Shabbir Shamsuddin
& Virgil Hammond
Argonne National Laboratory (ANL)

ANL - DOE CEDS Projects Collaboration and Support Activities

Cybersecurity for Energy Delivery Systems Peer Review
August 5-6, 2014

Summary: Industry Outreach (ONG)

- **Objective**
  - ANL FY'14 Outreach task is to continue FY'13 Outreach effort within the oil and natural gas (ONG) sector.
  - Focus on industry issues and continued improvements in control systems security per DOE Roadmap.
  - ONG sector participants will be solicited as appropriate for their input on critical security issues, best practices, application of standards, and feedback.
- **Schedule**
  - Oct 1, 2013-Dec 31, 2014.
  - Quarterly reports to DOE
  - Trust, partnership, and information sharing will continue in FY'15

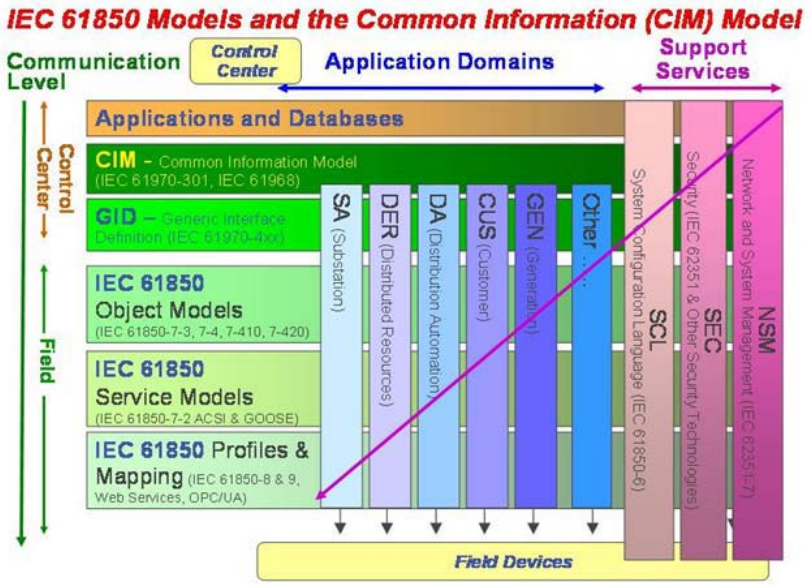
- **Total Value of Award:** ($50K)
- **% Funds expended to date:** 49 %
  Performer: Argonne National Laboratory
- **Partners:** AGA, API, INGAA, Multi-lab team

Progress to Date

- **Accomplishments**
  - ANL, in collaboration with INL and the Director at American Gas Association, supported the development of a presentation on “Cyber Impacts for Safety and Integration Decisions” presented by INL at the Gas Control Committee and for the AGA Conference industry participants at the AGA Annual Operations 2014 Conference in Pittsburgh , May 20-23,2014.
    - The presentation was very well received by the Gas Control Committee and the AGA conference participants.
  - ANL will continue to communicate and cooperate with the oil and gas sector industry organizations (AGA, INGAA, API, etc.) on various control system security bulletins, developments, and technical webinars.
  - ANL will continue the outreach effort by collaborating with and providing support for the DOE laboratories, industry, and academia under the DOE CEDS program.

Summary: IEC 61850 Cybersecurity Acceleration R&D Support

- **Objective**
  - FY'14 tasking provides for ANL 's continued support to PNNL on IEC 61850 Cybersecurity R&D.
  - Support finalizing the reference model software and testing plan.
  - Identify issues with approach from vendor feedback.
  - Introduce technical solution into the IEC



- **Schedule**
  - Oct 1, 2013-Dec 31, 2014.
  - Quarterly reports to DOE
  - Test bed and the modification of the reference model software/plug fest/closeout.

