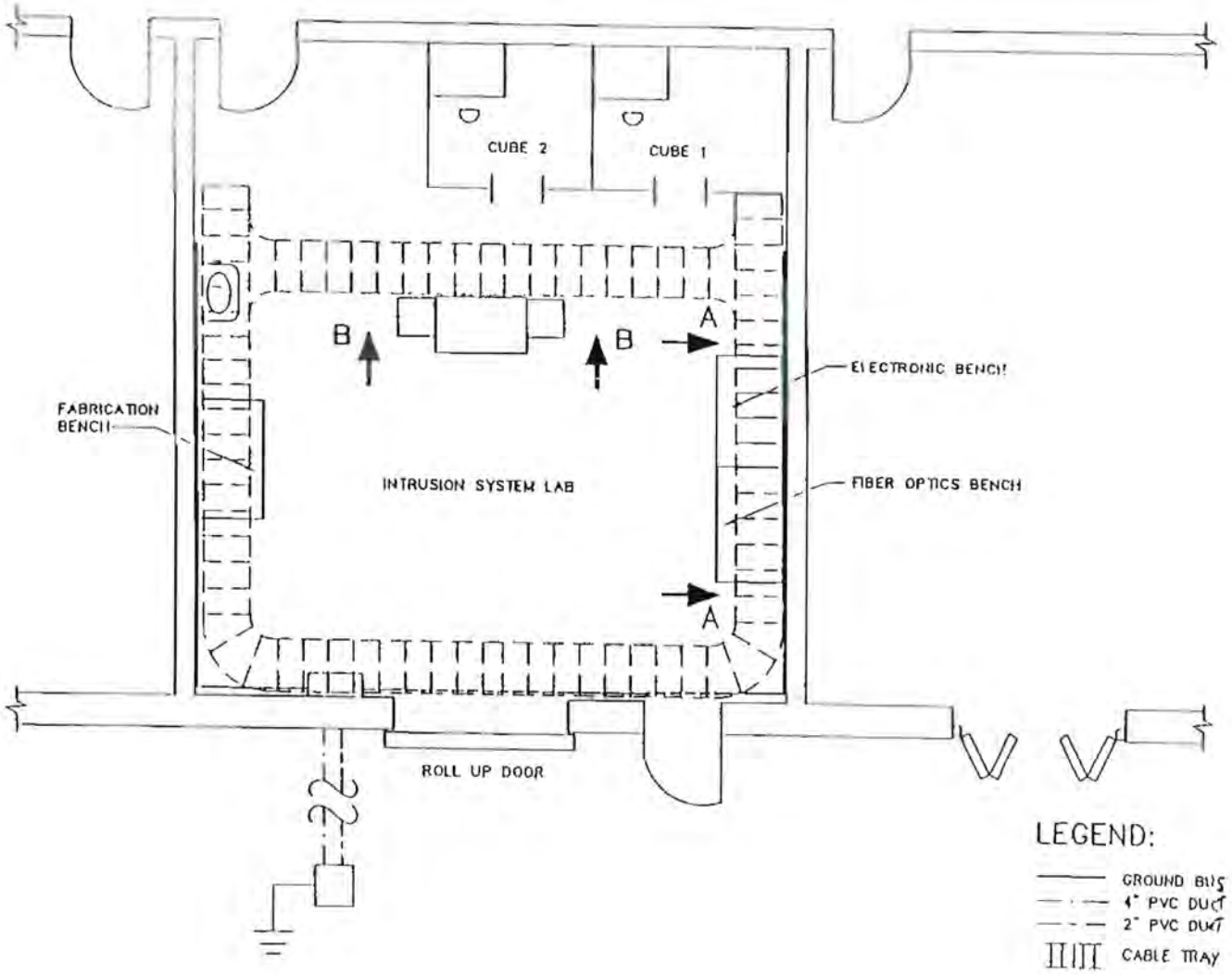


Figure 2. FAA Eastlab Floor Plan (Conceptual)

