Paul Skare, Shabbir Shamsuddin, Josef Allen

PNNL, ANL, ORNL

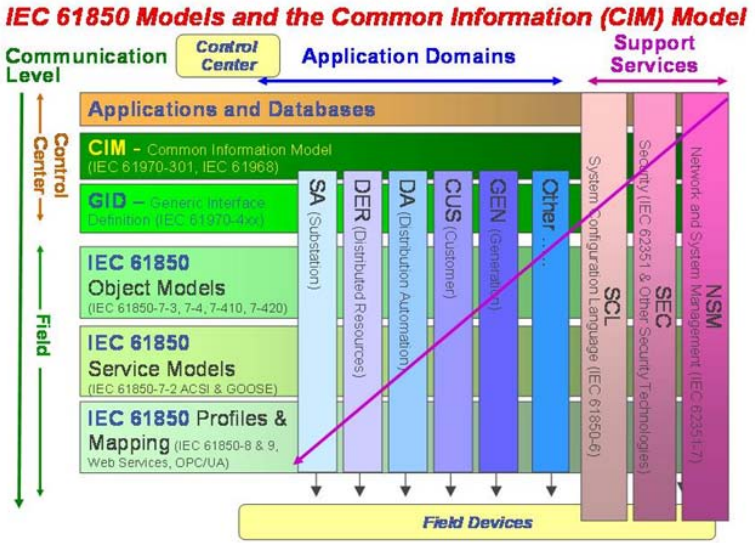
IEC 61850 Cybersecurity Acceleration R&D

Cybersecurity for Energy Delivery Systems Peer Review

July 24-26, 2012

Summary: IEC 61850 Cybersecurity Acceleration R&D

- **Objectives**
  - Goal of this project is to allow vendors to provide secure and interoperable control system solutions to the energy sector
- **Technical Approach**
  - Work with vendors to create a holistic IEC 61850 security approach
  - Develop a reference model to allow an independent test vehicle for the vendors to test



- **Schedule**
  - Key deliverables and dates expected/met
- **Performers:** PNNL, ANL, ORNL
- **Partners:** ABB, Alstom Grid, GE, Schneider-Electric, Siemens

Technical Approach and Feasibility

- **Approach**
  - Leverage existing work by IEC standards working groups draft technical standard on the communication security profiles specified within IEC 61850
  - Identify technical challenges, gaps, and mitigation
  - Creating a holistic security approach that allows vendors to implement security specified in IEC 61850 standard
  - Technical approach will be written in the IEC format and will be provided to IEC for integration into the IEC 62351 standards
  - Work with vendors to get devices compliant with IEC 61850 security and interoperability framework available for industry consumption

Technical Approach and Feasibility (contd.)

- **Challenges to Success**
  - IEC 61850 does not have a defined implementation approach for cyber security and lack of consensus between Vendors
  - Challenge is to obtain Vendor and IEC commitments and resources to participate
    - Held a Vendors Workshop to solicit feedback, and document technical challenges and gaps
  - Creation of a reference model for an independent test vehicle for vendors to test
    - Write technical approach in the IEC format and submit to IEC for approval

Progress to Date

- **Progress to Date**
  - Held IEC 61850 and 61970 CIM standards training at PNNL
  - Solicited Industry participation
  - Held Vendor workshop
  - Collected and distributed comments
  - Drafting plan for technical approach
  - Designing cybersecurity interoperability test framework

IEC 61850 Cyber security Acceleration Workshop

- Invited vendor representatives to participate in a face to face workshop
- Convened at PNNL April 25, 2012, in conjunction with Secure Coding workshop April 24.
- Participants from: ORNL, ABB, PNNL, Siemens, ANL and Alstom
- We discussed challenges with implementing IEC 62351, Interoperability needs, and future efforts
- Overall concerns: key management, sufficient interoperability, pace and motivation of adoption

Collaboration/Technology Transfer

- **Plans to gain industry input**
  - Discuss and solicit Vendor participation and agreement in the planned workshop
  - Held a first vendor workshop to identify challenges, issues, and gaps
  - Hold second workshop to discuss solutions to identified technical challenges and commitment to participate in testing the security under the proposed reference model
  - Solicit IEC input and approval on technology transfer and security framework

Collaboration/Technology Transfer (contd.)

