U.S. DEPARTMENT OF ENERGY

PNNL-22144

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

IEC 61850 and IEC 62351 Cyber Security Acceleration Workshop

April 25, 2012

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

This document was printed on recycled paper.
(9/2003)

Table of Contents

Acronyms and Abbreviations

AC	Access Controls
ASAP-SG	Advanced Security Acceleration Project for the Smart Grid
CEDS	Cybersecurity for Energy Delivery Systems
CIGRE	International Council on Large Electric Systems
CIM	Common Information Model
CIP	Critical Infrastructure Protection
DHS	Department of Homeland Security
DNP	Distributed Network Protocol
DOE	Department of Energy
EIOC	Electricity Infrastructure Operations Center
GDOI	Group Domain of Interpretation
GE	General Electric
GMAC	Galois Message Authentication Code
GOOSE	Generic Object Oriented Substation Event
GPS	Global Positioning System
HMI	Human Machine Interface
Hz	Hertz
ICCP	Inter-Control Center Communications Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
MAC	Media Access Control
MMS	Manufacturing Message Specification
MPLS	Multi-Protocol Label Switching
NASPI	North American SynchroPhasor Initiative
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
ORNL	Oak Ridge National Laboratory
PII	Privately Identifiable Information
PKI	Public Key Infrastructure
PMU	Phasor Measurement Unit
PNNL	Pacific Northwest National Laboratory
RBAC	Role-Based Access Control
RFC	Request for Comment
SGIP	NIST Smart Grid Interoperability Panel
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
SSR	Subsynchronous Resonance
TASE	Telecontrol Application Service Element

TCP	Transmission Control Protocol
TLS	Transport Layer Security
UCA	Utility Communications Architecture
UDP	User Datagram Protocol
VCC	Virtual Control Center
VPN	Virtual Private Network
WAN	Wide Area Network
WG	Working Group
WISP	Western Interconnection Synchrophasor Program
XML	eXtensible Markup Language

1.0 Meeting Summary

The purpose of this workshop was to identify and discuss concerns with the use and adoption of IEC 62351 security standard for IEC 61850 compliant control system products. The industry participants discussed performance, interoperability, adoption, challenges, business cases, and future issues.

Paul Skare from PNNL introduced the day's agenda. He described the objectives for the project and the purpose of the meeting involving industry vendors and DOE national laboratories. All attendees introduced themselves, their background/role, and their objectives for the workshop. Several methods of providing feedback, both in person and offline, were discussed. The tone of the day was to have an informal meeting to solicit information and discuss issues related to the IEC standards, their adoption, and the future.

David Manz from PNNL facilitated the discussions. The morning included introductions and expectations followed by discussions covering challenges to implement IEC 62351 TCP/IP Part 3 and MMS Part 4. During lunch, Phil Craig from PNNL presented a high level overview of the PNNL projects, capabilities, and activities. After lunch, all attendees were given a tour of PNNL's Electricity Infrastructure Operations Center (EIOC). The EIOC is a user-based facility featuring best-in-class tools dedicated to energy and hydro power research, demonstration, testing, operations training, and back-up resources for energy utilities and industry groups. The group reconvened in the afternoon to discuss interoperability, conformance, certification and testing issues. The group discussed a need for a remotely accessible means of testing interoperability of vendor solutions. The day ended with a conversation about future issues and challenges.

2.0 Attendee List

Last Name	First Name	Organization	Email
Allen	Josef	ORNL	Allenjd@ornl.gov
Alvarez	Fernando	ABB	Fernando.alvarez@ch.abb.com
Clements	Sam	PNNL	Samuel.clements@pnnl.gov
Craig	Phil	PNNL	Philip.craig@pnnl.gov
Dagle	Jeff	PNNL	Jeff.dagle@pnnl.gov
Edgar	Thomas	PNNL	Thomas.edgar@pnnl.gov
Fries	Steffen	Siemens	Steffen.fries@siemens.com
Johansson	Erik	ABB	Erik.z.johansson@se.abb.com
Manz	David	PNNL	David@pnnl.gov
Shamsuddin	Shabbir	ANL	Shamsuddin@anl.gov
Skare	Paul	PNNL	Paul.skare@pnnl.gov
Xia	Sharon	Alstom	Sharon.xia@alstom.com
Absent Project Participants			
McComber	Rob	Schneider Elec.	Robert.McComber@telvent.com
Thanos	Daniel	GE	Daniel.Thanos@ge.com