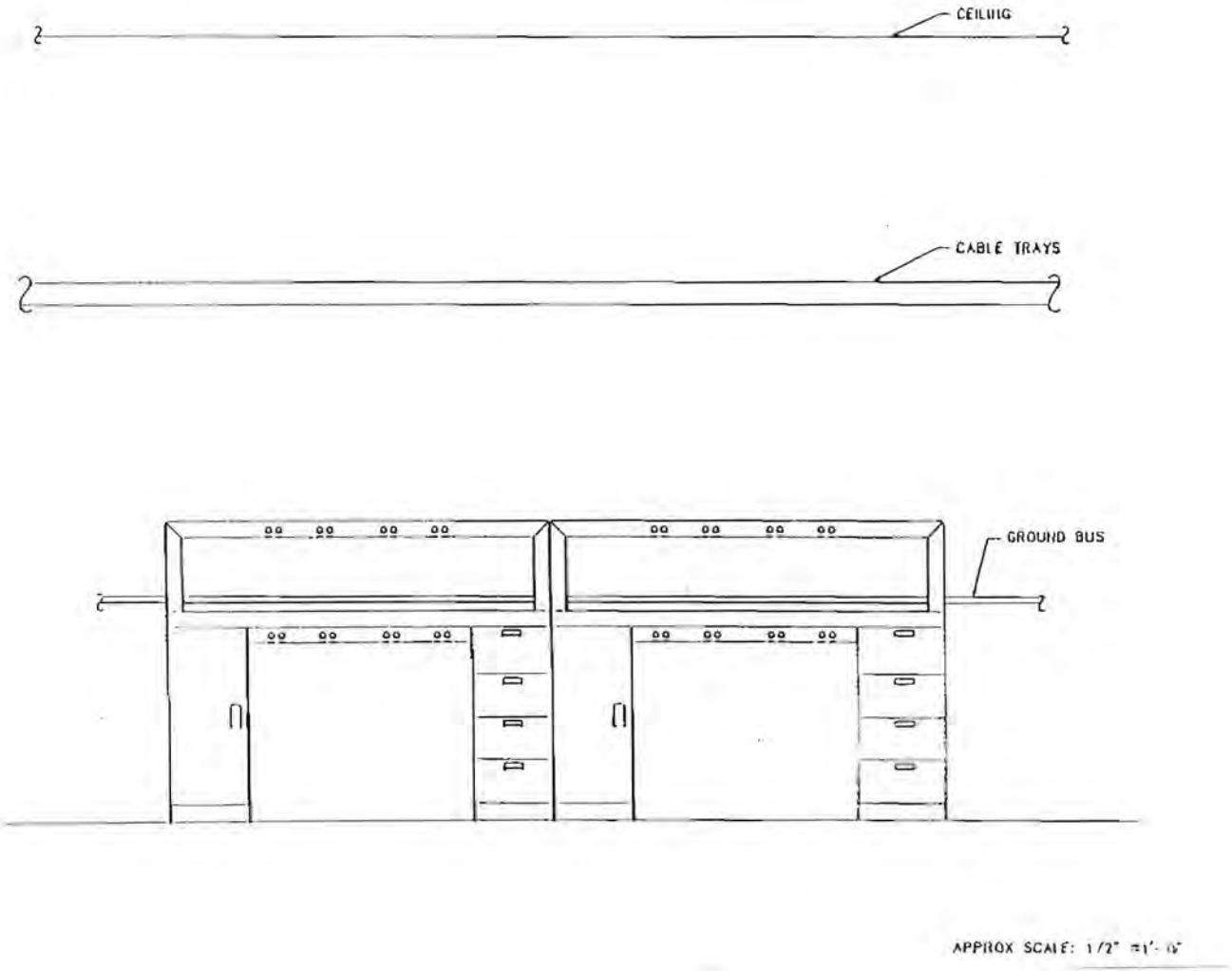


Figure 3. Electronics Workbenches (Elevation A-A)

