



US Army Corps
of Engineers ®

Electronic Technology Systems Center



Recently Updated

Unified Facilities Criteria

UFC 3-530-01 Design:
Interior and Exterior
Lighting and Controls

UFC 3-560-01:
Electrical Safety,
Operation and
Maintenance

UFC 3-580-01: Tele-
communications
Building Cabling
Systems Planning and
Design

UFC 3-600-01:
Fire Protection
Engineering for
Facilities

UFC 4-021-02 NF:
Security Engineering:
Electronic Security
Systems

UFC 4-022-01: Security
Engineering: Entry
Control Facilities/
Access Control Points

Visit Whole Building
Design Guide online
for more criteria info:
www.wbdg.org

Technical Bulletin

September 2007

Developing an access control point automation concept

By Charles R.
Malone

One of the continuing effects of the terrorist attacks of 2001 is an increase in security at access control points (ACPs) on military installations.

The policy of 100 percent ID checks for all personnel entering military installations initiated on Sept. 11, 2001, continues to the present, resulting in a very high annual manpower cost for ACP operations.

Routine ACP security screening involves guards visually checking the Common Access Card (CAC) or other

authorized credential of all incoming personnel and ensuring that each vehicle has a valid Department of Defense decal or temporary pass. Under certain conditions guards may stop a vehicle and conduct a thorough inspection looking for any prohibited items.

With a fully staffed, multi-lane ACP now requiring six or more security guards, military policy makers have been investigating an automation concept that will reduce ACP staffing levels and operating costs, while at the same time increase the effectiveness of driver/vehicle identity verification and maintain

or exceed current traffic throughput levels. To meet these objectives, an automation concept has been developed that, for a single successful transaction, requires the following operations:

1. Read the vehicle's radio frequency (RF) ID tag and the driver's card.

As the vehicle enters the ID check area, the RFID tag is read, and, once stopped, the driver presents his or her card to the reader. Biometric and personal identification number (PIN) options further verify the driver's identity, but these would increase transaction time and slow throughput.

Since *passengers are not required to present cards*, the registered driver/cardholder is identified



Courtesy photo

Successful entry transaction is displayed to the guard at the operator workstation.

See ACP on page 6

Selecting sensors for outdoor perimeter intrusion detection

By Charles R. Malone

Electronic security system designers are faced with many equipment selection decisions during a perimeter security design project. However, none is more important than choosing the appropriate sensor or sensors to provide reliable intrusion detection.

By carefully considering all aspects of the target (what you are trying to detect) and the background (environment “seen” by the sensor), a designer can select a sensor or combination of sensors to achieve the desired probability of detection as well as minimize nuisance alarms.

To be effective, this design analysis must be site specific, taking into account local terrain and environmental conditions as well as other facility features related to mission, assets and security posture.

Though not comprehensive, the following guidelines, grouped by general technology categories, serve as a good starting

point for a thorough sensor selection analysis.

Fence-Mounted & Taut Wire Sensors

Fence-mounted sensors, including both electromechanical point sensors and continuous cable (coaxial and fiber optic) sensors, attach directly to a fence and “listen” for noise generated by an intruder cutting, climbing or lifting the fabric.

These sensors are an economical option for providing a single line of detection, particularly if the site perimeter is already fenced. Fence construction details and overall fence condition are primary concerns as they can affect both probability of detection and nuisance alarm rate.

Even with a good fence, a site that experiences frequent high winds, especially when accompanied by heavy rain or blowing debris, will likely be bothered by nuisance alarms. As an alternative, a taut wire sensor, though more expensive and difficult to install, provides a single line of detection that is

more immune to weather-induced alarms.