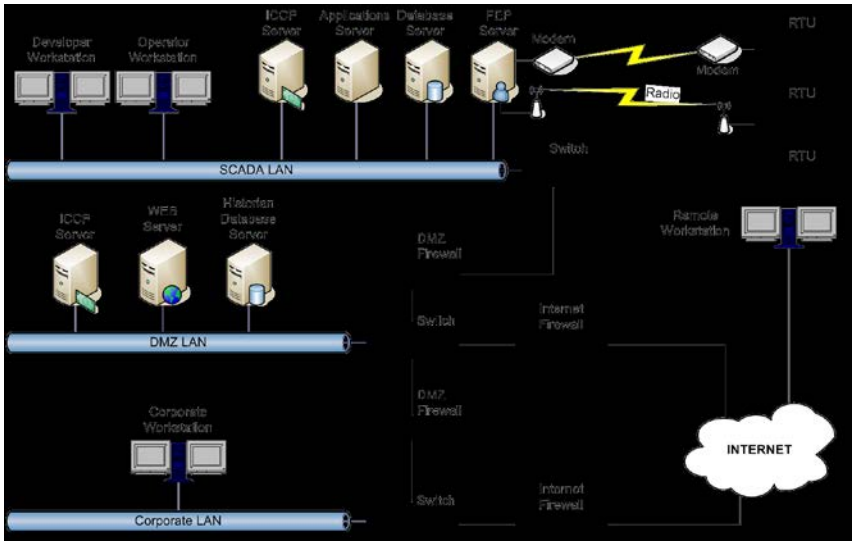
- **Total Value of Award:** ($50K)
- **% Funds expended to date:** 49%
  Performer: PNNL (Lead Lab), ANL
- **Partners:** Vendors, Asset Owners

Progress to Date

- **Accomplishments**
  - ANL continued to provide support to PNNL on the development of the IEC 61850 conformance testing design document and test scripts.
    - ANL studied the NIST Framework .
    - IEC 62351 suite of standards.
  - ANL provided support to PNNL on the IEC 61850 project and in reviewing the conformance test procedures and user guide against the IEC 62351 Part 3 and 4 standards and provided the input and comments edits to PNNL PI.
  - ANL reviewed Triangle MicroWorks Anvil and Hammer software
    - application to the testing of IEC 61850 standard requirements.
    - IEC 62351 standards requirements used in conformance testing harness.
  - ANL will continue to support and collaborate with the PNNL project team in the closeout of this project.

Summary: Vulnerability Assessment in Energy Sector under Risk Evaluation Nexus for Digital Age Energy Reliability (RENDER) Support

- **Objective**
  - FY'14 is the continuation of the ANL and INL FY'13 collaboration.
  - Recommendations made by the industry/vendor/government RENDER consortium.
  - To identify disclosed cyber exploits that will be analyzed against INL laboratory energy sector control systems.



- **Schedule**
  - Oct 1, 2013-Dec 31, 2014.
  - Quarterly reports to DOE
  - Final Report with Recommendations/closeout

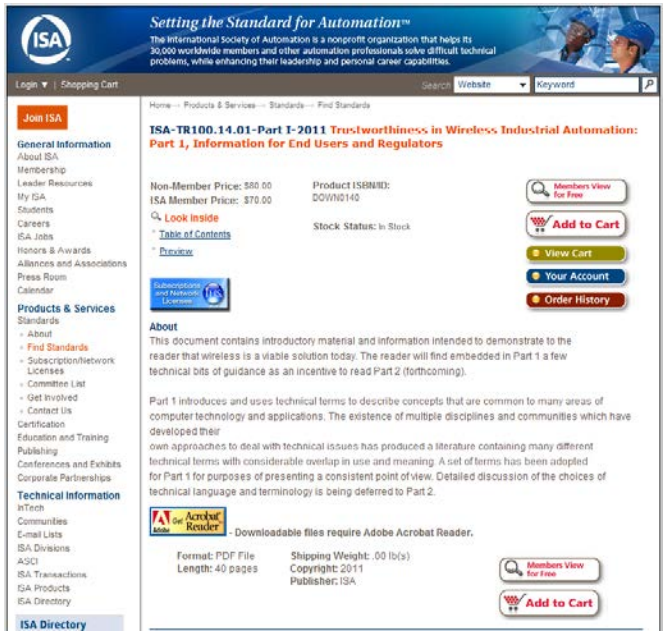
- **Total Value of Award:** ($30K)
- **% Funds expended to date:** 70%
  Performer: INL (Lead Lab), ANL
- **Partners:** Vendors, Asset Owners

Progress to Date

- **Accomplishments**
  - ANL continued support and collaboration with INL on the Risk Evaluation Nexus for Digital Age Energy Reliability (RENDER) project. ANL reviewed CRADA templates, system characterization plan , and other materials distributed by INL for the RENDER consortium review.
  - ANL provided exploit synopsis based on sector research/vendor literature on exploits such as DNP3 and cross-site scripting exploits for the RENDER consortium considerations.
  - ANL provided support to INL in the review of the RENDER final CONOPS report. ANL will continue its support to INL on the final RENDER report and the closeout of the pilot program.