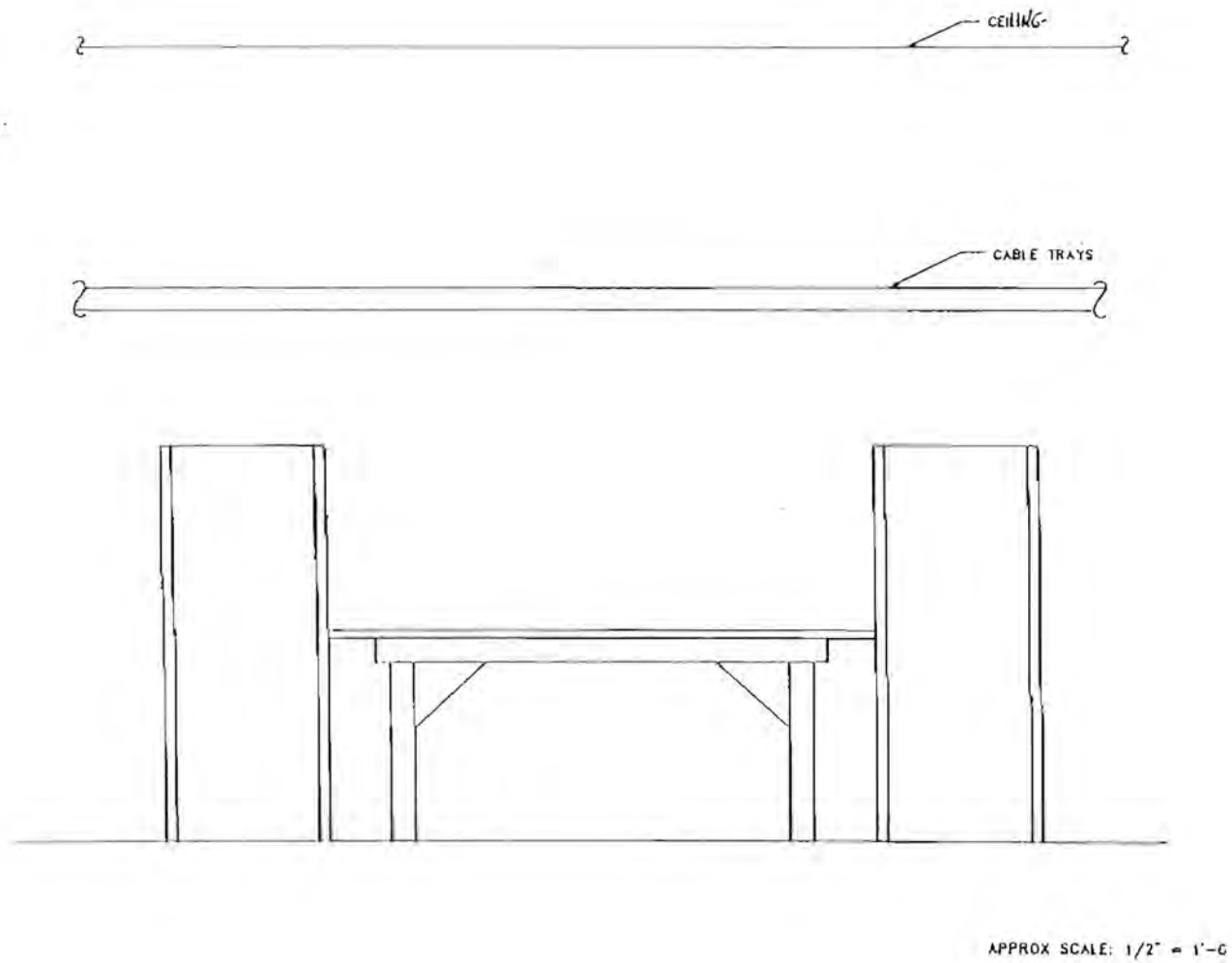


Figure 4. Test Systems Workspace (Elevation B-B)