Bistatic Microwave Sensor

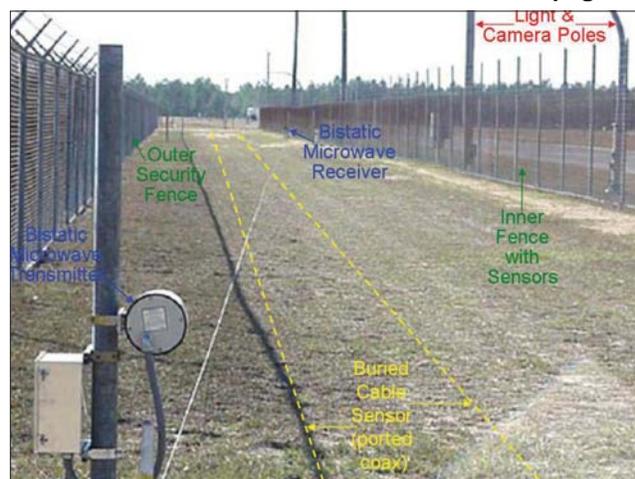
This sensor establishes a microwave detection field between two antennas, one a transmitter and the other a receiver, separated by a distance equal to the desired zone length (typically about 300 feet). Multiple zones are “chained” together with appropriate overlapping to cover an entire site perimeter. This sensor requires clear line-of-site between each transmitter/receiver pair. Therefore, each zone must be generally flat and free of any obstructions

including tall vegetation and snow accumulation. The large volumetric detection field is difficult for a person to circumvent, but is susceptible to nuisance alarms from water flowing across or standing in the field.

Buried Cable Sensor

This technology employs a pair of ported coaxial cables, each buried in the soil and connected to a processor, to generate an electromagnetic detection field above the ground surface. This field is created as energy “leaks” from the transmit cable and couples to the receive

See Sensors on page 5



Courtesy photo

Multiple sensor types are used in combination along this site perimeter.

Corps of Engineers can help get the job done right

Conducting QA inspections for ESS

By Michael Lewis

The reputation of many good electronic security products has been tarnished by poor installation from teams with inadequate oversight and quality control procedures.

Ensuring the installation is in compliance with manufacturers' instructions, organizational criteria and national codes is the responsibility of both the contractor's superintendent and the Contracting Officer's Representative (COR), a function performed by a government employee assigned to the project.

Failure to conduct thorough and timely quality assurance (QA) inspections can result in schedule delays, cost overruns, poor system performance, gaps in security coverage and, ultimately, a frustrated customer.

Prior to beginning a QA inspection, it is important to be familiar with all the requirements that apply to an Electronic Security Systems (ESS) design and installation project such as base contract provisions, the Performance Work Statement (PWS), design drawings, national codes (i.e., National Electric Code and Life Safety Code), Unified Facilities Criteria (UFC) and Unified Facilities Guide Specifications (UFGS). When incorporated into a military project, a UFC provides overall planning, design and construction guidance while a UFGS describes system performance requirements in detail down to the component level. On



Courtesy photo

Neat, easy to maintain enclosures (right) are preferable to crowded, unorganized enclosures (left).

Army projects, different security regulations may apply according to the protected asset and will prescribe increased levels of protection for arms, ammunitions and explosives (Army Regulation (AR) 190-11); medical, aviation, service and storage facilities (AR 190-51); Sensitive Compartmented Information Facilities (Director of Central Intelligence Directive (DCID) 6/9); and chemical (AR 190-59) and nuclear (AR 50-5-1) storage areas.

A key aspect of UFGS 28 20 01.00 10, *Electronic Security System*, is the first paragraph under Part 3, Execution: "The Contractor shall install all system components, including Government furnished equipment, and appurtenances in accordance with the manufacturer's instructions ..." The majority of commercial off-the-shelf security equipment works well when the manufacturer's instructions for installation and workmanship are followed. But because even a small ESS may incorporate a variety of devices including interior and exterior sensors, local processors, cameras, data transmission media/protocols and

software, even a seasoned site superintendent or COR cannot retain every significant installation detail. It is therefore recommended that each person with QA responsibilities, whether contractor or government, develop their own system of checklists or compiled documentation to use in the field when conducting inspections. This could take the form of a simple written list, annotated design drawings, or a binder of installation instructions and criteria documents with important details highlighted.

A good QA inspection should first be timely and take place during the initial phase of any new installation activity so that errors can be addressed early before they are duplicated multiple times. If it is not possible for the superintendent or COR to be physically present on site at specific times, some work details can be verified through a series of digital photos taken by another responsible person at the site (a customer representative, for example) that can be e-mailed for review. Second, a good inspection

See QA on page 7

Contract work - getting started right

A kickoff meeting could mean the difference between success and failure on a project

As the new fiscal year opens, many of you have either received or are anticipating receipt of funding for Utility Monitoring and Control Systems or Electronic Security Systems installation projects.

After months of planning and a substantial investment in the development of a Performance Work Statement (PWS) and system design documents, the project now shifts to a new phase.

