

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

FEBRUARY EPC MEETING

Date **2/24/2015**

Time Start-End **2:00-2:50 PM**

Attendees

Tim Clancy (Arch Street LLC)
Dion Bigornia (West Monroe Partners)
Mike Manske (West Monroe Partners)
Irene Gassko (Florida Power and Light)
Sanju Misra (Praxair)
Landon Roeder (NESPower)

Jim McCarthy (NCCoE)
Don Faatz (NCCoE)
Jim Bradshaw (NCCoE)
Mary Yang (NCCoE)

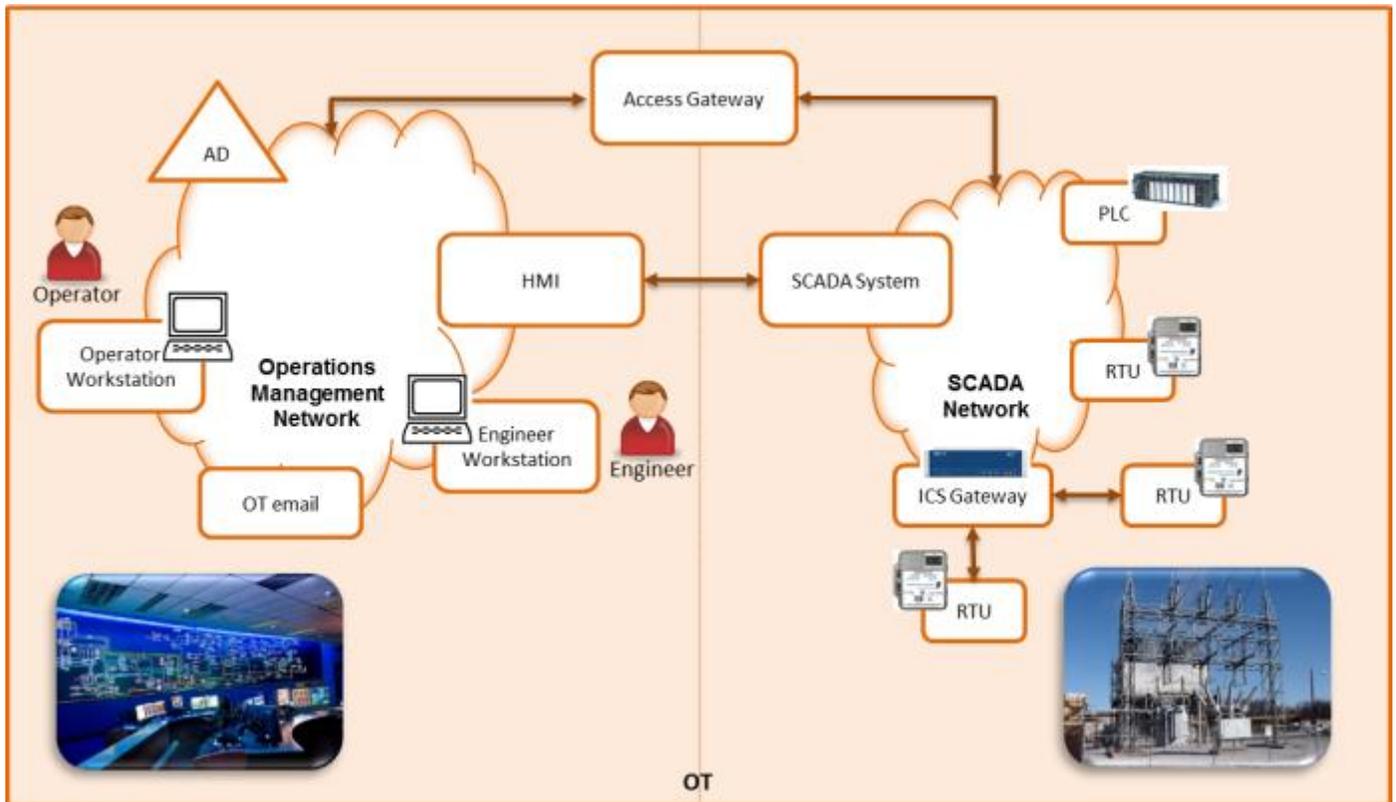
Discussion

- Jim McCarthy asked the community members to review Ron Beck’s comments regarding substation connectivity on the NCCoE Energy Sector Forum accessible from the NCCoE Web page <http://nccoe.nist.gov/forums/energy>.
- Jim McCarthy provided the current status of the IdAM Use Case build:

CRADA Partner	Status
CA	Scheduled to install Identity Manager on Feb. 25
RSA	Adaptive Directory and IMG have been installed. Currently configuring IdAM workflows in IMG.
MAG	Ozone has been installed. Certificates are needed to replace the default self-signed certificates used at installation.
AlertEnterprise	Preparing a VM image of Guardian for installation.
XTec	Installed.
Globalsign	Issuance of NAESB certificates for NCCoE IdAM users planned for Feb. 27.
TDi	Scheduled to install Console Works beginning Feb. 9.
Radiflow	Device is in the lab. Scheduled integration on Feb. 24.
Cisco	ISE will be added once other products are installed and working.

- NCCoE is configuring IdAM Build operating systems using the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs).
 - STIG’s provide a secure baseline configuration for the operating systems.
 - Deviations from the STIG-recommended configuration will be documented in the IdAM Build practice guide.
 - Some community members were familiar with STIGs. Community members did not have any recommendations for alternative security configuration guidance.
 - DISA STIGs are publically available at <http://iase.disa.mil/stigs>
- NCCoE plans to have a working version of the IdAM build in the NCCoE lab by March 1, 2015 and an initial draft practice guide for internal NCCoE review by March 23, 2015. Community members should receive a draft practice guide by mid April 2015.

- NCCoE shared a notional architecture for the Operational Technology environment (see below) derived from past discussions with community members and requested feedback on changes needed (additions, deletions, corrections) to reasonably represent current industry practice.
 - Community members discussed whether Bring-Your-Own Device (BYOD) access capabilities were needed for the Operations Management Network in the notional architecture.
 - Discussion of BYOD access concluded that community members are not currently supporting this capability but many are considering if/ how to accommodate such access. NCCoE will note this as a future capability for the notional architecture.



- Jim McCarthy provided an update on the Situation Awareness (SA) Use Case.
 - Following publication of the Federal Register Notice, NCCoE continues to receive inquiries from potentially interested vendors. Four vendors have submitted Letters-of-Interest (LOIs).
 - NCCoE is reviewing the products suggested by interested vendors to understand how the products can contribute to meeting the goals of the SA Use Case.
 - NCCoE will schedule a “Vendor Day” for vendors who have submitted LOIs. Vendors participating in Vendor Day will describe how they feel their products can be used in addressing the SA Use Case
 - Community members asked if ability to comply with DISA STIGs will be considered in selecting products for the SA Use Case
 - NCCoE is not using application STIGs only the operating system STIGs
 - Community members asked if the SA Use Case would build a centralized Security Operations Center.
 - NCCoE has not determined the SA Use Case architecture. The architecture depends on both the types of products available and the needs of the Energy Provider Community (EPC) for converged IT-OT security Situation Awareness. Available products are determined through the LOIs and Vendor Day. EPC needs will be reviewed during the March 2015 EPC meeting.
 - Following the Vendor Day, NCCoE will review potential SA Use Case architectures with the EPC members.

- Community members asked about the timeline for completing a build for the SA Use Case.
 - No schedule has been defined, however, NCCoE expects a build will be completed by late Summer 2015 with a draft practice guide provided for review in Fall 2015

Conclusion/Closing Notes or Need to Follow Up

- Attached to these minutes is a copy of “IT-OT Security Convergence for Dummies” provided by AlertEnterprise, a partner in the IdAM build. Chapter 5 of this book describes several scenarios relevant to the SA Use Case. NCCoE asks EPC members to review these scenarios prior to the March meeting as background for a discussion of EPC needs for converged IT-OT security situation awareness.