Leveraging A Secure Wireless Network for Automation and Control

Thurston Brooks & Keith Byerly
VP Product Marketing
Ultra Electronics, 3eTI
September 26, 2012
Introduction

- The US DoD/DHS are leading the way in defining, validating and deploying highly secure, industrial control systems.

- Information Assurance and Defense in Depth security concepts are being adopted by ISA for industrial automation and control applications.

- ISA100 incorporates “basic” security by design.

- Additional layers of security based on proven DoD solutions will address security concerns that are inhibiting adoption of industrial wireless sensor networks in Federal networks.
Industrial Automation and Control Systems
Evolving Security Threats

- 1970 to 1990s: Security by Obscurity
  - Legacy proprietary protocols
  - Isolated systems
- Today
  - Open standards-based protocols
  - Enterprise and control networks, applications and systems interconnected by IP
  - Expanded network security perimeter

Threat Vectors
- Backdoors, holes in network perimeter
- Vulnerabilities in common protocols
- Database attacks
- Communications hijacking and ‘man-in-the-middle’ attacks
- Insecure devices
- Wireless networks
Industrial Automation and Control Systems
ISA99 Security Standards

• Security Context
  – Threats, risks, and countermeasures
  – Relationships between them

• Security Objectives
  – CIA/AIC

• Security Concepts
  – Defense in Depth
  – Threat-Risk Assessment
  – Security Program Maturity
  – Security Policies
  – Role Based Access Control
Industrial Automation and Control Systems
ISA100 Security by Design

- **Authentication and Encryption**
  - Guarantee messages received truly originated by an authorized device and have not been modified
  - Data confidentiality provided via advanced AES encryption
  - Symmetric keys used for data encryption and authentication

- **Security Policies**
  - Based on authentication and authorization

- **Time-Based Security**
  - Time stamps provide protection against replay and delay attacks
ISA100 Security by Design Authentication and Encryption

• **Link Layer**
  – Hop-to-hop authentication and encryption of packets at Layer 2
  – Provides protection within the 802.15.4 mesh

• **Transport Layer**
  – End-to-end authentication and encryption of Protocol Data Units (PDUs) at Layer 5
  – Secure sessions established between IP ports at originating device and destination device
ISA100 Security by Design
Symmetric Keys

- **Global Key**
  - Well known key (not secure)

- **Join Key**
  - Created at the conclusion of symmetric key provisioning
  - Used to join the network, receive the Master Key

- **Master Key**
  - Created at the conclusion of the key agreement scheme
  - Used for communication between Security Manager and devices
  - Expires and needs to be periodically updated

- **DL Key**
  - Used to compute the Message Integrity Code (MIC) at the link layer
  - Expires and needs to be periodically updated

- **Session Key (Optional)**
  - Used to encrypt and/or authenticate PDUs at the transport layer
  - Expires and needs to be periodically updated
• Authentication and encryption are controlled by flexible security policy
  – Can be varied at both Link and Transport layers
  – Authentication and encryption independently defined

• Security policies distributed with cryptographic material
  – Allows application-specific security levels

• Security Manager
  – Controls policies for cryptographic materials it generates
  – Manages and distributes keys
    – Asymmetric keys
    – Master keys for session key distribution
Transport layer security utilizes a time stamp for protection against replay attacks (esp. important for industrial applications)

- Devices are continuously synchronized using TAI (atomic international time)
- Time stamp in the nonce needed for AES-128 indicates when each data packet was created
- Packets older than N seconds (configurable) will be discarded by recipient
Industrial Automation and Control Systems
The WSN Security Challenge

Most Important WSN Features

- **Data reliability**: 99% 97%
- **Data security**: 86% 90%
- **Standards**: 81% 70%
- **Plant-wide network**: 59% 52%
- **Easy access to data**: 69% 72%
- **IP addressability**: 56% 48%
- **Lower cost**: 60% 59%
- **No battery changes**: 70% 68%

Inhibitors to WSN Adoption

- **Security concerns**: 60% 56%
- **Battery lifetime**: 56% 54%
- **High costs**: 55% 51%
- **Data reliability**: 46% 48%
- **Lack of standards**: 45% 46%
- **Complexity**: 42% 42%
- **Education**: 41% 40%
- **Available products**: 29% 37%
- **No need**: 26% 26%