Very few installation phase activities are as important as the project kickoff meeting. Immediately upon award of the contract, a meeting should be scheduled with all interested parties to discuss and coordinate all aspects of the project. Items to consider include:

• **Attendees**

The attendance list is very important. From the contractor's side, the project manager and the superintendent or lead technician must attend.

Depending on the size of the project, the contractor's senior management should also be present. The list gets longer for the owner. Certainly, the owner's project manager must attend. Additionally, the following functions should be included:

1. **Facilities Manager** -

The contractor needs to know who to contact for facility-related questions, issues and repairs.

2. **Safety**

Manager - The contractor's activities will be

monitored for compliance with appropriate safety requirements. The point of contact for these issues needs to be clearly identified.

3. **Utility Manager** -

What are the requirements for obtaining a lockout permit? What is the procedure for getting a new service drop? Is a trenching permit required for exterior projects? There needs to be a clear point of contact for these issues.



4. Accounts Payable - Obviously, contractors need to get paid.

• **Agenda**

This is the time to review with the contractor all of the requirements in the PWS and system design documents. Here are a few likely topics:

1. Scope - Make sure the actual work to be performed is understood.

2. Equipment Requirements - Review any special or crucial equipment-related requirements.

3. Work Day Restrictions - Some organizations restrict work hours to something other than 8 a.m. to 5 p.m. An escort may be required (and in some cases, clearances) to enter certain areas. Make sure these restrictions are clear.

4. Testing - Your PWS and/or specifications should include a requirement to test the installed system. (If they don't, don't bother with the kickoff meeting.) Make sure the contractor understands that the testing will be point by point, documented in

writing and that successful completion will be required before final payment is authorized.

• **Conduct of Project**

Establish how you expect the project to proceed with regard to:

1. Schedule - Require that a schedule be prepared for the project. Realize that a number of factors, many within your control, can impact the contractor's ability to keep to the schedule. Require the schedule to be updated weekly.

2. Project Meetings - Require weekly project meetings. Review progress made during the past week and ask the contractor to discuss (in detail) activities for the upcoming week. Comparing actual with previously projected progress is an excellent way to spot trouble maybe even before the contractor notices.

3. Changes - Changes are a fact of life. A project without changes is a project with latent troubles. Require the contractor to submit all requests for changes in writing. You must in

See Start on page 6

Sensors

continued from page 2

cable. The net result is a sensor that is both covert and terrain-following and is capable of detecting intruders as they crawl, walk or run over the cables. Unlike other sensor types, the performance of the buried cable sensor is strongly influenced by soil properties, in particular the electrical conductivity and permittivity. In highly conductive clay

soils, for example, the electromagnetic energy from the transmit cable is significantly attenuated resulting in a weaker above-ground detection field. When the soil freezes, the conductivity decreases resulting in a stronger detection field and a need to recalibrate the system. As with the bistatic microwave sensor, water such as puddles or surface runoff near the sensor cables can trigger nuisance alarms.

Other sensor technologies such as active infrared, passive infrared, monostatic microwave, electrostatic field, differential capacitance and video motion detection could also be considered for a design project and analyzed in a similar fashion, realizing that two or more types of sensors may be needed at a site to meet all perimeter security objectives. A common approach for high-

security facilities is to deploy a fence-mounted or taut wire sensor in combination with either a bistatic microwave or buried cable sensor, thus meeting the "dual phenomenology" requirement for primary perimeter intrusion detection. Manufacturers' planning and installation manuals along with government test reports and criteria documents are valuable resources for a sensor selection analysis.

Ask

continued from page 8

request or defined schedule basis. The system is capable of providing usage information on at least a daily basis and can support desired features and functionality related to energy use management, procurement and operations.

Q3. What are some of the general specifications for all meters?

