



US ARMY CORPS
of ENGINEERS

ELECTRONIC
TECHNOLOGY
SYSTEMS
CENTER

Unmatched experience
and technical expertise
make Huntsville Center
the recognized leader
for electronic systems

Volume 1, February Issue, 2006



Controlled Exit Door Vulnerabilities

Doors secured with an electronic entry control system (EECS) must provide a means of authorized egress for personnel inside the controlled space. A request to exit (REX) device performs this function via two concurrent actions. First, the REX must cause the locking/latching mechanism to release and allow the door to swing open. Second, REX activation must shunt the door position switch alarm. Consequently, no alarm is generated if the door is opened through appropriate use of the REX device. Four general categories of REX devices are in common use throughout the electronic entry control industry:

1) Bars/handles: Normally incorporated into the door egress hardware, these devices have an electronic connection into the EECS which accomplishes the door switch shunt function. Depending on the device, the door release can also be electronically or mechanically activated.

2) Buttons: Possibly the most familiar in a DoD environment, the REX button is normally mounted in a highly visible location in the personnel egress path. Door release and alarm shunt is accomplished by depressing the button.

3) Motion sensors: REX motion sensors are very common in the commercial office environment. These devices normally consist of a passive infrared motion sensor with a curtain pattern. When an individual approaches the controlled door from the secure side, the REX motion sensor detects the motion causing the door to be released and the alarm shunted.

4) Card readers/keypads: Use of card readers and, in some instances, keypads as the REX device controls secure area egress in the same manner in which ingress is controlled. The use of these devices as the REX indicating agent is commonly seen in areas where building occupancy count is desired during emergency evacuation events or in high security applications.

The control of passage from a secure area will in some circumstances have life safety implications. In many cases, REX devices control passage along an emergency route. Therefore, the requirements of the authority having jurisdiction (AHJ) must be well understood and adhered to. Except in highly secure environments, the AHJ will often require a means to override the REX devices. Because of the variety of REX configurations and the associated life safety implications, it is important that security system designers and physical security inspectors have a basic understanding of REX devices, including their role in routine door operation as well as their potential to be exploited by a trained adversary to gain unauthorized entrance into a facility.

see EXIT DOORS page 2

EXIT DOORS *continued*

Locking/Latching Hardware. A door equipped for electronic entry control must have an electrically-activated locking/latching mechanism that interfaces with the REX device. Several hardware options are available including electromagnetic locks, electric bolts, and electric strikes. Generally, a design analysis for a given door will determine a smart pairing of REX and locking/latching device taking into account security, life safety, aesthetics, ergonomics, and wiring. The vulnerability analysis and mitigation information presented below addresses REX operation with any type of locking/latching hardware, realizing that the specific REX/lock/latch combination will vary from door to door.

Life Safety Considerations. No discussion of electronic entry control is complete without considering “means of egress” requirements set forth in NFPA 101®, *Life Safety Code*® and the interpretation and enforcement of these requirements by the AHJ for a specific facility. For REX devices, particular attention should be paid to code instructions regarding mounting constraints and operation methods. Achieving a proper balance between security and life safety is best accomplished by promoting dialog between the security designer and the AHJ in the early planning stages of a project. The discussion in this article is focused on the security application and implications of REX devices; actual, site specific implementation will be subject to the local AHJ.

REX Vulnerability Analysis. The postulated threat to an EECS controlled door is an individual on the non-secure side of the door attempting to activate the REX device and gain access to the secured space without “forcing” entry or triggering an intrusion alarm. The ability of an adversary to accomplish this task is based on several factors, the most important of which is the accessibility, both visual and physical, of the REX device. The ability of the adversary

to readily see the REX device (for example, through a glass door) greatly enhances his ability to plan and execute an unauthorized entry, taking into account the type and position of the device. The mechanics of REX activation (for example, pushing a button) dictates the degree of physical access required by the adversary to trigger the device from outside the secured space. Mounting location and configuration can greatly influence the mechanics of activating the device, particularly from the opposite side of the door. In some cases, a small opening near the door (for example, between the floor and the bottom of the door) may provide enough physical access for a skilled adversary to activate the REX device and gain unauthorized entry.

REX Vulnerability Mitigation. The first step to mitigate REX vulnerability, regardless of the device type, is to make every effort to eliminate, or severely restrict, visual and physical accessibility from the non-secure side of the controlled door. Appropriate device selection also plays a key role in mitigating REX vulnerability, taking into account the level of security desired. General guidelines for device selection are presented below. Another technique to mitigate REX vulnerability is to secure the door with a manual, deadbolt lock after normal duty hours when the area is unoccupied.

High Security. A card reader/ keypad is, by far, the most difficult REX device for an adversary to defeat. In this scenario, visual and physical access is not enough; the adversary must also have a valid card and/or personal identification number (PIN), in which case he would simply use the card reader/keypad on the non-secure side of the door to enter the secure space. In addition to virtually eliminating concerns over REX vulnerability, a dual reader/keypad configuration (one on each side of the door) will facilitate advanced access control features such as occupant tracking and anti-passback.

Medium Security. Several device types fit this category, offering varying degrees of protection. Probably the least vulnerable medium security configuration is a button mounted some distance away from the door assembly where accessibility to a potential adversary is limited. REX bars and handles also fit the medium security category but are somewhat more vulnerable since their physical attachment to the door promotes easier access by an adversary. The common strength of all medium security REX devices is the precise nature of their activation technique consisting of a specific action (touch, push, pull, etc.) directed at a specific location (bar, handle, button, etc.). These techniques can be difficult to perform from outside the secure area when access to the device is properly restricted.