9.1.2 Test Range 1. Figure 5 shows a proposed configuration of a test range (arbitrarily designated "Range 1"), which is adjacent to the EASTLAB for ease of access and control. The proposed configuration assumes that some degree of limited use may be made of the security fences already in existence, and a portion of the enclosed area which is not indicated as having other uses. The "range" includes a small tower which can be used, for example, for mounting CCTV cameras. It also includes two underground cable ducts with access holes spaced approximately every ten feet. One such cable duct is adjacent to the existing fence; the second, longer, duct is shown as traversing a relatively large area, from the loading dock of the laboratory building, and passing the Administration Building. These ducts are intended for cable runs to various outdoor sensors and devices undergoing tests. These might, for example, be fence-mounted sensors, microwave motion detectors, or even access control devices (including pedestrian or motorized gates). Note that there is no explicit provision for mounting any such devices (fence posts, etc.) since these would be unique to any specific series of tests. The exact length and placement of these ducts will, of course, be dictated by aesthetic considerations and other potential uses of the areas.

9.1.3 Test Range 2. It is recommended that a second test range ("Range 2") also be established, and that range be in the vicinity of Atlantic City International Airport. In addition to providing a larger test area than is available in the vicinity of the EASTLAB, Range 2 will be exposed to noise, vibration, electric and radio-frequency emanations and other conditions typical of an airport environment. For those reasons, and as shown in Figure 6, test Range 2 should be located within a few hundred yards of existing radar, radio ranging, or air traffic control communications emitters, if at all possible. As proposed, Range 2 would consist of a rectangular area approximately 200 ft by 200 ft, plus a small shelter and a short tower. (A proposed 20 ft, commercially available tower is shown in Figure 7.) The shelter should be equipped with a small workbench and two equipment racks for test devices and equipment. It contains the cable head junction box for the underground cable back to the EASTLAB. Power requirements are minimal, approximately 2 kva, unless heating and air conditioning is provided (optional). A telephone should be provided, although an option is to use one pair of the underground cable to EASTLAB. As in the case of Range 1, an underground cable duct is provided for connecting test items on the range to the shelter (and thence to EASTLAB if required).