Quantities measured include power (in kilowatt or kW), average demand over 15-minute intervals and energy used (in kilowatt-hours or kWh). The law does not specifically require them to be measured, but you should also consider phase voltage, amps, frequency, true power, reactive power, apparent power and power factor. The measurement configuration for single-phase application should

be 120 to 240 volts and 208 to 600 volts for a three-phase, three-wire delta or four-wire wye application. They should be able to operate from minus 20 degrees up to 60 degrees Celsius. If they are mounted on the exterior of the facility, consider your local ambient temperature extremes and moisture-proof enclosures. The meters should operate from 5 percent to 90 percent relative humidity (non-condensing). They should be accurate to within ± 0.2 percent at a power factor of one, and to within ± 0.5 percent at a power factor of 0.5. The meters should operate at a frequency of 60 hertz for continental U.S. (CONUS) applications and 50 hertz for outside the continental U.S. (OCONUS), ± 5 percent. For non-LonWorks meter applications digital output only, use MODbus RTU/RS485

protocol. For LonWorks meter applications digital output only, use ANSI/CEA-709.1b protocol (LonTalk) output for communications using Standard Network Variable Types (SNVTs) for measured values.

Q4. That sounds like a lot of technical information. Is there a specification available for them? If so, how can I get a copy?

The Utility Monitoring and Control Systems Mandatory Center of Expertise can help you with specification information as well as contract services. You can call at 256-895-1749 or visit us online at www.hnd.usace.army.mil/umcs/index.aspx.

Please send any questions you would like answered to: Contact-ESC@usace.army.mil

ACP
continued from page 1

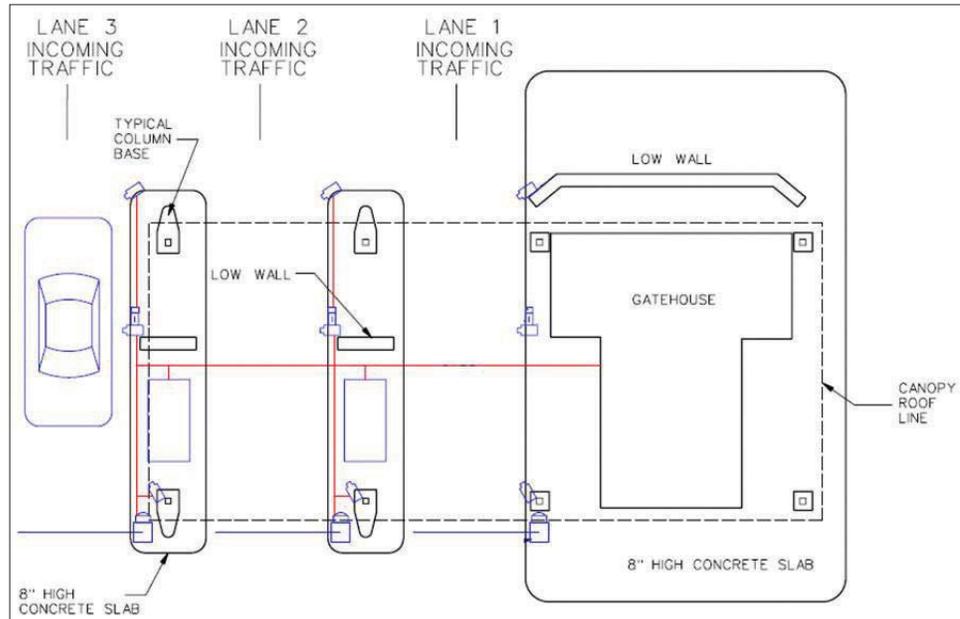
as a “trusted traveler” and is responsible for following all access control policies and not transporting unauthorized personnel or prohibited items onto the installation.

2. Capture images of the vehicle’s license plate and the driver’s face.

Two fixed cameras, one mounted low at the approach end of the traffic island and the other located with the card reader, are used to capture real-time images of the license plate and the driver.

3. Query the database for vehicle and driver information.

The unique RFID and card codes are used to query the access control database for vehicle and driver information. In addition to the basic vehicle/driver authorization status, other



Courtesy photo

This is the basic layout of access control point automation equipment.

information includes the vehicle’s description and license plate number and the cardholder’s name and archived photograph.

4. Display database query results and live images to the operator.

The operator is able to perform a quick side-by-side comparison of live images and archived information. If the operator notices any discrepancies, he or she can enter a “Stop

Vehicle” command and question the driver directly.

5. Signal the driver to proceed.

If the database query indicates that the vehicle and driver are authorized to enter the installation, and the operator has not intervened with a “Stop Vehicle” command, then the signal light will automatically cue the driver to proceed and the traffic arm will raise.

Ongoing efforts to further refine this automation concept, develop a fully integrated set of automation hardware and software, and perform small-scale deployment and testing are expected to yield an initial operational capability at several Army ACPs over the next two years, with the other services using a similar development cycle and implementation schedule.

