



US Army Corps
of Engineers ®

Electronic Technology Systems Center



Serving Customers Worldwide

Issue - June 2007

Recently Updated

Unified Facilities Guide Specifications

UFGS 21 30 00,
Fire Pumps

UFGS 26 26 00.00 40,
Power Distribution
Units

UFGS 26 27 26.00 40,
Wiring Devices

UFGS 28 05 26.00 40,
Grounding and
Bonding For
Electronic Safety and
Security

UFGS 33 71 02.00 20,
Underground
Electrical
Distribution

UFGS 34 41 26.00 10,
Access Control
Point Control
System

For more criteria and
specification
documents, go to the
Whole Building
Design Guide's
website at
www.wbdg.org

Transmission of Intrusion Detection System (IDS) Data via Army Local Area Networks (LANs)

By Craig Zeigler

In the U.S. Army, IDS data is, by regulation, transmitted via dedicated networks. Army Regulation (AR) 190-13, *The Army Physical Security Program*, states: "Transmission lines for the alarm circuits shall be electrically supervised and dedicated to minimize undetected tampering." The Office of the Provost Marshal General (OPMG) has clearly documented an interpretation of this policy statement to mean that transmitting IDS data over LANs or other shared systems is prohibited. This prohibition applies most notably to the Army installation level, where LAN connectivity typically extends to all facilities, making it an otherwise attractive choice for IDS data transmission.

Regardless of the policy, employing dedicated, stand-alone networks truly provides the most secure routing of IDS signals. The reluctance to leverage anything other than a dedicated network for IDS data transmission is understandable, and using a dedicated, stand-alone data transmission system (DTS) should be the primary choice for IDS data. However, today's networking technologies provide other options for transmitting IDS data, including LANs, wide area networks (WANs), and even the Internet.

Provided specific conditions are met, data transmission outside of a dedicated network can be performed with a high degree of security and low risk, and it is important to note that the OPMG is considering revising AR 190-13 and AR 190-11

Physical Security of Arms, Ammunition, and Explosives to allow transmission of IDS data over networks that are not dedicated to the security system. The OPMG is considering this policy change to facilitate leveraging state-of-the-art networking technologies while dictating minimum functional and security requirements for a DTS, regardless of the communications media and protocols used. The OPMG policy revision being considered will likely reflect the following provisions:

1. The primary choice for a DTS used to communicate IDS data is a stand-alone, autonomous, supervised network, operated and maintained by security personnel.

See *IDS via LAN* on page 3

Army Metering of Electrical Utilities

By Chuck Holland

The Energy Policy Act of 2005 (EPAct of 05) requires all federal facilities to be metered with advanced meters by 2012 where practicable. The Huntsville Center was selected for development and implementation of the Army-wide metering program to meet the mandate of EPAct of 05. The first group of Army installations will be surveyed, beginning in FY 08, for selection of facilities to be metered

for electrical power and energy use based on pre-selected criteria and budget constraints. The metered data will be collected and transmitted to a central location on site for manipulation of the data in a format of reports and graphs to facilitate the use of the metered data to create awareness and motivation to save energy. In order to maximize the number of installed meters, existing post-wide utility monitoring and control systems (UMCS) will be utilized to collect, transmit, and present the

meter data. Other Army installations will require the use of wireless radio frequency (RF) data transmission, power line carrier systems utilizing broadband transmission, and web-enabled meters. The metering of other utilities such as water, steam, and gas are considerations awaiting funding and their application will be considered when selecting and applying the electrical metering at each Army location.

LONWORKS Support Available for Installations

By Will White

The Huntsville Mandatory Center of Expertise for Utility Monitoring and Control Systems (UMCS) has teamed with the Engineer Research Development Center Construction Engineering Research Laboratory (ERDC-CERL) and the Savannah Directory of Expertise for HVAC Controls to provide technical support to installations interested in the transition to LonWorks® direct digital control technology.

The Installation Management Command (IMCOM) LonWorks® Building Automation Systems Implementation Plan outlines the approach. This plan was co-authored by CERL, Savannah District, and Huntsville.

Many believe LonWorks® offers an Open system with the best chance for an installation

to free itself from the clutches of proprietary controls and high prices. An Open system, in short, is one where there is no future dependence on the original installing Contractor. For the purposes of procurement, this means that there is no sole source dependence on any Contractor for future system additions, upgrades, or modifications.

Currently, there are 5 sites on the list to receive support: Fort Lee, Fort Bliss, Fort Bragg, Fort Sill, and Fort Hood. A team of engineers will visit each Army installation for about a week to provide fundamental training to the Building Automation System (BAS) workgroup for a successful LonWorks® implementation. They will coordinate, survey, train, and identify the path forward.

