U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

Rhett Smith

Hallmark Project

CenterPoint Energy

SEL

Pacific Northwest National Laboratory

Operated by Battelle for the U.S. Department of Energy

Hallmark Project

- **Outcomes:** Commercial solutions available to secure serial communications in a scalable, cost-effective manner that covers Engineering access and SCADA and provides a clear path for interoperability

SEL-3025
SCADA SHIELD
SEL
SCHWEITZER ENGINEERING LABORATORIES
MADE IN PULLMAN, WASHINGTON USA
SEL
SEL-3025
SCADA SHIELD
STATUS
CRYPTO
DEVICE

- **Roadmap Challenge:** Inherent trust in serial control system protocols. Major product replacement and firmware upgrades are to costly
- **Major Successes:** Commercialization of OEM and end user products. Successful lab and interoperability tests

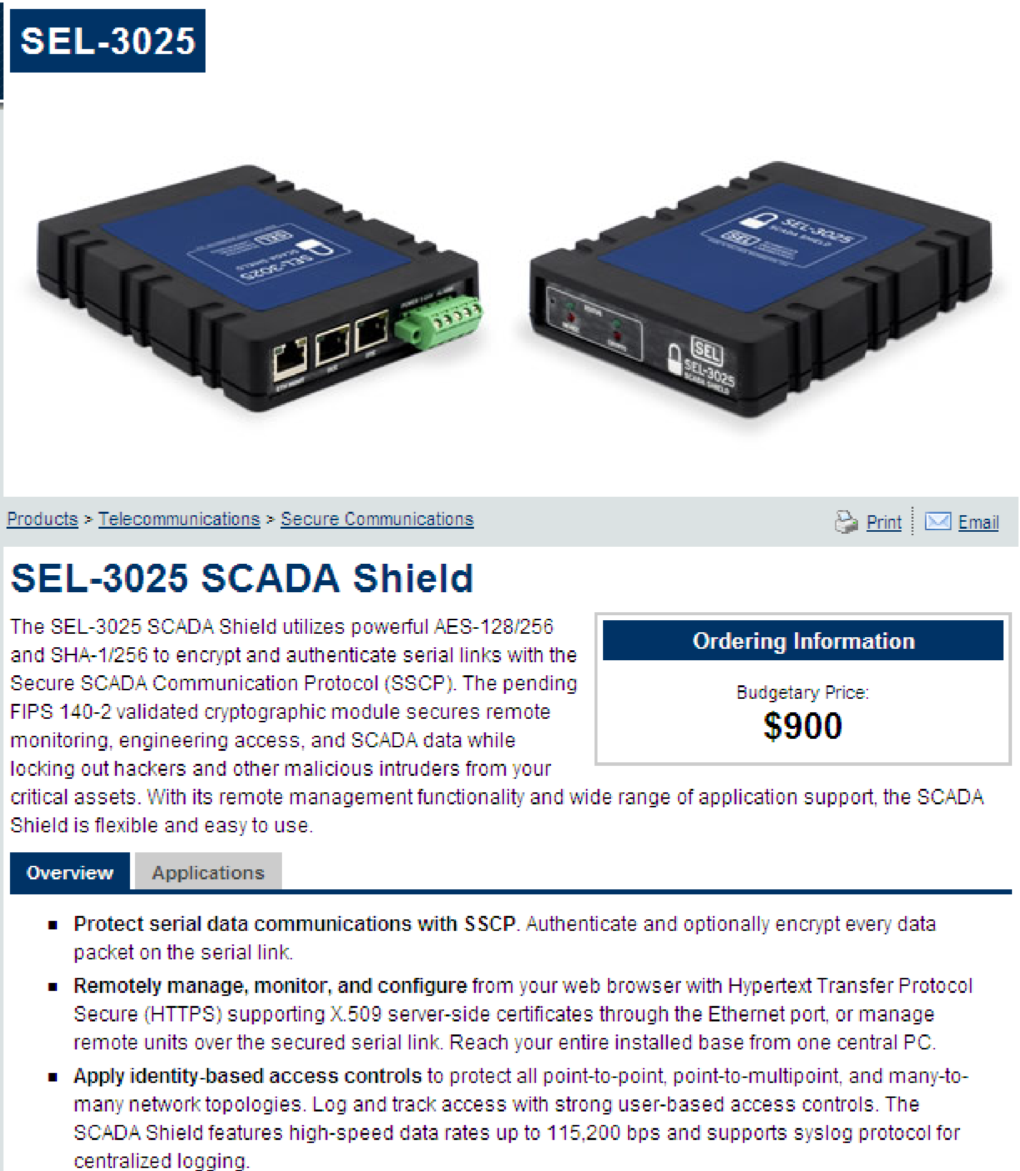
- **Schedule:** Interoperability test, lab test, and commercialization all complete
- **Level of Effort:** $1,353,191
- **Funds Remaining:** $346,808
- **Performers:** CenterPoint, PNNL, SEL

