U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

Secure Software-Defined Radio Project

Secure, versatile radio for "last mile" communications to utility distribution automation devices

Background

Communication to and from utility distribution automation devices provides greater system reliability and uptime, faster restoration, and more cost effective operations. However, many of these utility devices are located in remote locations, making secure communications difficult. Wired communication such as fiber optic cabling can be prohibitively expensive, and while wireless radio communication can offer a cost effective alternative, current capabilities may not offer adequate security. It is important to secure communications at this "last mile" of the utility network to prevent compromise from adversaries.

Barriers

- Most energy delivery system radios lack security capabilities found in wired communications, such as authentication of users and devices, event and access logging, encryption, disabling of unused ports, and intelligent password and network key management.
- Many radios have data throughput below 1 megabit per second (Mbps), limiting the use of radio links to low-throughput applications.
- Currently, multiple radios are required to effectively support different distribution automation applications, such as Ethernet SCADA, Engineering Access, and Mirrored Bits.

Project Description

The Secure Software-Defined Radio Project (SEL-3070) is developing a flexible platform for secure wireless communications to utility distribution automation devices, providing capabilities not offered in cellular, narrow-band licensed, or other unlicensed-band radios.

The versatility of the platform enables the ability to support communications for multiple applications in one radio while also providing precise time distribution across the wireless network. The platform is managed through a web interface using standardized management and messaging protocols, with advanced monitoring and troubleshooting tools. Multiple Ethernet and serial ports allow for connections to various types of distribution automation devices.

Security features include access through a secure web interface, strong passwords tied to user accounts, event and device access logging, advanced encryption with temporal keys, and user and device authentication.

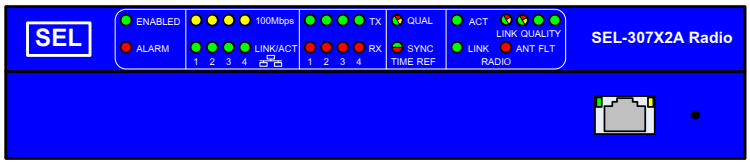
Performance improvements over conventional radios include 3-4 times faster data throughput, low latency, message prioritization, and adaptive channel access for multiple users.

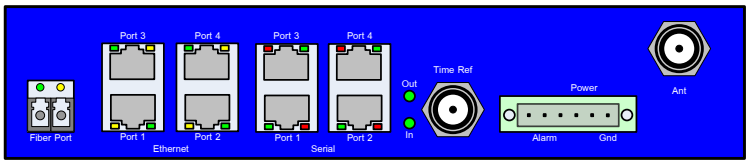
Benefits

- Enables security for wireless radio communications with capabilities found in standard wired communications infrastructure, supporting several encryption and authentication standards
- Simplifies system design by using one radio for multiple communication applications and protocols
- Provides precise time synchronization to remote distribution automation devices across the radio link
- Provides high throughput and low system latency for applications like synchrophasors, video, IEC-61850 GOOSE, and large file transfers
- Supports adaptive modulation and coding for efficient use of channel bandwidth

Partners

- **Schweitzer Engineering Laboratories (SEL)**
- San Diego Gas and Electric
- Pacific Northwest National Laboratory





SEL-3070 schematic: Four Ethernet ports, four Serial ports, IRIG Time Sync port, Alarm contact, Threaded Neill-Concelman (TNC) connector, Fiber Ethernet port (optional)

Technical Objectives

This project is developing a secure, flexible platform for wireless radio communications to utility distribution automation devices. Technical specifications include:

Security:

- User Authentication: Role-based Access Controls, Lightweight Directory Access Protocol (LDAP), and Remote Authentication Dial In User Service (RADIUS)
- Device Authentication: Media Access Control (MAC) filtering, IEEE 802.1x access control, and message authentication over wireless links
- Encryption: 256-bit Advanced Encryption Standard (AES) and temporal keys

Versatility:

- Ability to pass Ethernet Supervisory Control and Data Acquisition (SCADA) information, International Electrotechnical Commission (IEC) 61850 Generic Object Oriented Substation Events (GOOSE) messaging, Engineering Access, and Mirrored Bits
- Inter-range Instrumentation Group (IRIG) time distribution
- Management: Syslog event logging and messaging, and Simple Network Management Protocol (SNMP)
- 4 standard Ethernet and 4 standard Serial ports

Performance:

- Max data rate: 5-10 Mbps
- Max range: over 20 miles point-to-point (P2P) and 16 miles point-to-multipoint (P2MP)
- Latency: under 10 milliseconds (ms) per hop
- Channel bandwidth: 5 megahertz (MHz)
- Adaptive Time Division Multiple Access (TDMA)

Phase 1: Product Development

- Investigate technology
- Design and develop system specifications
- Develop and test prototype hardware
- Develop and validate application and wireless system firmware

Phase 2: Field Demonstration and Validation

- Conduct laboratory validation with utility partner
- Conduct field demonstration and performance assessment with utility customer

End Results

Project results will include the following:

- Radio platform that secures "last mile" wireless communications to remote utility sites and provides superior versatility and performance
- White paper on industry benefits
- White paper on field demonstration results and lessons learned

January 2015

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) research and development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyber attacks.

Contact Information:

Carol Hawk
Program Manager
DOE OE R&D
202-586-3247
carol.hawk@hq.doe.gov

Henry Loehner
Development Manager
Schweitzer Engineering Laboratories
509-592-5220
henry_loehner@selinc.com

For More Information:

- http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity
- www.controlsystemsroadmap.net