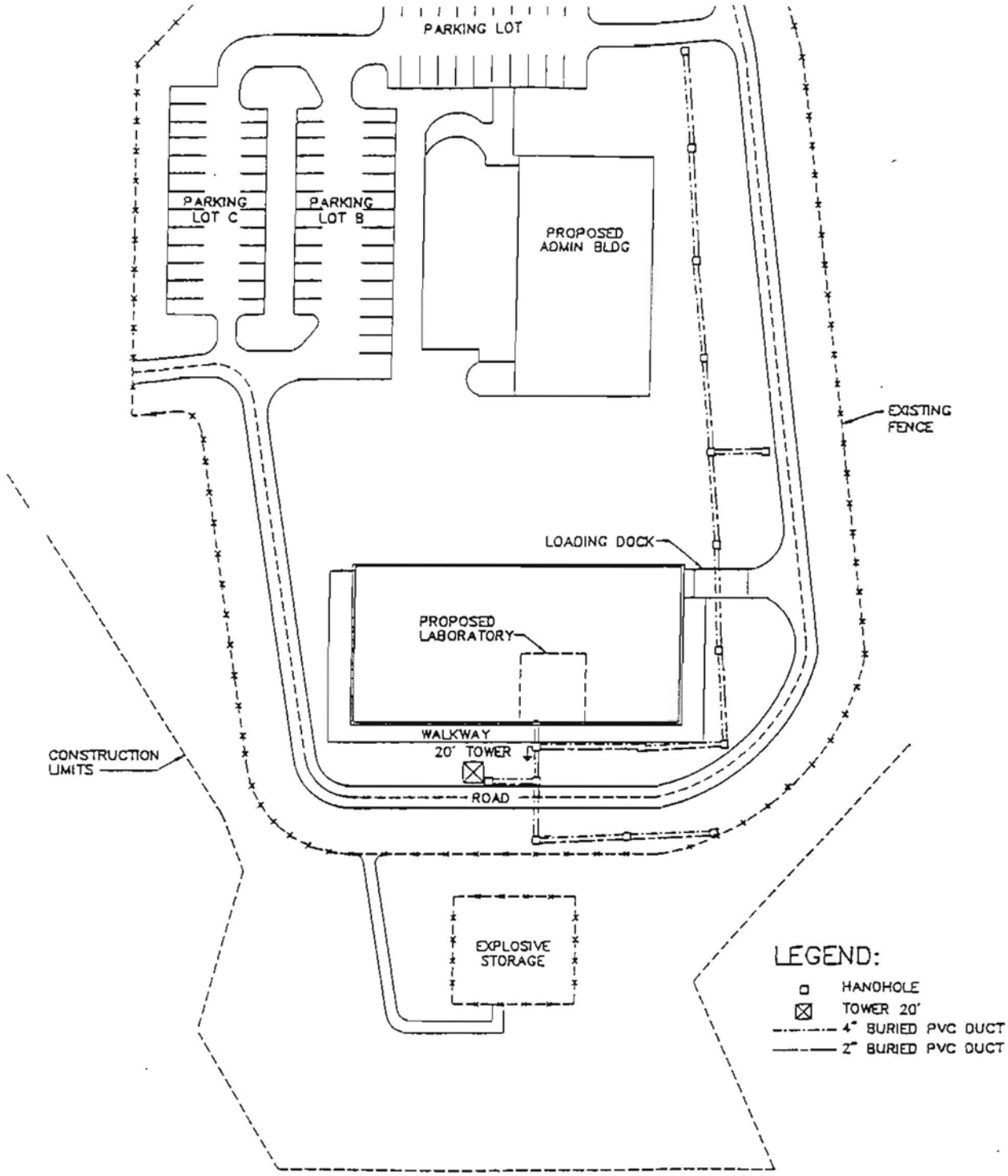
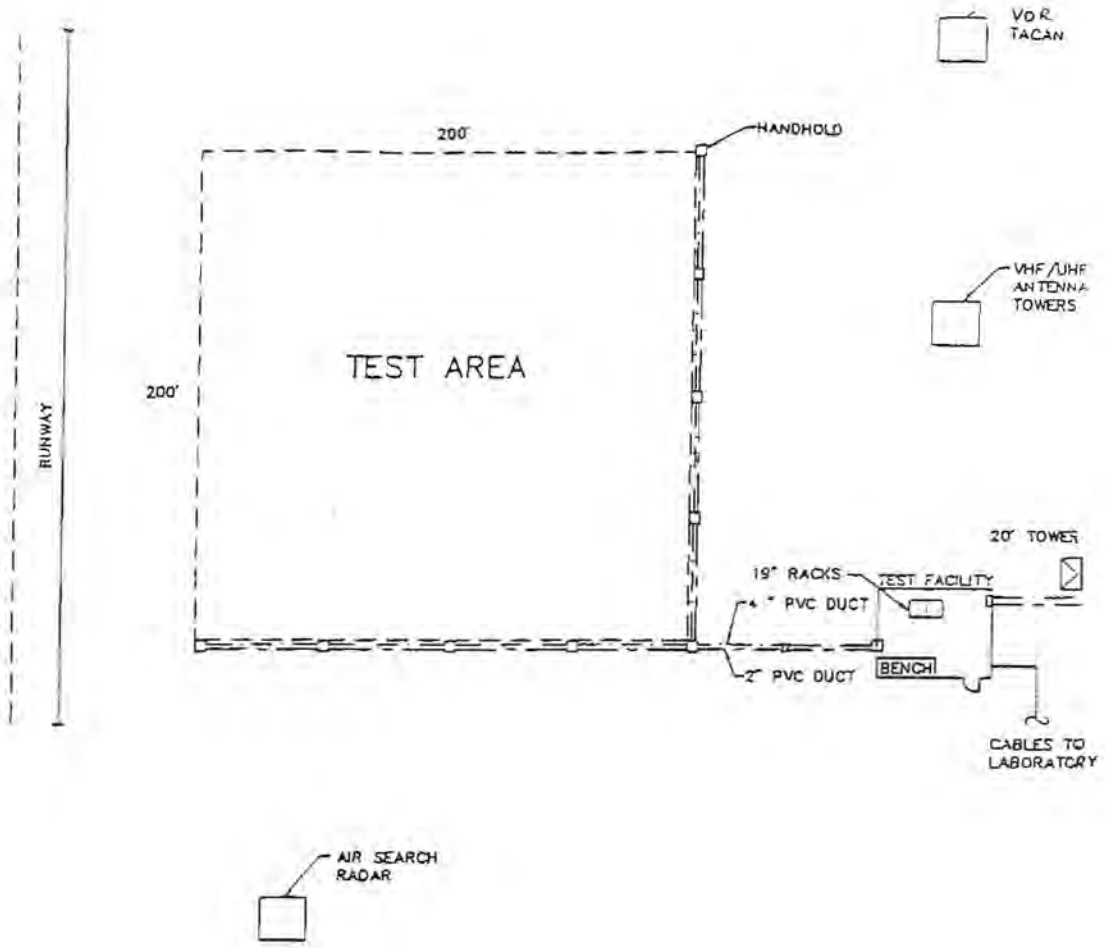