Source: ON World
A. Secure IP network connection to server
   - End users connect to server via SSL / HTTPS - no path to field devices
   - Access to the network is restricted to the system server’s specific IP and port
   - 802.1x port security ensures all physical connections are authenticated prior to network access

B. Secure wireless network connection
   - Wireless Intrusion Detection System (WIDS)
   - FIPS 140-2 & Common Criteria EAL4 Certified encryption and security

C. Embedded firewall w/Deep Packet Inspection
   - Stateful validation of protocol payload
   - Access Control Lists, port scanning

D. Enhanced SCADA controller
   - Secure, validated configuration
   - 802.1x port security

E. Locked, monitored enclosure
   - Physical security w/intrusion prevention and detection
   - Physical access automatically generates alarm at operator console
DoD – Cyber Security Initiative - DIACAP
Defense Information Assurance, Certification & Accreditation Process

- DoDI 8510.01 DoD Information Assurance Certification and Accreditation Process (DIACAP)
  - Federal Information Security Management Act (FISMA) of 2002
  - DoDD 8100.1 Global Information Grid (GIG) Overarching Policy
  - DoDD 8500.01 Information Assurance (IA)
  - DoDI 8500.2 Information Assurance (IA) Implementation

- IA Controls are determined based on the system's mission assurance category (MAC) and confidentiality level (CL).
## U.S. Government – Cyber Security Initiatives

### DIACAP vs. NIST IA

#### Integrated DIACAP / NIST Accreditation Strategy

- Reduce vulnerabilities through integrated IA approach
- Combine DIACAP and NIST IA controls into accreditation package for interoperable protection against cyberthreats
- Validate IA packages independently such as via DIACAP / NIST Validators and / or National SCADA Testbed (INL)

---

### DIACAP/Platform IT

**Defense IA Certification & Accreditation Program**

1. **Initiate and Plan IA C&A**
   - Register System with DoD Component IA program
   - Assign IA Controls
   - Assemble DIACAP Team
   - Initiate DIACAP Implementation Plan

2. **Implement and Validate Assigned IA Controls**
   - Execute DIACAP Implementation Plan
   - Conduct Validation Activities
   - Compile Validation Results in DIACAP Scorecard

3. **Make Certification Determination & Accreditation Decision**
   - Make Certification Determination
   - Issue Accreditation Decision

4. **Maintain Authority to Operate and Conduct Reviews**
   - Maintain Situational Awareness (Review of IA Controls must occur at least annually)
   - Maintain IA posture

5. **Decommission**
   - Retire System

---

### NIST Process

**IA Process for Civilian Government Agencies**

1. **Start the Process**
   - **ORGANIZATIONAL VIEW**
     - Risk Executive Function
     - Starting Point

2. **Select Security Controls**
   - **Step 2 SELECT Security Controls**
     - FIPS 200 / SP 800-53

3. **Implement Security Plan**
   - **Step 3 IMPLEMENT Security Controls**
     - SP 800-70

4. **Assess Security Controls**
   - **Step 4 ASSESS Security Controls**
     - SP 800-53A

5. **Authorize Information Systems**
   - **Step 5 AUTHORIZE Information Systems**
     - SP 800-37

6. **Monitor Security State**
   - **Step 6 MONITOR Security State**
     - SP 800-37 / 800-53A

---

**Architectural Description**

- FEA Reference Models, Segment and Solution Architectures, Mission and Business Processes, Information System Boundaries

---

**National SCADA Testbed (INL)**

---

---
Unified Capabilities Approved Products List

- Unified Capabilities Certification Office (UCCO) for all DOD
  - DISA drafts UC-APL requirements.
  - TIC drafts test cases for vendor equipment
    - Products may have different mix of functions.
  - Vendor must be sponsored to be tested.
  - Both IA and Interoperability required for APL listing.