Low Security. The only REX device that fits this category is a motion sensor. Typically mounted above the door and aimed down, this device offers convenient “hands-free” egress for occupants; however this convenience is gained at the expense of added vulnerability to unauthorized entry. Unlike medium security devices, REX motion sensors are imprecise in their activation technique, responding to random movement of both humans and other objects in their coverage area. This motion sensitivity can be exploited by an adversary to trigger activation using commonly known techniques requiring only a slight opening near the door. The adversary can also monitor the door for false REX activations from sources inside the secure space, listening for the locking device to release and timing his entrance accordingly.

The correct REX approach is a function of the specifics of the facility, the asset to be protected, the level of the threat, and the regulatory guidance. With proper and careful analysis of these factors and selection of appropriate door hardware, the risk associated with unauthorized REX activation can be minimized.



NEW SPECIFICATION FOR UMCS & DDC FOR HVAC TESTING

The U. S. Army Engineering Support Center, Huntsville, with support from E M C Engineers, Inc., has completed the development of a new UMCS testing specification, Section 25 08 10. This new Unified Facilities Guide Specification (UFGS) covers factory, performance verification, and endurance test procedures for the Utility Monitoring and Control System (UMCS) and Direct Digital Control for HVAC. An engineer specifying a control system on a DoD project will need to decide which of the tests covered in the new specification will be required, based on the size and type of system. For example, the engineer may choose to make the factory test a contract option on a smaller project.

The specification was written for a host-based system where the LonWorks® LNS database resides on the main computer (server) and communicates over the Ethernet (TCP/IP) connection to the field level controller nodes. The testing specification will test various UMCS server hardware and software, IP network hardware and software and building point of connection (BPOC) hardware and software, as well as the interfaces to the DDC systems. The specification was written to be used in conjunction with UMCS specification section 25 10 10 and Direct Digital Control for HVAC and Other Local Building Systems section 23 09 23. There are over twenty system tests the contractor performs to demonstrate the control system is operating correctly. The test procedures in the specification do not cover functional testing of control sequences performed by the HVAC systems; this is covered in the DDC for HVAC specification section 23 09 23.



An example of how the specification will be used for control system testing:

- A UMCS and/or DDC for HVAC project is awarded.
- The Contractor completes the submittal process.
- As a contract option, the Contractor provides a factory test plan and procedures for review and approval by the Government. Test procedures are developed by the contractor by customizing the 20+ tests from the specification into project specific, system specific tests.

see DDC & HVAC TESTING page 4

For more information contact one of the ETSC project managers at 256-895-1756.

ETSC POINT OF CONTACT

PHONE: (256) 895-1740

Contact-ESC@hnd01.usace.army.mil

UPCOMING ELECTRONIC SECURITY SYSTEM COURSES

- 23 - 27 January 2006 - *ESS Design Course, Huntsville, AL*
- 06 - 10 February 2006 - *ESS Design Course, Seoul, Korea*
- 27 February - 3 March 2006 - *ESS Design Course, Huntsville, AL*
- 14 - 16 March 2006 - *ICIDS Operator Course - # 06-01*
- 27 - 31 March 2006 - *ACP Training (Salt Lake City, UT)*
- 24 - 28 April 2006 - *ESS Design Course (Tentative)*
- 1 - 5 May 2006 - *ACP Training (San Antonio, TX)*
- 16 - 18 May 2006 - *ICIDS Operator Course - # 06-02*
- 5 - 9 June 2006 - *ACP Training (Charleston, SC)*
- 26 - 30 June 2006 - *ESS Design Course (Anchorage, AK, Tentative)*
- 17 - 21 July 2006 - *ESS Design Course (Germany)*
- 24-28 July 2006 - *ESS Design Course (Tentative)*
- 18 - 20 July 2006 - *ICIDS Operator Course - # 06-03*
- 28 August - 1 September 2006 - *ESS Design Course (Location TBD)*
- 29 - 31 August 2006 - *ICIDS Operator Course - # 06-04*

Please check the ESS Design Course web page
<https://eko.usace.army.mil/training/ess/>
and the ICIDS Operator Course web page
https://eko.usace.army.mil/training/icids_training/
for up-to-date information on each session.

TESTING from page 3

- Once the procedure and plan is approved, the Contractor performs the factory test at a company site for a Government Representative. The contractor performs the basic functions of the UMCS and building level DDC to assure that the performance requirements of the specifications are met.
- After successful completion of the factory test, the contractor is approved to install and checkout the control systems.
- As part of the 25 10 10 and 23 09 23 specifications, there are control system start-up requirements, including point checkout, point calibration, loop tuning, network testing, actuator range check, and functional control sequence checking. All these requirements must be completed and documented before performance verification testing.
- The contractor prepares a performance verification test plan and procedures for review and approval by the Government. Again, the test procedures are developed by the contractor by customizing the 20+ tests from the specification into project specific, system specific tests.
- Once all the start-up tests are completed and approved and the test procedures and plans are approved, the contractor performs the performance verification test for a Government Representative on the installed control systems at the site.
- At the successful completion of the performance verification test, the contractor goes into the endurance test, which is designed to demonstrate the specified overall system reliability requirement of the completed system.
- The endurance test runs the system for two sets of 24 hour, 15 day tests. If the system operates with little or no system failure, the test is passed.
- If there were problems during the endurance test, the contractor identifies the failures, determines the causes of all failures, repair all failures, and submits a test failure report to the Government.

Words of warning to project managers and project engineers: Make sure to take into account the added time and cost for good testing and building commissioning to assure a proper working UMCS and DDC systems.