Response to the DOE: **Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure**

Date of Submittal: June 7, 2021

Submitted by:

Margaret Goodrich – PCITech – Margaret@pcitek.com
Herb Falk - Out of The Box Consulting Services - Herb.Falk@otb-consultingservices.com
Mark Adamiak - Adamiak Consulting LLC – AdamiakConsulting@aol.com

1. What technical assistance would States, Indian Tribes, or units of local government need to enhance their security efforts relative to the electric system?

The transition of the electric grid to the Smart Grid has made the operation of the grid dependent upon communications. There are to several factors that have contributed to this transition which are, but not limited to:

- Significant penetration of Distributed Energy Resources (DERs) – specifically rooftop solar
- Forthcoming migration to Electric Vehicles (EV) and required charging stations
    - Vehicle-to-Grid generation
- The need to be able to perform more work with fewer people due to downsizing
    - Fewer engineers entering the electric utility industries
- Faster restoration expectations
- Operation optimization and Distribution State Estimation (through Synchrophasors)
- Demand Side Management (DSM) for load management and the ability to respond to climate change through low carbon/no carbon generation
    - Integration of Smart Buildings into the grid
- Replacement of old technologies that are no longer available.

This short list identifies functions that are dependent upon reliable and trustworthy communication and information exchange.

Trustworthy information is dependent upon establishing the authenticity of the source of the information and that the information has not been modified at rest or in transit (a.k.a. integrity). Confidentiality of information may be required due to privacy or operational concerns, but the need should be determined via policy. These precepts form the basis of a triad of Confidentiality Integrity and Authentication (CIA). CIA is often augmented by the need to Authorize or restrict allowed actions (expanded to CIAA). It is these concepts and the protocols that support them that enable the aforementioned functions to be achieved in a secure manner.

The reality is that most of the communication infrastructure in the US is not capable of providing CIA and Authorization. A plan needs to be developed:

- Remove the technologies that are not capable of providing CIAA
- Evaluate CIAA needs based upon defense in depth and breadth
- Based upon the evaluation deployment of appropriate technologies - address the identified CIAA requirements.

As an example, consider that most inverters in the US utilize Modbus. Modbus inherently does not provide the ability to provide CIA or Authorization. This would mean that Modbus should be replaced by secure Modbus which provides CIA, or the selection of a more modern protocol in inverters such as IEEE 1815 or IEC 61850. IEC 61850 contains a profile called Routable GOOSE that can SECURELY send a message or control to millions of meters very quickly (10s of milliseconds) – the speed being a function of the communication media.

Additionally, there are a number of protocols that can provide CIA ranging from proprietary protocols to standards-based protocols. An order of evaluation of preference should be developed such as: international (e.g. ISO/IEC, IEEE); national; de facto industry standards; and then proprietary. Part of the reason for prioritization is to provide more interoperability of deployed assets from different vendors which can provide deployment diversity. The need for deployment diversity is especially needed when considering redundant and resilient system and the real possibility of Hidden Failures in devices.

In analyzing the various communication requirements/use cases (found in the EPRI IntelliGrid[1] architecture report), one finds that communication security spans all potential communication profiles. In the US, there are two primary profiles in use for utility SCADA, namely, IEC 61850 and DNP (listed in the NIST Framework and Roadmap for Smart Grid Interoperability Standards) – both of which have well-defined security definitions. (Note: DNP security is under revision.) In as much as Interoperability among utility systems is a requirement, the specification of a select few would facilitate interoperability.

From a technical assistance perspective, the following next steps are recommended:

- Assistance in developing a secure communication Vision and deployment architecture for the future which should include, but not be limited to Analysis of security zones, risks, and mitigations based upon IEC 62443

- Secure Communications Education
    - Fundamentals of Communications (Ethernet, IP, TCP, Application layer)
    - Fundamentals of Security (for Protection, Control, and SCADA engineers)
    - Use of communication test tools (e.g. WireShark) Note: Mr. Falk has created a 61850 Utility Specific version of WireShark

- Training
    - Hands-on in-person
        - Client-Server
        - Secure GOOSE, Secure Routable GOOSE, Swecure Sample Values (SV), Secure Routable SV (for Synchrophasors)
    - Virtual presentations
    - Recorded presentations

2. What specific additional actions could be taken by regulators to address the security of critical electric infrastructure and the incorporation of criteria for evaluating foreign ownership, control, and influence into supply chain risk management, and how can the Department of Energy best inform those actions?