Unified Capabilities Approved Products List

Ultra Electronics | 3eTI - © 2012
The WSN Security Challenge
Enhanced Confidentiality: FIPS 140-2

• Local Requirements
  – Correctness of implementation or deployment
    – cryptographic boundaries, random bit generators

• Algorithmic Requirements
  – Known-answer tests for algorithms
  – Assure interoperability
  – Symmetric key encryption w/AES, hashing using SHA-1
  – AES-CCM used to protect the data exchanged
  – Defined approved key establishment techniques
    – Diffie-Hellman, EAP-TLS
The WSN Security Challenge
Enhanced Integrity: Common Criteria

• Unlike FIPS 140, CC does not provide a list of product security requirements or features that they must contain.

• ISO/IEC 15408 describes a framework in which:
  – system users can specify their security requirements
  – vendors can then implement and/or make claims about the security attributes of their products
  – testing laboratories evaluate the products to determine that they actually meet the claims.
The WSN Security Solution Overview
The WSN Security Solution
Federal/DoD Implementation Options

• Low-Power Sensor Crypto Library
  – Optimized for battery-powered applications
  – Incorporates FIPS security into wireless sensor software

• Sensor, Gateway Crypto Modules
  – All-in-one ISA100 wireless modules with FIPS security and CC Evaluated
  – Integrates secure wireless technology into wired sensors

• Sensor Node and Gateway Devices
  – ISA100-compliant nodes provide secure, universal network connectivity to sensors and meters
  – Gateway seamlessly and securely bridges 802.15.4/ISA100, 802.11/Wi-Fi and 802.3/Ethernet networks using accepted certifications (FIPS 140, CC, IA, UC-APL)
Conclusion

• The US DoD & DHS are leading the way in defining, validating and deploying highly secure, industrial control systems

• Information Assurance (CIA-AIC) and Defense in Depth security concepts have been adopted by ISA for industrial automation and control applications

• ISA100 incorporates basic security by design

• Additional layers of security based on proven DoD solutions can help address security concerns that are inhibiting adoption of industrial wireless sensor networks into Federal applications
Q & A

Thurston Brooks
Vice President, Product Marketing
3eTI
thurston.brooks@ultra-3eti.com
+1 301.944.1343
Thurston Brooks, VP of Product Marketing

- Developed new technologies and solutions for industrial and commercial applications for the protection of critical infrastructure.
- More than 30 years of professional experience in developing and managing a wide variety of solutions for military and industrial applications.
- Engineering Degrees from the University of Florida (BS) and the Massachusetts Institute of Technology (MS) with a thesis in Human-Machine Systems and Controls and an MBA from the University of Chicago.
- 45+ publications in referred Journals, Symposiums and Conferences
Agenda

• Secure Wireless Sensor Networks in the DoD
  – Information Assurance / CIA
  – Defense in Depth

• Industrial Automation and Control Systems
  – Evolving Security Threats
  – ISA99 Security Standards
  – ISA100 Security by Design
    – Enhanced Confidentiality: FIPS 140-2
    – Enhanced Integrity: Common Criteria
About 3eTI
About 3eTI

- Founded in 1995
- Headquartered in Rockville, MD
- Technology company with ~16 patents
- ~90 employees
- Fully owned subsidiary of Ultra Electronics
  - $1.1B+ Public company (London Stock Exchange)
  - 26 business units
3eTI provides highly secure wireless networks that enable critical systems security, infrastructure security and industrial automation for the military, government, industry and utility markets.

### Wireless Mesh Networks
Robust and scalable networks that assure delivery and security of your integrated video, data

### CyberFence™
Military-grade protection of IP networks that cannot be pinged, hacked or compromised

### Wireless Sensor Networks
Scalable networks that monitor environmental conditions and enable control activity

### VirtualFence™
Out-of-the-box wireless video surveillance and auto-detection systems
**What We Do**

**Onboard Ship Communications**
Secure wireless access to shipboard networks

**Virtual Perimeter Monitoring**
Virtual perimeter monitoring with remote video and sensors

**Advanced Metering Infrastructure (AMI)**
DoD
Real-time, advanced monitoring and collection of building-by-building energy usage

**Energy Management and Resource Management**
Integrated, adaptive, intelligent energy management on a building, base and region level

**Vessel Boarding Communications**
Wireless reach back system for video, data, and voice connectivity with boarding teams

**Military Base Security**
Remote 24-hour monitoring and intrusion detection systems