The approach as outlined in the Implementation Plan is:

- Assemble a Work Group
- Identify Issues, Goals, and Obstacles
- Develop Implementation Plan
- Develop performance work statement (PWS) to obtain external technical assistance
- Coordinate with internal and external organizations/entities
- Coordinate with DOIM
- Identify building integration approach (including funding & contracting mechanism)
- Develop UMCS PWS (including Source Selection criteria)
- Define/develop building acceptance methodology and checklists
- Define training requirements
- Develop Installation Design Guide (IDG) requirements

- Execute UMCS procurement

As this plan unfolds this summer, we expect to see installation engineers recognize the value of an open protocol standard in the competitive controls industry to save procurement dollars on the many new buildings needed for the Army's realignment. This IMCOM investment will pay dividends for many years as energy managers learn to maximize their efficiencies and save Army dollars. We will seek additional funding from IMCOM to expand this program to all installations that have needs to go Open.

Impact of Regulations on Selection and Manufacture of Future Power Supplies

By Jeff Alford

On a recent ETSC project, intrusion detection system processors and related components were installed in field distribution boxes (FDBs) along a perimeter fence line. Communications between the FDBs and the head-end was via a fiber-connected RS-485 data network. A thermostatically-controlled heater was installed in each FDB to protect electronic components during the extremely cold winter conditions at the site. A single 13.6 VDC switching power supply was used in each FDB to feed both the IDS equipment and heater.

While attempting to test the exterior IDS equipment, several intermittent communication failure alarms were annunciated

at the head-end, with most of these failures lasting a short duration before clearing. The DC power circuits for the IDS equipment were checked, and voltage levels seemed adequate. It was noted that the exterior IDS equipment operates within an allowable range of 11-16 VDC. Further troubleshooting utilized an oscilloscope to analyze both the power supply circuit and the communications circuit at the FDB. A constant high-frequency noise level of approximately 4 volts peak-to-peak was present on the power supply circuit with an occasional 12-volt peak-to-peak noise level occurring when the heaters were activated. The communications signal was measured to be a relatively clean square wave with a 4-volt positive magnitude. The communications equipment has

a typical poll-and-response data rate of 9-bits each with a quiescent period, and a poll-and-response reset with a longer quiescent period. Noise during the quiescent period was apparently interpreted as a parity error, causing a retransmit. Therefore, the troubleshooting process pointed to the noise generated by the switching power supply when the heater started as the most likely cause of the communication failure alarms.

To eliminate these alarms, separate power supplies and cabling were used for the IDS equipment and heaters. In each FDB, the switching power supply was configured to feed the IDS equipment only, and a new linear power supply was installed for the heaters. This allowed the heaters to draw

power as required from the linear power supply without affecting the power for the IDS equipment.

RECOMMENDATION: When thermostatically-controlled devices such as heaters and heat exchangers are required for an enclosure, designers and installers should consider isolating these devices from electronic components by using separate power supplies. This will reduce the potential for introducing noise into the electronics through the power circuit.

IDS via LAN

Continued from page 1

2. The DTS used to communicate IDS data shall assure complete data availability, confidentiality and integrity throughout the system, end-to-end. The DTS shall be secured against tampering, jamming, interception, interference and intrusion by employing line supervision, tamper detection and, when required by specific system security standards, data encryption.

A. The system shall supervise the signal lines by monitoring the circuit for changes or disturbances in the signal, and for conditions as described in Unified Facilities Guide Specification 28 20 01.00 10, *Electronic Security System* for line security equipment. The system shall initiate an alarm in response to a change or disturbance in the signal. The system shall also initiate an alarm in response to opening, closing, shorting, or grounding of the signal.

B. When encryption is required, IDS data shall be encrypted using a National Institute of Science and Technology (NIST) approved algorithm with a minimum of 128-bit encryption.

3. If a dedicated network is not available, achievable or deemed not cost effective, an alternative DTS may be used. An alternative DTS may consist of a LAN, WAN, wireless communications system or a combination of these technologies. The decision to employ an alternative DTS should be based on the results of a risk assessment conducted

jointly by designated representatives of the installation commander, the using unit or activity, and the supporting installation provost marshal or equivalent security officer representative. The risk assessment shall be conducted in accordance with the requirements in AR 25-2 and be performed according to the guidance found in the NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems." The following provisions apply to the alternative DTS:

A. The DTS must provide an equivalent, or higher, level of security for the IDS data compared to a dedicated network.

B. Vulnerabilities identified during the risk assessment and corresponding mitigation measures must be documented.

C. The Designated Approving Authority (DAA) accepts and approves the risk assessment report, including the mitigation measures identified and incorpo-

rated into the design and installation of the DTS.