Figure 5. FAA EASTLAB Test Range (Conceptual)



LEGEND:

- HANDHOLE
- TOWER 20'
- 4" BURIED PVC DUCT
- 2" BURIED PVC DUCT

NOTES:

TEST FACILITY SHOULD BE EQUIPPED WITH PHONE, 220VAC 100AMP SERVICE, 25 PAIR PHONE LINES AND MULTIFIBER FIBER OPTIC CABLE TO LAB.

THE TEST RANGE SHOULD BE LOCATED IN THE VICINITY OF THE RUNWAY, RADAR VOR(OR TACAN) AND VHF/UHF ANTENNA TOWERS FOR INTERFERENCE STUDIES.

Figure 6. FAA Eastport Test Range (Atlantic City International Airport)

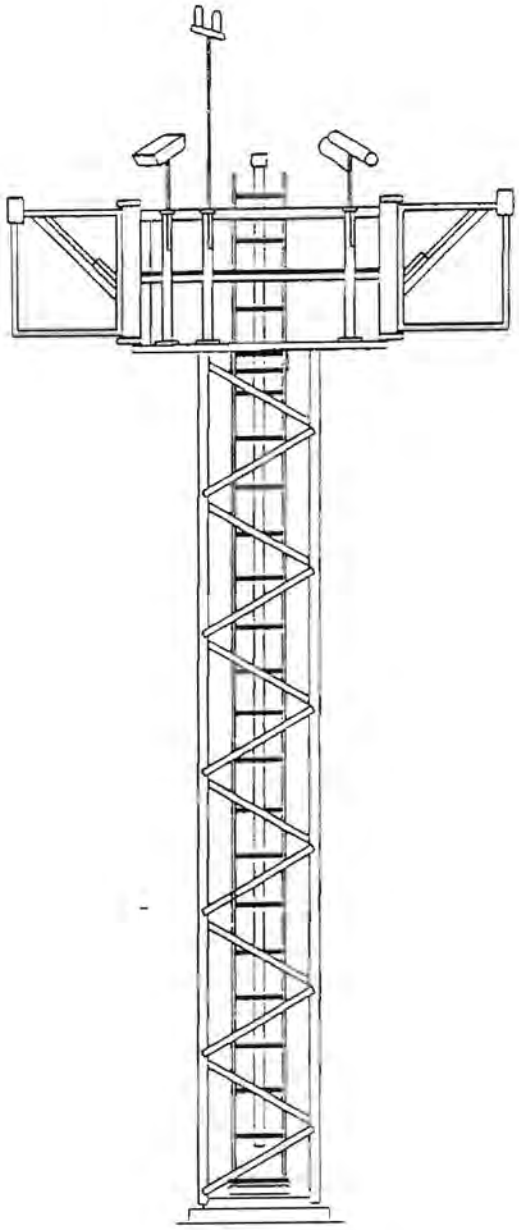


Figure 7. Electronic Security System Test Tower (Conceptual)