3.0 Discussion Points

- What is the social perspective? The question was raised to identify stakeholders and responsible parties and to determine who is ultimately responsible for deploying IEC 62351 compliant products in the field. We discussed utilities and how their interests are motivated by regulation and the final bottom line.
    - What affects the bottom line? For-profit utilities need to justify security in this context.
- What is the warranty structure for products? The question was raised about vendor warranty with regards to security features and performance.
- Perhaps leverage the DOE CEDS Lemnos project profile approach? The Lemnos project developed secure communication profiles for virtual private network (VPN) connections. Those profiles might be of interested and use in the development of usability profiles for IEC 61850 security acceleration.
- Standards are reviewed every 3-4 years. Several participants explained that the standards themselves are reviewed periodically. During this discussion, several points were raised:
    - How does the standard process work in the cyber environment?
    - Some amendments are processed more quickly.
    - If not reviewed after 5 years, a standard becomes inactive until reviewed.
- How do we future proof? Must plan for future compromise. The question was asked how the vendors can try to future proof products to ensure that they can be upgraded and maintained once deployed as opposed to being replaced. One answer was that vendors are more interested in selling new products than in future proofing.
- The topic of IPv6 was raised.
    - With the wide spread use of network address translation technologies, IPv4 will continue to be in use for a while.
    - Privacy concerns. IPv6 raised privacy concerns and issue that will need to be addressed. If, for example, a media access control (MAC) address is embedded into the IP address, that might be construed as Privately Identifiable Information (PII).
    - Regardless of the new features and sophistication of IPv6, it will add complexity and require new devices to utilize the features properly.
- The topic of protocol negotiation was mentioned. For example, Transport Layer Security (TLS) provides for communication security protocol negotiation. One party can declare what protocols and methods they support and the other party can do so as well, then they decide if their security requirements are met and communication secured.
    - IEC 62351 Part 3.5.3 partially addresses this topic. But is it possible to state exactly what TLS protocol suites are supported?
- Compliance. How does this relate to conformance and certification? These words have connotations that we will have to be sensitive to when addressing conformance and certification
- Must add authentication. Several participants mentioned that for secure communication, authentication cannot be optional. If communication is encrypted for confidentiality it must always authenticate for integrity as well. However, the converse is not true. You can provide authentication without encryption if confidentiality is not a concern.
    - This approach must account for legacy systems.
    - When evaluating security for communication, the sample rate for authentication and negotiation must be data aware. The security solution should fit the requirements for

confidentiality, integrity, and availability without incurring cost prohibitive performance impacts.

- Integrity seems to be universally important for power grid applications though there may be varying levels of encryption needed.
- Define common roles and use cases. It was suggested that the creation of use cases and common roles would help facilitate the evaluation, interoperability, and testing of devices that use IEC 62351 to secure IEC 61850 devices. This could include:
    - Role-based access at the field level.
    - Educational guidelines.
- It was recommended that standards should not force highest security policy possible; rather they should allow graded approach for lower powered or legacy systems. Some went so far as to say this must be done.
    - Standard should be a common denominator that is flexible.
- Benefit of strict and simple when enforcing some mandatory security. In other words, have a minimum level of mandatory security and then have an optional range which will then allow the freedom to implement what is necessary/relevant for the vendor.
    - Having a standard that is too loose has serious downsides. These two needs will have to be balanced.
- There was a suggestion of mapping standards together. Identifying the relationships/overlaps and relevancies for various standards:
    - NISTIR 7628
    - DHS Catalog of Standards
    - NERC CIP
    - German standards (relating to ISO/IEC 27001, ISO/IEC 27002 and domain-specific implementations)
- It was mentioned that logging is an important topic for security and IEC 62351 should have some logging requirements which are defined in 1686.
- Phasors and synchrophasors were discussed. There were several issues and discussions on various topics (including but not limited to):
    - Sampling rates
    - Physical layer
    - WISP (Harris data network)
    - UDP (user datagram protocol)
    - MPLS (multi-protocol label switching)
- It was mentioned that developing 5-10 uses cases would be helpful. Europe and SGIP have hundreds of use cases; but this raises the question, are they regionally specific?
    - Gap analysis based on the use cases could be of value as well.
- Common Criteria was discussed briefly; but it might not be practical for things like smart meters.
- The topic of audits was brought up. Audits will be Part 10 of IEC 62351 which as of yet us unwritten.
    - Should this only be a recommendation?
    - NERC CIP requires audits.
    - What is IEEE's audit approach? Could this be useful to leverage?
- The conversation then migrated to "What can we do together?" How can the various groups at the workshop improve the state of security for control system devices using IEC 61850 and IEC 62351?

