Civil Engineer (CE) Industrial Control Systems (ICS) and Information Assurance (IA)

Mr. Mark Correll, SES
AF/A7C
26 March 2013
Version #1.2
ICS Cyber Security Evolution

Future ICS (Integrated ICS – Late 2000’s)

Current ICS (Early 2000’s)

Past ICS (1990’s and Prior)

- Specialized Software
- Specialized Hardware
- Proprietary Protocols
- Isolated Systems/Closed Network Architecture

- Networking Multiple Systems
- Enhanced Features (Middleware, Security, etc.)
- Internet Protocol (IP) Based
- Remote Access
- Unsecured Architecture
- Open Network Architecture

Increased cyber vulnerability and incidents

Security through “obscurity” is an Obsolete Strategy
AF CE ICS Inventory

- **Fire/Life Safety Systems**: Building Fire Alarm Reporting and Mass Notification Systems
- **Building Automation Systems**: HVAC Controls, Interior/Exterior Lighting Controls, Irrigation Systems, etc.
- **Utility Monitoring and Control Systems**: Electrical, Water, Wastewater, and Natural Gas distribution systems, Chlorination Generators and Utility Meters
- **Airfield Control Systems**: Airfield Lighting, Ramp Lighting, Aircraft Arresting Systems, Runway Ice Detection System, and Bird Scare
- **Vehicle Traffic Control Systems**: Traffic Signals and Drop-arm Barriers

AF CE has over an estimated 1,800 ICS in Operation
AF CE Challenges

- Legacy Industrial Control Systems (ICSs) lack modern cyber security protection and Information Assurance (IA) controls
- CE ICSs are designed to last and operate for decades and tech refresh of Information Technology (IT) assets is problematic
- True ICS isolation is difficult, costly, and often impractical
- ICS configurations (hardware, software, and mode of communication) vary from installation to installation even within same manufacturer/vendor product line
- Base ICS technicians lack the necessary IA and IT skills to identify, mitigate, and monitor system vulnerabilities and risks
- AF CE has no dedicated or fenced funding for securing ICS from cyber threats

ICS Technicians Operate & Maintain nearly 4,500 IT Servers and 11,000 Computer Workstations
2011

- Established centralized ICS program within CE to address cyber security issues
- Established partnership with AF Communications (Comm) Community to jointly solve ICS cyber security problem
- Released guidance to CE on cyber security, CE ICS determination, and acquisitioning governance
- Began conducting risk assessments of CE ICS across USAF

2012

- Developed the CE Virtual Local Area Network (CE VLAN) toward enterprising ICS, deployed at 6 AF installations
- Assessed 39 AF Installations across 7 AF Major Commands
- Participants in OSD AT&L Enterprise Energy Implementation Management (EEIM) Working Group

146 Risk Assessments Complete w/ 39 ATOs
Way Ahead

- Continue conducting on-site risk/vulnerability assessments
- Continue mitigating known vulnerabilities. Logically separate ICSs from the AF-GIG IAW CE ICS PIT DAA Approved Virtual Local Area Network (VLAN) that utilizes Virtual Routing and Forwarding across Base Comm Infrastructure.
- Continue incorporating IA into new system acquisitions
- Continue supporting new energy savings and conservation improvement projects by providing secure data transport solutions and data storage capabilities
- Continue to capitalize on existing base communications infrastructure assets and enterprise services
- Develop a comprehensive, enterprise-wide ICS solution to consolidate, modernize and standardize AF ICS systems that are commonly isolated and proprietary
CE ICS Point of Contact

Mr. Tarone Watley, P.E., Security+, GS-13
Chief, Civil Engineer Maintenance, Inspection and Repair Team (CEMRIT) Industrial Controls System (ICS) Branch
AFCEC/COMI
(850) 283-6736
DSN 312-523-6736
(888) AFCESA1, ext 283-6736
afcec.comi.ics@tyndall.af.mil

ICS and IA Definitions

- **Industrial Control System (ICS).** A general term for several types of control systems, including Supervisory Control and Data Acquisition (SCADA) systems, Digital Control Systems (DCSs), and other control system configurations such as skid-mounted or panel-mounted Programmable Logic Controllers (PLCs) often found in the industrial sector and critical infrastructure. ICSs are typically used in utility/industrial systems such as electrical, water, wastewater, oil and natural gas, chemical, transportation, and discrete manufacturing such as automotive, and aerospace industries.

- **Information Assurance (IA).** Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.