With respect to securing the electric power infrastructure, there are both existing requirements (NERC CIP) and security solutions (IEC 61850/62351, Secure DNP, TLS). Clearly, isolation of utility operation networks (already a utility practice) should be mandatory. Mechanisms for better securing the utility external information network are needed. All remote access should use two-factor authentication using either a token or a verification code (obvious best practice). Jump Boxes are already in use in many utilities for connection between IT and OT networks and should be emphasized going forward.

The implementation of Security execution among control elements on the grid should be automatic with no human intervention other than configuration (i.e. – Key not visible to any human) and configuration should be a secure role. Implementation of key distribution is standardized in IEC 62351 through the use of Key Distribution Centers (KDCs).

As noted above, development of any security vision should reference IEC 62443 – defense in depth which would include both Physical and cyber security.

Implementation and periodic testing of protection, control, and monitoring functions in a utility is a critical part of assuring proper operation when needed. As test equipment is inserted into a secure communication path, functional operation can only be achieved if the test set is temporarily admitted to the secure communication group under test. The test equipment used in these test scenarios has been termed Transient Cyber Assets (TCAs). Going forward, system designs need to plan for the incorporation of TCAs into secure communication groups.

3. What actions can the Department take to facilitate responsible and effective procurement practices by the private sector? What are the potential costs and benefits of those actions?

It is to be noted that the new executive order from the Biden administration restricts the purchase of Utility equipment from a list of foreign vendors. Adherence to this EO by utilities AND industrials should be emphasized.

4. Are there particular criteria the Department could issue to inform utility procurement policies, state requirements, or FERC mandatory reliability standards to mitigate foreign ownership, control, and influence risks?
   No comment

References

1. EPRI IntelliGrid overview; http://mydocs.epri.com/docs/Portfolio/PDF/2011_P161.pdf

Submitted to: *ElectricSystemEO@hq.doe.gov*

Biographies:

Herbert Falk

Herbert Falk has been involved with cyber security since 2002 through his involvement with the EPRI Utility Communication Architecture (UCA), EPRI Intelligrid, NIST Smartgrid, and IEC TC57. He is the US Technical Advisory Group lead to IEC TC57 WG15 which is responsible for cyber security within IEC TC57. He is an editor of IEC 61850 and was responsible for several of the security standards associated with IEC 61850 and is actively working with the DNP Security Task Force. He actively participates in IEEE Power Systems Communication and Cyber Committee (PSCCC). He has performed several cyber risk/cost assessments around the world and has assisted many companies in improving their cyber footing and products.

Margaret Goodrich

Ms. Goodrich is the Treasurer and President of the UCA Users Group and President of Project Consultants, LLC (DBA: PCItek), a cyber-security products company that provides cyber security products for the 61850 and DNP3 communications protocols for the electric Utility Industry. She has been involved with various standards organizations including NERC, IEEE and the IEC to establish electric industry standards. Currently, she is active in the IEC 61850 and Common Information Model standards organizations and is the Co-Chair of the IEEE-PES CIM WG. Ms. Goodrich is very active in the testing community and serves as Co-Chair of the UCA Testing Committee working to develop a full ITCA Testing Organization for the 61850, CIM and OpenFMB standards. She has written and published reports and papers on behalf of her clients surrounding various topics regarding the standards, training, testing and integration platforms. Ms. Goodrich received her Bachelor's degree from the UT Austin. In Feb, 2001, she received a patent for the Operational Database Maintenance System (ODMS) and was awarded the IEC 1906 award in 2013. She is currently serving as the ANSI US Representative for the IEC Standards committees.

As Owner and President of PCItek, Ms. Goodrich is responsible for delivery and integration of all products and services and is currently providing consulting and integration solutions and cyber-security products to several utility clients around the world.

Mark Adamiak

Mark Adamiak is an independent consultant for the electric power industry. Mark started his career in the utility business with American Electric Power (AEP) and in mid-career, joined General Electric where his activities have ranged from advanced development, product planning, application engineering, and system integration in the Protection and Control industry. Mr. Adamiak is an original member of the IEC61850 WG on Utility Communications, a Life Fellow of the IEEE, and a registered Professional Engineer in the State of Ohio. Mark was the Principal Investigator for the EPRI IntelliGrid project to develop a reference architecture for the Smart Grid. In 2012, Mr. Adamiak was elected to the US National Academy of Engineering.