- **Plans to transfer technology/knowledge to end user**
  - Energy Sector vendors can use this knowledge and apply the IEC 61850 technical security requirements in their products
  - Submit the reference model to IEC and obtain approval to gain industry acceptance
  - Solution allows vendors acceptance of IEC 62351-6 which specifies mechanisms for protecting IEC 61850 for substation communication security
  - Provides implementation of IEC 62351-6 without the overhead of cryptography in field equipment with severely constrained memory and processing power

IEC 61850 Cyber security Acceleration Impact

- **Year one solicited industry for challenges and roadblocks**
  (This year we heard the demand at the workshop and individually)
- **Year two the laboratory team will design and develop a framework to provide *remote* security and interoperability testing to industry (high priority need identified in year 1)**
  - Like the TVA Bradley substation experience… We are providing access to interoperability, security and performance testing.
- **Third year demonstrate framework capability with industry partners, by providing impartial access to the framework hosted at PNNL.**
  - **Another workshop with face to face for a plug fest.**

Next Steps

- **Approach for the next year or end of project**
  - Finalize the reference model software and testing plan
  - Identify issues with approach from vendor feedback
  - Introduce technical solution into the IEC process
- **Project results that may form the basis of future control systems security work or link to other programs/organizations**
  - Develop business plan for the reference model and test results for using the reference model with vendors and obtain IEC approval
- **Describe potential follow-on work, if any**
  - Setup a service center for cybersecurity interoperability tests
  - Define as part of the third year efforts
  - Cost to be included in existing third year plan

Argonne National Laboratory Collaboration

- **ANL collaboration activities to support PNNL and ORNL**
  - ANL participated in the IEC 61850 and IEC 61970 training at PNNL.
  - ANL supported the project team in soliciting select sector partners and vendors for the workshop. ANL participated in the IEC 61850 Standard Vendor and Secure Coding workshops
  - ANL will continue to assist team in the development of the security framework, solicit feedback, document challenges, and technical issues
  - ANL will continue to participate and support PNNL and ORNL in the development of a technical approach that addresses the vendor concerns, and security requirements submittal to IEC for approval
  - ANL continues to provide subject matter expertise from the oil and gas sector perspective in supporting the development of a reference model and to allow an independent test vehicle for the vendors to test their implementations against this model

Oak Ridge National Laboratory Collaboration

- **ORNL collaboration activities to support PNNL and ANL**
  - ORNL participated in the IEC 61850 and IEC 61970 training at PNNL.
  - ORNL supported the project team in soliciting select sector partners and vendors for the workshop. ORNL participated in the IEC 61850 Standard Vendor workshops
  - ORNL will continue to assist team in the development of the security framework, solicit feedback, document challenges, and technical issues
  - ORNL continues to provide subject matter expertise from the information security, cryptography and trusted computing perspective in supporting the development of a reference model and to allow an independent test vehicle for the vendors to test their implementations against this model
  - ORNL will continue to participate and support PNNL and ANL in the development of a technical approach that addresses the vendor concerns, and security requirements submittal to IEC for approval

Questions

Paul M. Skare	Paul.Skare@pnnl.gov	(509) 372-4210
Shabbir A. Shamsuddin	Shamsuddin@anl.gov	(630) 252-6273
Josef D. Allen	allenjd@ornl.gov	(865) 576-0994

IEC 61850/IEC 62351 Issues & Gaps

- Security standard for communication in substations and beyond
- The purpose of IEC 61850, as a whole, is to provide automation for heterogeneous Cyber-Physical Devices/Intelligent Electronic Device (IED) platforms
- Strictly application layer protocol (TCP/IP)
- IEC 61850 standard lacks an accepted security standard to support its functional capability
- IEC 61850, does not have a defined approach for cyber security that the vendors supplying the products have accepted
- IEC 62351 addresses information security for several protocols of IEC 61850 though at present it does not fully address security issues
- Specific needs include security for Generic Object Oriented Substation Event (GOOSE), Generic Substation Status Event (GSSE), and Sampled Measured Values (SMV) profiles
- Goose/SMV messaging not secured due to vendor resistance to existing IEC 62351 approaches

IEC 61850/IEC 62351 Issues & Gaps (contd.)

- **Hash-based Message Authentication Code (HMAC) for message integrity and authenticity of data (IAD)**
- **Galois Message Authentication Code (GMAC - is based on the Galois/Counter Mode) is faster and Galois based methods have been proven to be computationally more efficient**
- **Message Authentication Code only provides (IAD) for message BUT how can we trust the sender and receiver**
- **Group Domain of Interpretation (GDOI) at the router level (group key protocol whereby all group members register with a key server) strongly pushed by CISCO (can you say vendor lock)**
- **Key Management protocol is unsolved**
- **Backwards compatibility for different security levels and impacts heterogeneous computational elements**
- **Secure Remote updates of Cyber-Physical Devices**
- **Remote Attestation of integrity of software/hardware modules**