Paul Skare

PNNL

PNNL CEDS Projects Overview

Cybersecurity for Energy Delivery Systems Peer Review

August 5-6, 2014

IEC 61850 Cybersecurity Acceleration R&D

Start/End: FY12/FY 14

Purpose: Accelerate introduction of secure products to market for IEC 61850

Challenge: Standards are conflicting and confusing. Vendors are competing. There is no cyber security interoperability test tool.

– Roadmap Goal 1.5

Technical Results: Met with vendors to identify IEC 61850 cyber security issues. Worked to update the IEC standards. Developed conformance test tools for the vendors to test how their products work with other vendor's products. Designed Interoperability environment.

Major Deliverables: Conformance test tool, interoperability test capability

Vendor Feedback Results

"Can we have the conformance tool now?"

They need to revise their own budgets and roadmaps to integrate and use our work

They see value in the laboratory leading by example with PNNL hosting the lab with devices, and allowing remote accessibility.

Performers: PNNL, ANL

Partners: ABB, Alstom Grid, GE, Schneider-Electric, Siemens

EDS Procurement Language

Start/End: FY13/FY 14

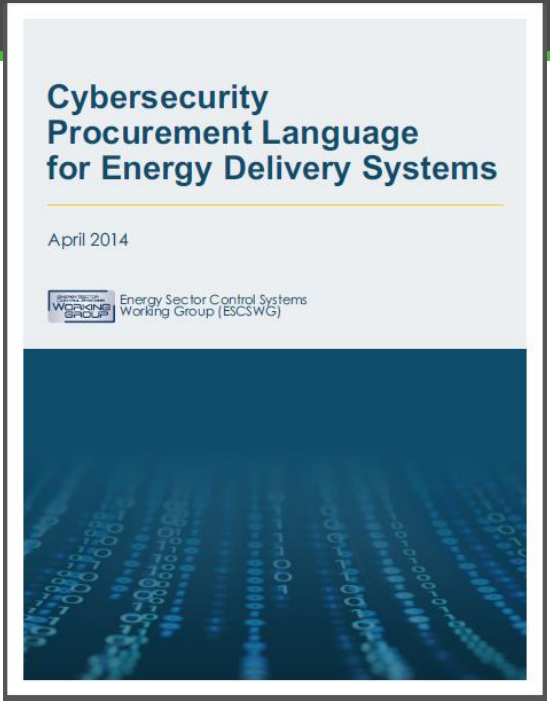
Purpose: Enable the EDS industry to easily include cyber security requirements in their procurement documents

Challenge: Vendors will not develop security features if they are not specified in procurement documents. Utilities would benefit from a guidance document to aid them in defining their requirements

- ***Roadmap Goal*** *1.5*

Technical Approach: Review existing procurement guidance and then work with SMEs to create a streamlined, user-friendly guidance document tailored to energy delivery systems.

Major Deliverables: *Cybersecurity Procurement Language for Energy Delivery Systems (April 2014)*



Cybersecurity Procurement Language for Energy Delivery Systems

April 2014

Energy Sector Control Systems Working Group (ESCSWG)

- **Performers:** PNNL
- **Partners:** Energy Sector Coordinating Council, ICS-CERT, Duke Energy, EEI, Energetics, EPRI, FERC, IESO (Ontario), and UTC. Additional contributions from the APPA, AGA, and INL.

Facilitate Secure ICCP Rollout

Start/End: FY13/FY 15

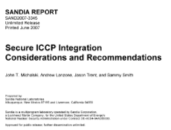
Purpose: **Work with Utilities and Peak RC to turn on Secure ICCP associations at strategic select existing installations.**

Challenge: **Utilities have received Secure ICCP products for many years (standard defined in 2003), but have not turned on the secure aspect. There has been a lack of coordination on how to setup and share certificates and a lack of direction to enable security.**

- ***Roadmap Milestone*** *1.3*

Technical Approach: **Write a white paper on how to define and manage certificates and how to turn on, operate, debug, and maintain secure ICCP connections. Work with the Peak RC to define a CA concept for the keys, and facilitate strategic utilities to begin the process. Support the industry to let the industry complete the work. Informed by SAND2007-3345.**

Major Deliverables: **Coordination, site visits, white paper and final report**



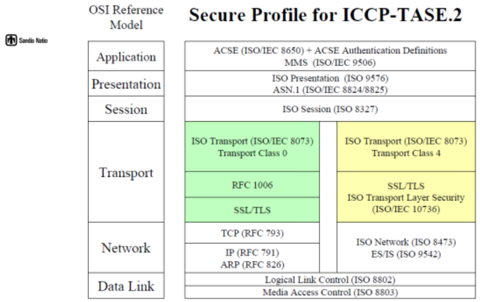
SANDIA REPORT
SAND2007-3345
Unlimited Release
Printed June 2007