    - Participate in a test lab. A venue or means of accessing a test interoperability, conformance, performance and security suite would be useful. This could be remotely used by the vendors to test and evaluate new products.
    - Another suggestion was to combine resources for reference architecture.
- We need people to join the IEC working group discussions. DOE Laboratory involvement would help us understand the vendor and industry perspective.
- IETF Credo: “Rough Consensus & Running Code.”
    - Developing standards while attempting to implement is a challenge but it can be done.

4.0 Top Issues/Challenges

- Few utilities request IEC 62351 compliant products. Utilities are motivated by regulation and owner directives. Regulations could increase adoption of security products as well as articulating and demonstrating the business case for security solutions.
- The topic of performance issues was brought up. Security is always a tradeoff. Cost and performance are sacrificed for increased security. But this tradeoff needs to be well understood. Furthermore, performance requirements in many critical infrastructures are real-time and mission critical. Any communication or security solutions must ensure that the operations and mission are not impacted.
- Cost of equipment, commissioning, maintenance was also raised. Security adds complexity which needed to be factored in as well.
    - Utilities need to make money. Some utilities are investor owned, and all utilities need to ensure they can cover their costs.
    - Utilities are forced to comply with regulations, see previous comments above.
- The important topic of key management was discussed by all parties. Several topics were raised including:
    - PKI issues. Infrastructure remains a complex problem in traditional IT environment as well and critical infrastructure deployments.
    - Expensive. The complexities, labor, and scale of key management often make it an expensive endeavor.
    - Revocation. This topic was debated. Some participants thought the topic was overblown and not as difficult as it has been made out to be. However, other participants were not convinced and thought revocation is still a challenge for key management.
    - Special characters should be required in creating keys.
- Several participants mentioned the lack of interoperability. The idea of a test center or test lab was an idea to explore to rectify this problem.
- The topic of conformance was brought up. What is conformance? What is minimal conformance? What would conformance look like?
    - IEC 62351 Part 6 isn’t used; the rest could have conformance.
- What are the differences between interoperability, conformance, and certification? What is needed? What is the appropriate role for a DOE national laboratory?
    - For example, several vendors use OpenSSL; this should help with interoperability and possibly conformance.
- Hardware constraints are always an issue. For example, a lot of security depends on memory, which can’t be depended on in an embedded system. Hardware costs and the supply chain are also issues.
- Industry experience and knowledge. The skillsets are often rare and hard to replace.

- Dynamic nature of cyber and rapid changes in the security environment. Do we need a standard that is flexible enough to keep pace with the changing security environment? Given the rapid pace of cyber, computer, and network security, can we expect a standard to keep up with this changing pace? Is that the role of a standard? If so, how does a standard adapt at that increase speed. Most other domains and topics are as fast passed. If there is not a standard how does security keep up?
- Real-time. The real-time performance characteristics of control systems in the critical infrastructures are crucial and key to their mission. This performance constraint must be respected and supported.
- Does the standard require, use, or ignore TLS negotiation? What is the point in reinventing the wheel if many devices can implement TLS protocol suite negotiation?
- How do we articulate the differences between IEC 62351 and a virtual private network (VPN)? How do we explain to a non-technical audience the difference?
- How do we articulate the differences between IEC 62351 and role-based access control (RBAC)? How do we explain to a non-technical audience the difference?
    - IEC 62351 includes RBAC; need to be clear about this from a perception as well as standards content point of view.
- Performance must be able to support authentication (e.g., hash). Several participants mentioned that authentication must not be optional. To have security you must have authentication.
    - There's interest in having authentication without confidentiality.
    - As an example, TLS and MMS (manufacturing messaging specification) requires confidentiality.
- Performance must balance the issues of cryptographic performance in legacy devices and architectures.
    - For example, a system that has defaulted or become a legacy can alarm and report the issue but continue to operate to ensure mission continuity.
- Terminology discrepancy is an eternal bane for any technical discussion, oral or written. This was no different for this meeting. Several times we discussed "correct" terminology and there was no consensus. For example, confidentiality is not the same as encryption; encryption is converting clear text to cipher text.
- The current standard of IEC 62351 does not allow an engineer to set the security policy such as the TLS configuration which does not accept low security connection parameters. These decisions are forced on the engineer for simplicity's sake but do not allow customization or tweaking to satisfy varied security policies.
- Protocol conformance statements. It was often repeated that the industry needs protocol conformance statements for each standard to create testing of use cases for security, performance, etc.
- Bootstrapping (updating equipment) in the field. In an attempt to future proof devices, and given the quickly changing security landscape, secure and reliable means of updating and upgrading devices is a must. This is of course, tempered by a commercial interest in selling new devices to customers.
- Another topic that was brought up was web services. The industry is seeing a faster adoption of web services but no current part of the IEC 62351 standard supports it. This is a complex issue and there has been little convergence by industry to date.
- Gaps in alarms/alerts can be a concern for utilities deploying these devices. The reliance on alerts and the associated false positives and false negatives have a real financial cost.
    - It is worth noting that this topic will be addressed in a future section of the IEC 62351 standard.