Summary: Wireless Standards Development (ONG) Support

- **Objective**
  - ANL's ongoing FY'13 work in FY'14 tasking to collaborate and provide support to ISA.
  - Delivery and closeout of the work products of the ISA100 Trustworthy Wireless Working Group (WG14).
  - ISA99 Standards Working Group 4 (WG4) for energy sector benefits.
- **Schedule**
  - Oct 1, 2013-Dec 31, 2014.
  - Quarterly reports DOE
  - Standards: ISA100.11a; ISA-62443-1-3; trustworthy wireless projects closeout



- **Total Value of Award:** ($50K)
- **% Funds expended to date:** 54%
  Performer: ANL
- **Partners:** ISA100 WG14; ISA99 WG4

Progress to Date

- **Accomplishments**
  - During Q3 of FY'11, Part 1 of a planned two-part technical report was approved by the ISA100 membership. This document is titled "Trustworthiness in Wireless Industrial Automation: Part I – Information for End Users and Regulators", and is available to interested parties
  - Part 2 of the report was approved during Q3 of FY'13 and is also available to those interested. Part 2 is titled "Trustworthiness in Wireless Industrial Automation: Part 2 – Understanding the Issues Associated with Implementing a Trustworthy System"
  - Concurrent with the end of Fourth Quarter FY'13 ISA100 WG14 (TWWG) was declared inactive and ceased meeting on a regular basis. A few of the regular members, including ANL, agreed to continue the effort to develop guidelines for securely configuring an ISA100.11a wireless sensor network.

Progress to Date (contd.)

- **Accomplishments**
  - ANL's current effort during FY'14 has been to address the provisioning and joining requirements as described in the standard. Issues being investigated include;
    - security levels afforded by use of asymmetric key vs. symmetric key; and
    - provisioning over-the-air (OTA); using out-of-band (OOB) communication; wired; or infrared.
  - During Q2 of FY'14 the ISA trusted wireless working group has reduced the scope of its assessment of ISA100.11a security options to study those options directly related to the provisioning and joining activities. The effort is now envisioned to proceed at a slower pace, owing to the decommissioning of ISA100 WG14 and the resultant loss of available man-hours.

Progress to Date (contd.)

- **Accomplishments**
  - ANL continued to participate in regular (biweekly) conference calls for the wireless security effort through Q2 of FY'14. This effort was discontinued early in Q3 when it became evident that the group remaining from the original TWWG was insufficient to make consistent progress on what was already a very limited scope.
  - ANL also participates in the work of ISA99 WG4, including the work of Task Group 1 and Task Group 5 in support of the effort to further a culture of trustworthiness in control systems.
  - Task Group 5 (TG5) completed and during Q1 of FY'14 issued for ISA approval a revised draft of the proposed standard, "Security for industrial automation and control systems, Part 1-3: System security conformance metrics".

Progress to Date (contd.)

- **Accomplishments (cont'd)**
  - The draft of Part 1-3, "System security conformance metrics" was submitted to both the ISA and IEC memberships for approval vote and comments during Q3 of FY'14. Unofficial results were received just before the end of Q3.
  - The draft missed gaining approval by the ISA WG4 membership by a single vote, with about 30% of those members eligible to vote failing to do so. (Failure to vote is considered the same as a 'no' vote.)
  - The draft also failed approval by the IEC membership, but details have not yet been made available.
  - Work is underway to respond to the comments received, and to resolve the issues brought forth, to revise the draft accordingly, and to obtain a revote.

Questions?

- **Contact Information**

Shabbir A. Shamsuddin

(630) 252-6273

shamsuddin@anl.gov

Virgil B. Hammond

(630) 252-6522

vhammond@anl.gov