Design for Long Term Success

- Tech transfer SSCP from PNNL to industry
- Identify use cases and management process
- Develop products
    - OEM
    - Asset owner
- Test and deploy products
- Easy to use
- Clear path for integration and interoperability

SSCP
SEL-3045
SECURE SCADA CARD
SCHWEITZER ENGINEERING LABORATORIES
SEL
MADE IN PULLMAN, WASHINGTON USA
WARNING: NOT A PCMCIA CARD. USE WITH SEL APPROVED PRODUCTS ONLY.

Metrics for Success



SEL-3025

Products > Telecommunications > Secure Communications   Print | Email

SEL-3025 SCADA Shield

The SEL-3025 SCADA Shield utilizes powerful AES-128/256 and SHA-1/256 to encrypt and authenticate serial links with the Secure SCADA Communication Protocol (SSCP). The pending FIPS 140-2 validated cryptographic module secures remote monitoring, engineering access, and SCADA data while locking out hackers and other malicious intruders from your critical assets. With its remote management functionality and wide range of application support, the SCADA Shield is flexible and easy to use.

Ordering Information

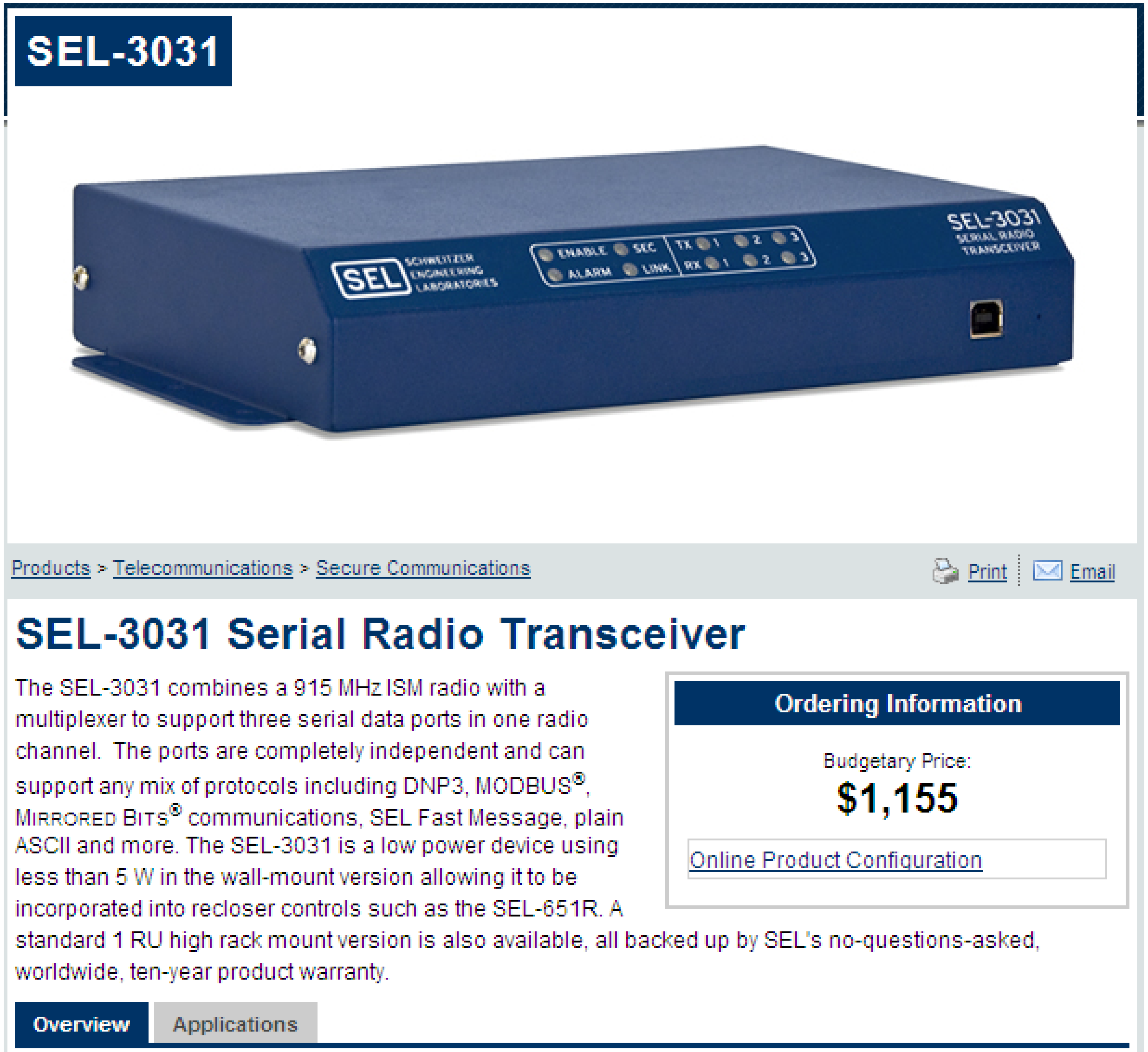
Budgetary Price:

$900

- **Protect serial data communications with SSCP.** Authenticate and optionally encrypt every data packet on the serial link.
- **Remotely manage, monitor, and configure** from your web browser with Hypertext Transfer Protocol Secure (HTTPS) supporting X.509 server-side certificates through the Ethernet port, or manage remote units over the secured serial link. Reach your entire installed base from one central PC.
- **Apply identity-based access controls** to protect all point-to-point, point-to-multipoint, and many-to-many network topologies. Log and track access with strong user-based access controls. The SCADA Shield features high-speed data rates up to 115,200 bps and supports syslog protocol for centralized logging.

- Pass protection level reliability testing
- Successful testing
  - – Legacy systems
  - – Negative
  - – Interoperability
  - – OEM’able
- Selling, supporting, and protecting

Metrics for Success
Proven Growth Path



SEL-3031

SEL SCHWEITZER ENGINEERING LABORATORIES
ENABLE
SEC
ALARM
LINK
TX 1 2 3
RX 1 2 3
SEL-3031 SERIAL RADIO TRANSCEIVER

Products > Telecommunications > Secure Communications   Print | Email

SEL-3031 Serial Radio Transceiver

The SEL-3031 combines a 915 MHz ISM radio with a multiplexer to support three serial data ports in one radio channel. The ports are completely independent and can support any mix of protocols including DNP3, MODBUS®, Mirrored Bits® communications, SEL Fast Message, plain ASCII and more. The SEL-3031 is a low power device using less than 5 W in the wall-mount version allowing it to be incorporated into recloser controls such as the SEL-651R. A standard 1 RU high rack mount version is also available, all backed up by SEL's no-questions-asked, worldwide, ten-year product warranty.

Ordering Information

Budgetary Price:

$1,155

Online Product Configuration

Overview | Applications

IEEE

Advancing Technology for Humanity

IEC

Challenges and Lessons Learned

- Technology Transfer (PNNL)
  - Many face-to-face visits and conference calls
- Solving the total business needs (CenterPoint)
  - Many face-to-face visits and conference calls
- Developing a product that supports reliability (SEL)
  - Use protection relay development processes

Lessons learned about what “done” looks like:

- To the point the technology works
- To the point the technology can’t fail
- To the point it can’t fail and easy to use

Technical Achievements to Date

- Commercialize SSCP
- OEM kit available (hardware, software)
- End user bump-in-the-wire product complete
- Scalable and maintainable solution proven through technology and processes
- Security assurance through FIPS validation and robust negative testing
- Successful interoperability (PNNL and Siemens)
- SEL products released and customer orders
- Standards development started

Collaboration/Technology Transfer

- **Plans to gain industry input**
  - CenterPoint kept technical development focused on solving the business need
  - SEL worked closely with many customers in development and has sold production units for field deployment
- **Plans to transfer technology/knowledge to end user**
  - For sale and supported by SEL
  - Standards are being developed (IEEEP1711)
  - Shown to work in bump-in-the-wire and capable of being integrated in end devices.
  - **It is protecting our electric sector systems as we speak!**

Potential Follow-on Work

- **Technology Development**
  - Middleware and USB docking station to secure all serial engineering access
  - Central management software
- **Industry Integration**
  - IEEE and IEC standards
  - Field deployment case studies
  - OEM integration
- **Timeline and budget**
  - Additional 12 months
  - $914,777 (DOE+PNNL) and $530,565 cost share (SEL)