Start
continued from page 4

respond in writing. Establish the process.

4. Documentation - Keep excellent records, schedule now to visit the project area weekly and record the work being done and changes from the last review.

5. Develop a Team - Develop a team with each member shouldering assigned responsibilities. Compliment when deserved and only criticize when it can be helpful. Make sure to deal with issues openly, quickly and decisively.

Experience has shown that a kickoff meeting does not always guarantee project success, but that many failed projects can trace problems back to ineffective coordination early in the installation phase.

You can learn more about Huntsville Center and its many programs by accessing online fact sheets.



Find fact sheets on:

Access Control Points

Electronic Security Systems

Utility Monitoring and Control Systems

... and many more!

Check them out at
www.hnd.usace.army.mil/pao/factshts.aspx

QA

continued from page 3

should include verification of the following: 1. quantities of equipment; 2. placement, mounting, orientation and effective coverage of sensors; 3. construction details of sensor platforms and physical barriers; 4. type and mounting of conduit and hardware; 5. grounding, surge and tamper protection of equipment; 6. routing, protection and neatness of cables, wiring and connectors; 7. backup systems; and 8. general appearance and workmanship.

Thorough documentation of discrepancies should be made at the time of observation. Detailed notes are essential and digital photos can be helpful to recall and display the nature of the problem in case there is a question or dispute after returning to the office.

You should also note concerns and observations that you may be uncertain about at the time of the inspection. Some details may require research and verification of



Courtesy photo

Properly anchored Balanced Magnetic Switch armored cables (right) are much better than loose BMS armored cables (left).

regulations, codes, specifications or contract language before including the discrepancy on a “punch list” for corrective action. In drafting the punch list, it helps to organize the content in some logical fashion, explain each problem in sufficient detail, cite the governing criteria for making the correction and provide direction on how to implement the modification. Providing clear instructions for the solution is just as important as identifying the problem.

Supplying QA guidance and direction at the proper time can assure project success and enhance the reputation of the entire project

team including the equipment manufacturer, the installation contractor and the COR.

Unfortunately, many military organizations are stretched thin for resources or lack the technical expertise to perform adequate oversight of ESS projects.

The U.S. Army Corps of Engineers, Electronic Security Center (ESC) in Huntsville, Ala., has an experienced technical staff of engineers and security professionals who can assist with QA inspections in addition to offering a broad range of services related to ESS design, installation and maintenance.

Check us out online:

ESC

www.hnd.usace.army.mil/esc

- **History of the ESC**
- **Why choose the ESC?**
- **List of clients**
- **Services offered**

UMCS

www.hnd.usace.army.mil/umcs

- **What does UMCS offer?**
 - **Why choose UMCS?**
-

Useful Acronyms:

ACP: Access Control Point

ESC: Electronic Security Center

ESS: Electronic Security Systems

ETSC: Electronic Technology Systems Center

MCX: Mandatory Center of Expertise

UMCS: Utility Monitoring and Controls Systems

ASK ETSC!

What's new with Army metering?

Q1. What are advanced meters?

Advanced meters are those that have the capability to measure and record interval data (at least hourly for electricity), and communicate the data to a remote location in a format that can be easily integrated into an advanced metering system.

Q2. What is an advanced metering system?

An advanced metering system is a system that collects time-differentiated energy usage data from advanced meters via a network system on either an on-

See Ask on page 5

Who We Are

The Electronic Technology Systems Center (ETSC) is a team within the U.S. Army Corps of Engineers that provides unmatched experience and technical expertise in the specialized fields of Utility Monitoring and Control Systems (UMCS) and Electronic Security Systems (ESS).

Located in Huntsville, Ala., the ETSC supports the Corps of Engineers, the Army, other services and various defense and federal agencies. ETSC has hundreds of active projects around the world.

In its technical consulting role, the ETSC performs engineering surveys, develops criteria, reviews designs and conducts special studies and training for a wide variety of customers. For those customers needing "turn-key" project execution, the ETSC provides indefinite delivery, indefinite quantity (ID/IQ) contracts for system engineering, procurement and installation through a seamless, expedited task order process.

Each year the ETSC participates in numerous conferences, symposia, working groups and trade shows to build relationships and influence future development and application of UMCS and ESS technology.

Point of Contact

contact-esc@usace.army.mil
256-895-1740