- When discussing security devices the topic often comes to liability, responsibility, and accountability. This topic covers security devices when they are operating correctly and more importantly when they are operating incorrectly. In the current environment for security devices, vendors are not held liable.
- Authorization is addressed in the RBAC section, which usually requires PKI. The local policy will decide this.
- Engineering access/management is covered in Part 7.

5.0 Interoperability Testing

- Interoperability was brought up several times by different participants. One issue that was raised was to have another face-to-face meeting. For example, should there be a plug fest? Alternatively, or in addition, a continuous service for testing interoperability is preferred by some participants. A remotely accessible service that could be used without travel and equipment relocation could provide a framework for interoperability, performance, and security testing. PNNL GridOPTICS powerNET testbed that was presented to the audience could be used to support the testing framework.
- This interoperability is similar to the DNP3 protocol testing tools.
    - The exception from DNP3 is that this would be a remotely accessible resource.
- UCA International could be a potential partner or example for this type of testing. Furthermore, NIST SGIP has testing examples that could be leveraged for this as well. A final example was mentioned: CIM & ICCP, with contact information for the two topics as needed.
- It is important to point out that conformance and operability are NOT claims of security.
- There is a need for a reference or mark client implementation and a mark server implementation.
- Key management is an issue for interoperability. Do we use PKI. If we use PKI how do we do system of system composition? For example, how do we handle Group Domain of Interpretation (GDOI- 90-5; & 90-6) multicast RFC?
- How do we accomplish initial registration, key updating, and bootstrapping?
- Testing cases:
    - Protocol level
    - Client server
    - PKI (public key infrastructure)
    - Key updates
    - Scalability
    - Real-time responses
    - Performance
    - RBAC
    - Group Domain of Interpretations (GDOI Part 90-5)
- Phased testing
    - Conformance with protocol
    - Interoperability within own products
    - Interoperability with other vendors
    - Use cases
- Testing by part or granularity within parts?
- Should this be binary? (Pass/fail, red/green per part? Overall?) Or cite performance characteristics?
    - Make the granularity be pass fail per part?
    - But also be able to combine parts IEC 62351 (3 & 8 for example)?

- Vendors conduct backwards testing with older products; vendors at this meeting didn't want to identify how far back they can go.

5.1 Testing Use Cases

- Discussed ASAP-SG protection profiles, but decided to be more specific.
- Start with use cases/roles
    - To develop tool
    - Then share tool
    - Use powerNET
- Example use cases:
    - State estimation (or multiple)
    - Intra-substation (GOOSE (generic object oriented substation events) messages)
    - Substation to substation (WAN)
    - Remote engineering access
    - Visualization (HMI to a system)
- There are multiple dimensions to these uses cases
    - Multiple telecommunication paths
    - Confidentiality, integrity, availability
    - Parts of IEC 62351
- Basic conformance testing
- Future use cases could include:
    - Substation to control room
    - PKI
    - State estimation (this may be better in the future due to its complexity)
- Expectations should be clearly defined (e.g., performance, jitter, delay, latency, etc.).
- Can we use the IEC 61850 use cases (e.g., the timing scenarios 4ms)?
    - These aren't fully developed. There was a suggestion to work with IEC TC57 WG10 to help them better define their use cases.
- Use case gap analysis