Secure ICCP Integration Considerations and Recommendations

John T. Michalski, Andrew Lanzone, Jason Trent, and Sammy Smith

ENERGY

Secure Data Transfer Guidance for Industrial Control and SCADA Systems



OSI Reference Model

Secure Profile for ICCP-TASE.2

OSI Reference Model		
Application	ACSE (ISO/IEC 8650) + ACSE Authentication Definitions MMS (ISO/IEC 9506)	
Presentation	ISO Presentation (ISO 9576) ASN.1 (ISO/IEC 8824/8825)	
Session	ISO Session (ISO 8327)	
Transport	ISO Transport (ISO/IEC 8073) Transport Class 0	ISO Transport (ISO/IEC 8073) Transport Class 4
	RFC 1006	SSL/TLS ISO Transport Layer Security (ISO/IEC 10736)
	SSL/TLS	
Network	TCP (RFC 793)	ISO Network (ISO 8473) ES/IS (ISO 9542)
	IP (RFC 791) ARP (RFC 826)	
Data Link	Logical Link Control (ISO 8802)	
	Media Access Control (ISO 8803)	

- **Performers:** PNNL
- **Partners: Peak RC / 3** Utilities, Alstom Grid

Cybersecurity for EMS Decision Support Tools

Start/End: FY13/FY 15

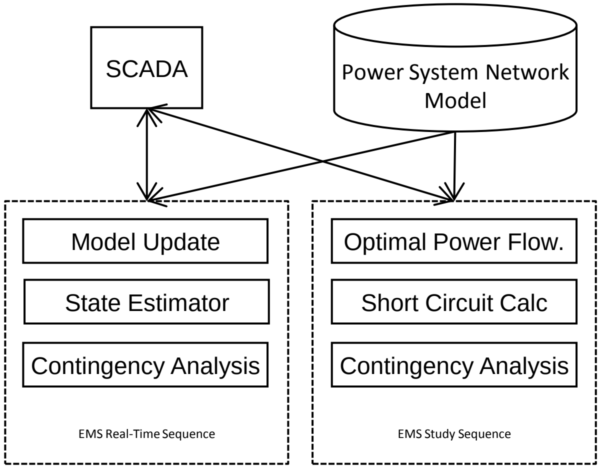
Purpose: Define cybersecurity functions that can be added to EMS decision support tools.

Challenge: Understand where EMSs can be extended to include Cybersecurity in the decision support process. Functions such as *State Estimator (SE)* and *Contingency Analysis (CA)* can consider the impacts of cybersecurity scenarios in their *EMS study functions*.

- ***Roadmap Milestone 2.3***

Technical Approach: In EMS power system planning functions, consider *SE* observability regarding each communications channel, and adding cybersecurity contingencies into the existing *CA* function and associated alarms. Develop concepts, algorithms and mockups of a prototypical EMS user interface, and review with partners.

Major Deliverables: Technical report on real-world applicability including mockups of prototypical user interfaces.



- **Performers:** PNNL
- **Partners:** Alstom Grid, Siemens, CenterPoint Energy, Sempra/SDG&E

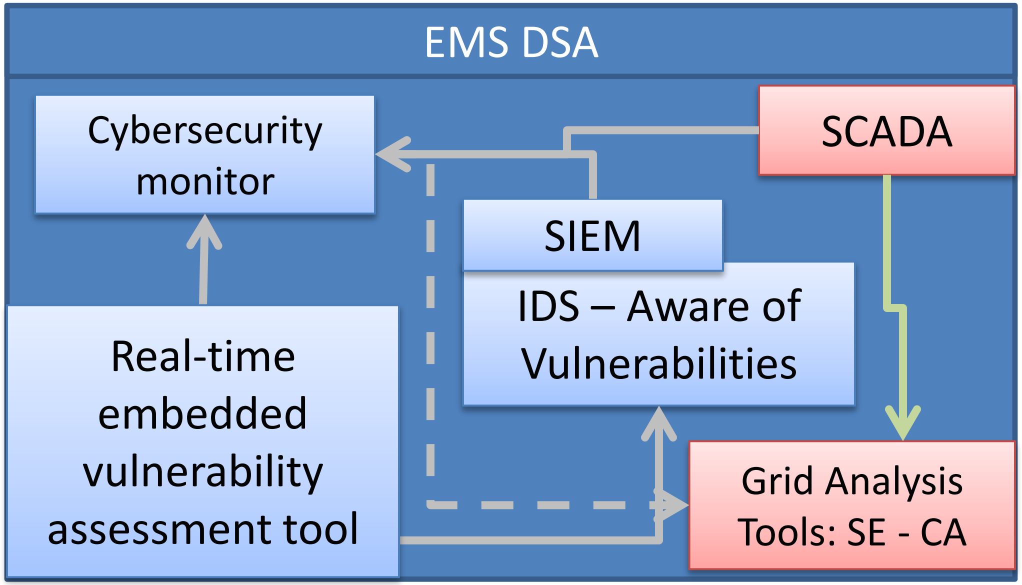
FEDSEC

Start/End: FY14/FY 16

Purpose: Federate data models for utility control centers in order to increase cyber security information sharing in the context of energy delivery.

Challenge: Interoperability, Information Sharing, and Situational Awareness is inhibited by the many data models such as IEC TC 57 CIM, DMTF CIM, and NIEM for cyber components.

– ***Roadmap Milestone 2.1***


EMS DSA
Cybersecurity monitor
SCADA
SIEM
IDS – Aware of Vulnerabilities
Real-time embedded vulnerability assessment tool
Grid Analysis Tools: SE - CA

- **Performers:** PNNL
- **Partners:** UISOL, ERCOT, TVA

Technical Approach: Create a generalized framework to align the different cyber security aspects of the domain models that can be used by a utility.

Major Deliverables: A framework aligning multiple UML models into a single profile including mockups of prototypical user interfaces.