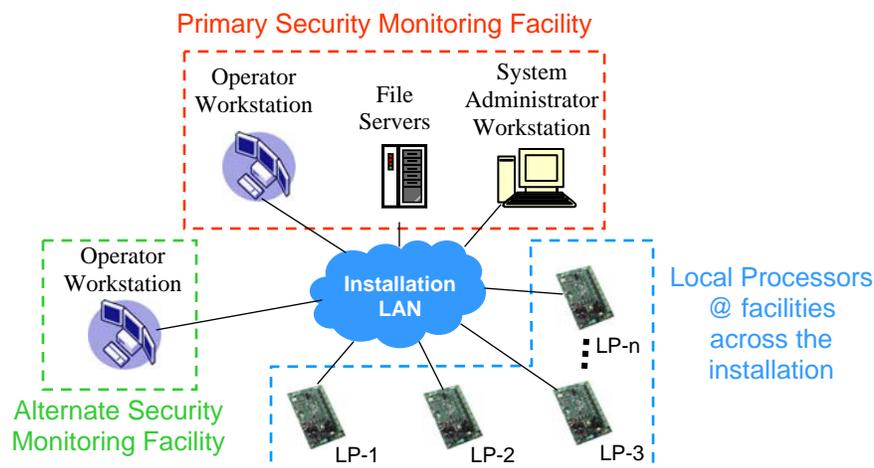
D. If a LAN is selected as the DTS, the LAN must have a minimum availability rating of 99.9%. This equates to a total yearly downtime of just under nine hours.

E. If the selected DTS cannot achieve an equivalent, or higher, level of protection for the IDS data a dedicated network provides, a second independent means of communicating the data from the protected area to the monitoring station should be provided. The dual transmission equipment must continuously monitor the integrity of both links. Upon loss of either communications path, the system must immediately send a communications fault alarm to the monitoring facility via the active link and then automatically switch to this link for any subsequent IDS alarms.

Although shared networks offer potential for economical and effective IDS data transmission, it is clear that, until OPMG revises the applicable regulations, transmitting IDS data over an Army installation LAN,

or any other network not dedicated to the security system, is prohibited. If future revisions to Army policy do allow the use of an alternative DTS, project planning and network integration will be the keys to success.

The Directorate of Information Management (DOIM) must be consulted early in the project planning phase when considering an installation LAN for transmitting IDS data. A few of the more important issues to resolve relative to the LAN infrastructure (cables, hubs, switches, routers, servers, etc.) are emergency backup power, physical & electronic protection, IDS data rate & latency, supervision & encryption of virtual IDS circuits, and priority of IDS data on the network. Another important topic to address with the DOIM is the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) as it applies to IDS processors, file servers, workstations, and system software. Finally, the day-to-day operation and maintenance of the LAN, to include the technical and security qualifications of DOIM technicians, should be discussed.



Concept for IDS Data Transmission via LAN at Army Installations

US Army Corps of Engineers
4820 University Square
Huntsville, AL 35816-1822

Phone: 256-895-1740
DSN: 760-1740
Fax: 256-895-1519

We're on the Web!

www.hnd.usace.army.mil/esc

- History of ESC
- Why Choose ESC?
- List of Clients
- Services We Offer

www.hnd.usace.army.mil/umcs

- What UMCS can provide
- Why Choose UMCS?

Ask ETSC!

Q: How do I register for the ESS Design Course or the ICIDS Operator Training Course?

A: First, check the course web page (<https://eko.usace.army.mil/training/ess/> or https://eko.usace.army.mil/training/icids_training/) to see the schedule of upcoming sessions.

After you determine which session you would like to attend, just email a registration request to Contact-ESC@usace.army.mil. Please include your name, job title, organization, and contact information along with the specific session you would like to attend. You will receive an email reply indicating your registration status including any further instructions for completing the

registration process. The availability of seats in any given session can vary, depending on the needs of the sponsoring organization.

If you have a question that you would like answered, please send your question to:

Contact-ESC@usace.army.mil

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, AL, the ETSC supports the Corps of Engineers, the Army, other Services, as well as many DoD and Federal agencies. The mission of the ETSC is global and includes 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 actively participates in numerous conferences, symposia, working groups, and trade shows to build relationships throughout Government and Industry and to influence future development and application of UMCS and ESS technology.



ETSC Points of Contact

Darrel Anerton, ETSC Chief

256-895-1741

darrel.l.anerton@usace.army.mil

Jeffrey Mitchell, ESS Program Manager

256-895-1243

jeffrey.b.mitchell@usace.army.mil

Steven Willoughby, ESS Technical Deputy

256-895-1757

steven.a.willoughby@usace.army.mil

Laura Mabee, UMCS Program Manager

256-895-8235

laura.w.mabee@usace.army.mil

Chuck Holland, UMCS Technical Deputy

256-895-1749

charles.w.holland@usace.army.mil

Leigh Young, MCX Program Manager

256-895-1403

melinda.l.young@usace.army.mil

Ken Haynes, MCX Technical Deputy

256-895-1747

doyce.k.haynes@usace.army.mil