6.0 Adoption Challenges

- IEC 62351 Part 3 Data and Communication Security – Profiles Including TCP/IP, and IEC 62351 Part 5 Data and Communication Security – Security for IEC 60870-5 and Derivatives (e.g., DNP 3) are most adopted
- Understanding how it is better than VPN
    - VPN is just for remote use but IEC 62351 Part 7 Data and Communication Security – Security Through Network and System Management is not
- Expensive
- Implementation challenges
- Key management issues
    - Utilities often lack infrastructure
- High risk (new technology)
- Quality of service

- Cryptography is too high strength for legacy systems
- Mobility
- Vague
- Application-specific
- Virtual Control Center (VCC) needs limiting
- Only see ICCP Norway TASE.1

7.0 IEC 62351 Part 4 Profiles Including MMS

- Is IEC 62351 Part 4 Data and Communication Security – Profiles Including MMS needed? T-profile security is more popular than A-profile security. No known deployments of A-profile security.
- There are several functions in MMS that aren't used. Should we limit the functionality of things not used by ICCP or IEC 61850 (e.g., web services)?
- Security is arguable.
- Elcom TASE-1.

8.0 Future Activities

- Upcoming meeting Fall 2012:
    - Workshop at PNNL: Joint WG19, NIST SGIP AC, EU M, 490.
    - Including Study Committee – SC CIGRE D2.28 (Communication Architecture for IP-based Substation Applications).
    - IEC TC57 WG15 security architecture into TC57 reference architecture of information standards.
- The group recommended that David Manz or someone else from PNNL join IEC TC57 WG15.
- Security profiles should be driven by use cases.
- Management interfaces (currently on hold).
- End point security (field devices) was going to be addressed but is currently on hold (funding issue).
- Conformance may be country specific.
- The participants suggested reviewing electric and plug-in vehicles.

8.1 IEC 61850 Part 90-5 (PMU)

- *Supplementary Information: IEC/TR 61850-90-5 extends the capabilities of IEC 61850 to include support for synchrophasor information distribution in a scalable manner over a WAN through utility and public communication networks.*Integrity for PMU traffic is critical. Review IEC 61850 90-5. What level will be supported as well as what groups and individuals. How will security be handled will all messaged be cryptographically signed?
- What are the gaps?
    - What about wide area? These solutions must work over various physical networks (e.g., wire, fiber, wireless). ~~[~~*Supplementary Information: According to IEC 61850 Part 90-5, the standard provides the scalability needed for large wide area measurement systems such as those envisioned by NASPI. With Part 90-5, synchrophasors can leverage existing widely-deployed IP multicast technologies for reliable and robust communications on large scale*

wide area networks while also supporting the advanced key management techniques needed for electric grid monitoring.

- Likely going to go to 120 samples per second. *Supplementary Information: Time synchronized phasor measurement (i.e., synchrophasors) involves measuring electric system frequencies and phase angles very precisely from 20-120 times every second at various points across the electrical grid over large geographic areas. Synchrophasor measurements are time stamped using very precise time sources such as GPS satellite signals. This provides very detailed and precise time synchronized measurements of the state of the electrical grid.*
    - Question was raised by the participants if it is possible to get to 1,000 samples per second?

8.2 IEC 61850 Part 90-6 Use of IEC 61850 for Distribution Automation

Supplementary information based on the meeting minutes of Power System Relaying Committee, Main Committee Meeting Agenda, January, 13, 2011, Atlanta, GA:

- *IEC 61850 Part 90-6 standard addresses use of IEC 61850 for Distribution Automation*
- *IEC TC57/WG17 is currently working on a technical report to address IEC 61850 Part 90-6 user requirements.*

The discussion below was on messages and sample rates. PMU discussion relates back to IEC 61850 Part 90-5 above.

- Can handle up to 4000 messages per second using GMAC
- Starts with signing which is way too slow
- 30 samples per second in PMU can find sub-5Hz information
- SSR needs 120Hz information

8.3 XML

- How sensitive is labeling CIM data?
- Applying XML security
    - IEC 61850 commands/data packets
    - Configuration files
        - Multiple signature approach
        - Offline configuration of device
- XML doesn’t have session concept
- XML that uses signing is very expensive
- Same problems as GOOSE – performance issues

8.4 SNMP

- SNMP isn’t required; should it be?

9.0 Disclaimer

These minutes are an aggregation of multiple sets of notes taken during the workshop. Effort has been made to remove attribution to comments and discussion points while still keeping the value of the contribution.