10. CONCLUSIONS. It is possible to fulfill the purpose of testing electronic security systems and devices within the general scope of the facilities designated for this purpose, plus at least one outdoor test range (preferably two outdoor ranges). Adequate test and support equipment is readily available on the commercial-industrial market. The test facility, including one or both ranges, can be constructed in phases if required; if so, the logical progression is EASTLAB, Range 1, and Range 2. Similarly, the EASTLAB may be equipped in phases, beginning with the general-purpose test equipment (Table 1), then selected items from Table 2 (special purpose equipment) as the need arises. Most or all of the support equipment (Table 3) should also be provided in an early stage.

11. RECOMMENDATIONS. Proceed with the electronic security testing facility as described in this document, with minor configuration changes to the size, shape, and exact locations of the outdoor ranges as may be required.

Implement the facility as a single project if budgetary constraints permit.

APPENDIX A

DEVICE TEST SHEET

DEVICE TEST SHEET

Device (Name, manufacturer, model, other pertinent data):

Device Type (IR Sensor, Card Reader, etc):

Advertised Characteristics (as pertinent):

Sensitivity/range/response time, etc.:

Interface Specifications (Data rate, RS-232/485, etc):

Power requirements and consumption:

Size/weight:

Environmental requirements (temperature/humidity, etc.):

Others:

Test Objectives:

( ) Confirm advertised parameters/characteristics
( ) Determine unknown characteristics:
_____
_____
_____
( ) Compatibility with _____
( ) EMI/RFI generation and/or susceptibility
( ) False Alarm Rates
( ) Environmental Effects
( ) Other:_____
_____
_____

Test Equipment Required:

_____
_____
_____
_____

Fabrications Required:

_____
_____
_____
_____

Test Facilities:

( ) EASTLAB
( ) Range 1
( ) Range 2
( ) Other

Test Procedures and Sequences:

(Must correspond to Test Objectives)
(May require a lengthy separate document)

Special Precautions and Instructions:

Data to be Collected:

( ) Standard Data Sheet
( ) Special customized sheet (attached)

Analysis of Data:

( ) How empirical data is to be analyzed for a result or conclusion)

Final Product:

( ) Informal Report (Laboratory Use only)
( ) Formal Report
( ) Certification/Standards Publication

APPENDIX B

LESSONS LEARNED

LESSONS LEARNED

Detailed technical descriptions: Whether it is an overall "Security consciousness" inherent in the industry, or just ordinary self protection in a business sense, most manufacturers of security devices (especially sensors) are extremely reluctant to provide schematic diagrams and similar details of their equipment. Thus, if it is necessary to modify or adapt these devices to any usage other than that specifically intended by the manufacturer, it will usually be necessary to buy the rights on a non-disclosure basis, or to perform "Reverse Engineering" on a device in hand. Stress testing or failure analysis may lead to similar requirements for purchase of information beyond the standard installation literature provided with the devices.

System Computers and Processing: The software which comprises the heart of most modern security systems is generally even more closely guarded than the hardware. Much of it is also stored in ROMs, frequently soldered in place, and even less accessible for "Reverse engineering" than the hardware mentioned above. Typically, the system vendors employ "IBM clone" CPUs, with commonly-available option cards. Relatively few vendors have chosen to build or incorporate truly unique cards into the CPUs themselves. However, they do tend to design and provide "Smart" data concentrators and "Pre-processors" which interface to the sensors and other devices themselves, converting their signals into forms more easily utilized by the CPU proper.

