



**Process Control Systems
Industry Conference**



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

Hallmark Project



Pacific Northwest National Laboratory
Operated by Battelle for the U.S. Department of Energy

DOE Roadmap Vision

- ◆ In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyberassault with no loss of critical function
- ◆ Goals
 - Measure and assess security posture
 - Develop and integrate protective measures
 - Detect intrusion and implement response strategies
 - Sustain security improvements

DOE Roadmap Challenges

- ◆ Coordination of research and development (R&D)
- ◆ Focused R&D efforts
- ◆ Ongoing oversight and industry involvement



DOE Roadmap and Hallmark Project

- ◆ Goal – develop and integrate protective measures
- ◆ Milestone – see widespread implementation of scalable and cost-effective, secure communications between remote access devices and control centers
- ◆ Challenge – match industry security objectives, operational requirements, and R&D efforts

Hallmark Project

- ◆ Plug-in module: upgrade security, not primary equipment
- ◆ OEM cryptographic card
- ◆ FIPS 140-3 validation
- ◆ Bump-in-the-wire link module running Secure SCADA Communications Protocol (SSCP)
- ◆ Scalable and maintainable deployment

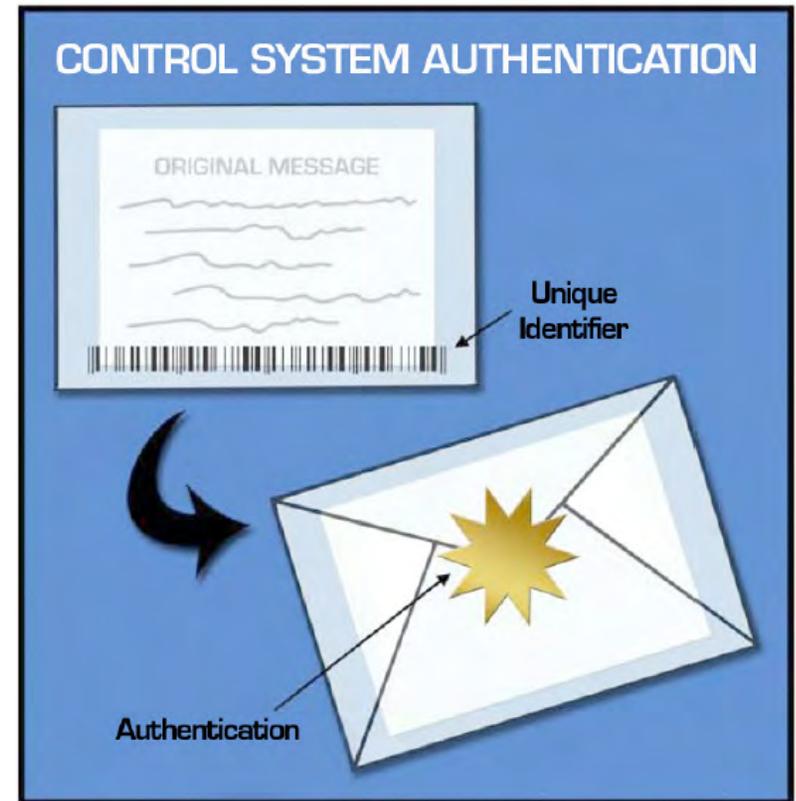


SSCP

- ◆ Originally funded by National Center for Advanced Secure Systems Research (NCASSR) through Office of Naval Research
- ◆ Field-tested at CenterPoint Energy in their production substations running DNP protocol
- ◆ Secures all byte-oriented protocols
- ◆ Provides message integrity
- ◆ Protects current, future, and legacy systems

SSCP

- ◆ Adds unique identifier to each message
- ◆ Computes hash with unique identifier and message
- ◆ Validates before accepted
- ◆ Uses unique cryptographic keys per device
- ◆ Supports two in-band methods to update session keys



Cryptographic OEM Card

- ◆ PCMCIA form factor
- ◆ FIPS 140-2 validated
- ◆ Development kit
- ◆ SSCP
- ◆ OEM and commercial product
- ◆ Prototypes April 2009



Impact Analysis and Best Practices Reports

- ◆ Impact on control system
- ◆ Impact on operators and engineers
- ◆ Best practices for deployment and maintenance