Production changes: Because the security device manufacturers do not routinely publish detailed technical information, they also do not take any special pains to inform the customers about changes in production or design, as long as those changes do not affect the "Normal" and expected use. In specific applications, however, such production changes may result in varied performance (For example, RFI/EMI susceptibility or generation). In most commercial systems, production-line changes are not likely to show up as performance differences--the specific devices either do or do not work properly when installed. In the case of "Standard" device selection, however, guiding the purchase and use of many devices over a period of years, and for many different locations, production-line changes certainly can make differences. There is no simple "Fix" for this potential problem; it must be resolved by liaison with the manufacturer and/or testing of each new version.

Laboratory personnel: Ideally, the personnel who operate the laboratory should be qualified by either education or experience in "The art of scientific investigation". The overriding need is for personnel who understand how to set up controlled experiments, determine what data is to be collected, and how to analyze the results.

Generally, these people tend to be "Scientists" rather than "Engineers;" however, it is often the case that the engineers or technicians are more skilled in the actual set-up of devices to be tested, and in the actual data collection operations. There is also a requirement for

personnel to do general light fabrication work (including light welding), although these people do not have to be an integral and permanent part of the laboratory manning if they are available for occasional tasking.

APPENDIX C

COST ESTIMATE - CONSTRUCTION

COST ESTIMATE - CONSTRUCTION

The approximate costs for the EASTLAB equipment and support items are given in Tables 1 through 3. The approximate costs of construction and installation are provided in this Appendix. Although the installation within the Laboratory building can be estimated with reasonable accuracy, the uncertainties in precise location and extent of the outdoor Ranges does not permit the same degree of estimation. (For example, the costs of land clearing or levelling will be determined by terrain, vegetation, etc. at the final site. Similarly the exact costs of cable trenching from Range 2 (at Atlantic City International Airport) will be dependent on the exact location selected.)

The installation costs which can be identified with reasonable accuracy are as follows:

Lab Cable Tray (East Lab)

Material:	$ 1,650.00
Labor:	1,100.00
Total:	$ 2,750.00

Test Tower (Range 1, Range 2)

Tower:	$ 6,800.00
Foundation:	2,000.00
Shipping:	1,200.00
Total: (Estimated cost per tower)	$10,000.00

Cable Trenching: Depending on the distance, conditions, road cuts, etc. Typical cost should run about $15.00/Ft.

Cable Costs: (Range 2 to East Lab)	25/Pair	$ 840.00/1,000 Ft
	4/Fiber	$ 850.00/1,000 Ft
Range 2 Shelter (12' x 20')		$4,000.00
Concrete Foundation		$1,000.00

Above figures do not include any cost for AC power distribution (East Lab or Range 2).

NTIS does not permit return of items for credit or refund. A replacement will be provided if an error is made in filling your order, if the item was received in damaged condition, or if the item is defective.

Reproduced by NTIS

National Technical Information Service
Springfield, VA 22161

This report was printed specifically for your order from nearly 3 million titles available in our collection.

For economy and efficiency, NTIS does not maintain stock of its vast collection of technical reports. Rather, most documents are printed for each order. Documents that are not in electronic format are reproduced from master archival copies and are the best possible reproductions available. If you have any questions concerning this document or any order you have placed with NTIS, please call our Customer Service Department at (703) 487-4660.

About NTIS

NTIS collects scientific, technical, engineering, and business related information — then organizes, maintains, and disseminates that information in a variety of formats — from microfiche to online services. The NTIS collection of nearly 3 million titles includes reports describing research conducted or sponsored by federal agencies and their contractors; statistical and business information; U.S. military publications; audiovisual products; computer software and electronic databases developed by federal agencies; training tools; and technical reports prepared by research organizations worldwide. Approximately 100,000 *new* titles are added and indexed into the NTIS collection annually.

For more information about NTIS products and services, call NTIS at (703) 487-4650 and request the free *NTIS Catalog of Products and Services*, PR-827LPG, or visit the NTIS Web site **http://www.ntis.gov**.

NTIS
Your indispensable resource for government-sponsored information—U.S. and worldwide